Struggling to strike the right balance between interests at stake

Moyakine, Evgeni; Tabachnik, A.

Published in:
Computer Law & Security Review

DOI:
10.1016/j.clsr.2020.105512

Publication date:
2021

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology

E. Moyakine[a,b,*], *A. Tabachnik*[b]

[a] *University of Groningen – TLS, Groningen, the Netherlands*
[b] *University of Haifa – CCLP, Haifa, Israel*

ARTICLE INFO

Keywords:
Russian legislation
Yarovaya law
Fake news law
Disrespect law
Human rights
Privacy
Data protection
Freedom of expression
Public safety
Public security

ABSTRACT

The article deals with the legislative amendments that have been recently adopted in the Russian Federation, the so-called 'Yarovaya' law, the 'fake news' law and the 'disrespect' law. It explains the essence and problems of implementation of the above-mentioned legal instruments and assesses them from the human rights angle. It is established that the rather complex laws under analysis pose significant threats to the human rights and fundamental freedoms of individuals, including privacy, data protection and freedom of expression, and introduce other additional negative effects to the Russian society and economy. While in the adoption of such legislation it is crucial to give due weight to the involved interests, the used examples indicate that the State's interests seem to prevail at the cost of the rights and freedoms of those who need to be adequately protected.

1. Introduction

Cyberspace has become deeply integrated in our lives: it is currently impossible to imagine the existence of a modern individual without a variety of technical tools, including smartphones, tablets and computers, that are constantly connected to the world wide web and utilized on a daily basis. Cyberspace not only offers many new opportunities in the struggle for democracy and respect of human rights but also poses a wide range of challenges and can be used and abused in the domain of national security. It constitutes a unique battlefield where governments – often with the assistance of various private actors – fight new types of war, including struggles for the minds of people, a realm which ever more deeply influences the development of our economy and civil society.

In the recent years, information warfare (hereinafter: IW) in cyberspace has become Russia's major tool in its conflict with the West. Through IW, particularly propaganda efforts in cyberspace, Russia has allegedly repeatedly intervened in the election processes and internal affairs of the US, Germany, the United Kingdom, Ukraine and several other countries.

* Corresponding author at: University of Groningen – Faculty of Law – TLS, Oude Kijk in 't Jatstraat 26, 9712 EK Groningen, the Netherlands.
E-mail address: e.v.moyakine@step-rug.nl (E. Moyakine).

https://doi.org/10.1016/j.clsr.2020.105512
0267-3649/

Additionally, through IW Russia has reportedly striven to challenge the stability of the leading Western countries.[1]

At the same time, the Russian leadership is convinced that Moscow is endangered by internal and external foes seeking to challenge Russian national security, including that of the information sector. From Moscow's perspective, the internet, and the free flow of information generally, threatens Russian national security. Thus, in order to prevent a possible Western (or/and pro-Western forces in Russia) effort to destabilize Russia (as it is perceived in Russia) through IW in cyberspace, Moscow should take the necessary precautions.[2]

Moscow accordingly strives to keep information flow in Russian cyberspace under its strict control. Thus, it aims to prevent or deter as much as possible dissemination of information which may create a negative image of the country and its leadership, or any activity which may endanger the regime's stability.

Therefore, through legislation and regulation Moscow tries to strengthen control over the information flow in the Russian segment of cyberspace and accordingly to preserve the stability of the current regime (as believed by the authorities in Moscow). In this regard, a number of laws/amendments accepted by the Russian parliament and signed by the President in the last years are particularly noteworthy: the 'Yarovaya' law, the 'fake news' law and the 'disrespect' law, which will be discussed below.[3] To the general public, this legislation is presented as a necessary measure for the preservation of public safety and as an anti-terrorist measure.

It is and remains a question however whether this legislation is a feasible and effective tool for ensuring public safety and which human rights complications it may have, more specifically those related to privacy and data protection. Moreover, how will this legislation affect other fundamental rights such as the right to freedom of expression?

2. Background

Balancing between national security needs and data privacy rights remains a core dilemma in the field of rule of law in cyberspace. In this regard, 'data privacy rights represent a special form of respect for the human right to privacy. An individual's right to have his or her personal data – name, telephone number, address, health, physical location, financial information, and other such identifiers – protected from use by others without his or her consent is derived from the general right of the individual to privacy. This right has been codified at the international level, *inter alia*, by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR), the European Convention for the Protection of Human Rights and Fundamental Freedoms, and several other regional human rights treaties'.[4]

Also 'in the cyberspace context, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations notes that international human rights law applies to cyber-related activities of a state as a matter of *lex lata*, and that individuals enjoy the same international human rights (such as privacy) with respect to cyber-related activities that they otherwise enjoy'.[5] Overall, the ideas regarding a level of control of governmental structures over cyberspace range from digital libertarianism to complete digital sovereignty. At the same time, particular national and regional jurisdictions interpret and apply data privacy rights in different ways.[6]

The majority of EU Member States seems (in comparison to other major internationals governmental players) to take the most balanced position in protecting privacy rights and freedom of expression and taking into account the needs of national security, for example the EU General Data Protection Regulation (hereinafter: GDPR), which includes explicit data protection mechanisms and introduces a variety of obligations and rights.[7] At the same time, considering the balancing act between digital libertarianism and digital sovereignty, the European regulation is rather closer to the libertarian approach than to digital sovereignty. That is, the GDPR

[1] Keir Giles, *Handbook of the Russian Information Warfare* (Fellowship Monograph, NATO Defense College (Research Division) 2016); Raphael S Cohen and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat* (Report, RAND Corporation 2019).

[2] Valeriy Gerasimov, 'The World on the Edge of War: It is not Enough to Take into Account Today's Challenges, It is Necessary to Predict Future Ones' (in Russian) (*Voyenno-promyshlennyi Kuryer*, 13 March 2017) <https://vpk-news.ru/articles/35591> accessed 20 August 2020; 'Patrushev Urged to Protect Young Internet Users from Foreign Intelligence Services' (in Russian) (*Interfax*, 19 July 2019) <https://www.interfax.ru/russia/669683> accessed 20 August 2020.

[3] Federal law dated as of 06.07.2016 No. 374-FZ 'On the Adoption of Amendments to the Federal Law "On Countering Terrorism" and Specific Legislative Acts of the Russian Federation Regarding the Establishment of Additional Counter-terrorism Measures and Ensuring Public Security' (in Russian) (*Kremlin.ru*) <http://kremlin.ru/acts/bank/41108/page/1> accessed 25 August 2020; 'A Law Has Been Signed Establishing Administrative Responsibility for the Dissemination of Knowingly Inaccurate Socially Significant Information' (in Russian) (*Kremlin.ru*, 18 March 2019) <http://kremlin.ru/acts/news/60082> accessed 25 August 2020; Mark Krutov, 'You are violating the law, dear [Sir]! The First Day with the "Law on Disrespect Towards Authorities" (in Russian) (*Radio Liberty*, 29 March 2019) <https://www.svoboda.org/a/29849863.html> accessed 20 August 2020.

[4] Deborah Housen-Couriel, 'Balancing National Security and Data Privacy: A Key Regulatory Challenge in Cyberspace' (4 March 2018) <https://csrcl.huji.ac.il/people/balancing-national-security-and-data-privacy-key-regulatory-challenge-cyberspace> accessed 25 August 2020.

[5] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) ('Tallinn Manual 2.0'); Deborah Housen-Couriel, 'Balancing National Security and Data Privacy: A Key Regulatory Challenge in Cyberspace' (4 March 2018) <https://csrcl.huji.ac.il/people/balancing-national-security-and-data-privacy-key-regulatory-challenge-cyberspace> accessed 25 August 2020.

[6] Jack M Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' 2004 79 New York University Law Review, 1-58; James Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors' 1997 66 University of Cincinnati Law Review 177-205.

[7] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation).

contains provisions that allow governmental structures to collect and process personal data that otherwise have a protected status. However, the GDPR incorporates a set of constraints which limits government's capabilities to access personal information and thus protects the fundamental rights of data privacy (inter alia, necessity, proportionality, transparency and fairness).[8]

This corresponds to the criteria defined in the Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age. The report recognizes that the right to data privacy can be subject to restrictions under certain extraordinary circumstances: for example, by means of governmental surveillance measures directed at prevention of terrorism or serious crime. However, there is a need for further practical guidance with regard to this interference that must be 'grounded in international human rights law, on the principles of necessity, proportionality and legitimacy in relation to surveillance practices'.[9] Also, the European Data Protection Supervisor underlines relevance of the fundamental rights to privacy and data protection in the current day and age, more specifically when it comes to online manipulation, and a mutual dependency between these rights and freedom of expression.[10]

Therefore, 'in line with the Special Rapporteur's view, an optimal regulatory balance between the protection of personal data and national security considerations will permit necessary and proportional exceptions to the protection regime. Criteria for swaying the balance away from individual privacy rights will be included in a transparent way within the statutory regime, so that judicial review of national security and other exceptions is feasible and available to data subjects who want to contest carve outs'.[11]

However, complexities of the application of international law in cyberspace are rising due to a recent trend on the advancement of digital sovereignty by a number of key countries in the international system, foremost the People's Republic of China and the Russian Federation. Digital sovereignty can be defined as an effort to control and govern access, information flow and infrastructure in digital sphere by governments within their sovereign jurisdictions.[12]

China and Russia promote digital sovereignty in order to protect their national security and regimes' stability, as claimed by the respective regimes. Both countries strive for greater control over their own cyberspace and consequently more control over information flow, disregarding data privacy and freedom of expression.[13] Moreover, these efforts may encourage other countries such as Iran, Turkey, Saudi Arabia, Egypt and many others to reinforce strict control over their 'parts' of cyberspace and to infringe fundamental human rights in cyberspace.[14] Consequently, the last efforts of 'sovereignization' of cyberspace widen the gap between the Western-liberal democracies (foremost the EU and US) on the one hand and the key non-democratic countries such as the PRC and Russia on the other hand in the field of cyber regulation and particularly data protection and implementation of basic human rights such as freedom of expression in the digital domain.

These developments shape a new momentum in the sphere of privacy, data protection (retention) and freedom of expression in cyberspace and shift the balance in favor of State actors at the expense of respect for and protection of fundamental human rights and freedoms such as the rights to privacy and data protection and freedom of expression. Moreover, differences between approaches towards upholding the abovementioned human rights and freedoms and protecting national security in various countries lead to new questions regarding the protection of personal data in the global context, especially considering trans-jurisdictional flow of personal information.[15] In particular, it becomes pertinent to answer the question how the EU should deal with the latest changes in the Russian legislation and regulation in the field of data

[8] Deborah Housen-Couriel, 'Balancing National Security and Data Privacy: A Key Regulatory Challenge in Cyberspace' (4 March 2018) <https://csrcl.huji.ac.il/people/balancing-national-security-and-data-privacy-key-regulatory-challenge-cyberspace> accessed 25 August 2020.

[9] Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, 'The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights' (U.N. Doc. A.HRC/27/37, p. 16, 30 June 2014) <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf> accessed 16 July 2020.

[10] European Data Protection Supervisor, *EDPS Opinion on Online Manipulation and Personal Data*, Opinion 3/2018 (19 March 2018) <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf> accessed 25 August 2020.

[11] Deborah Housen-Couriel, 'Balancing National Security and Data Privacy: A Key Regulatory Challenge in Cyberspace' (4 March 2018) <https://csrcl.huji.ac.il/people/balancing-national-security-and-data-privacy-key-regulatory-challenge-cyberspace> accessed 25 August 2020.

[12] Stephane Couture and Sophie Toupin, 'What Does the Notion of "Sovereignty" Mean When Referring to the Digital?' (2019) 21(10) *New Media & Society*, 2305; Abid A Adonis, 'International Law on Cyber Security in the Age of Digital Sovereignty' (*E-International Relations*, 14 March 2020) <https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/> accessed 21 August 2020.

[13] Stanislav Budnitsky and Lianrui Jia, 'Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance' 2018 21(5) European Journal of Cultural Studies, 594-613.

[14] UN Human Rights Council, 'The actions of the Russian Federation are jeopardising online freedoms everywhere' Item 4 General Debate - Oral Statement, (27 June 2018) <https://rsf.org/sites/default/files/unhrc_item_4_statement_on_russia_-270618_en.pdf> accessed 19 August 2020.

[15] UN Human Rights Council, 'The actions of the Russian Federation are jeopardising online freedoms everywhere' Item 4 General Debate - Oral Statement, (27 June 2018) <https://rsf.org/sites/default/files/unhrc_item_4_statement_on_russia_-270618_en.pdf> accessed 19 August 2020; Karina Barbesino, 'Treatment and Evolution of Digital Rights: A Comparative Analysis of China, Russia, the United States, and Germany' 2019 Rollins College: Honors Program Theses. 97. <https://scholarship.rollins.edu/honors/97> accessed 16 July 2020; Hao Yeli, 'A Three-Perspective Theory of Cyber Sovereignty' 2017 7(2) Prism, 109-115. <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1983767/a-three-perspective-theory-of-cyber-sovereignty/> accessed 30 July 2020.

protection and freedom of expression in cyberspace (that can be found in the 'Yarovaya', 'fake news' and 'disrespect' laws).

Apparently, the Russian vision of appropriate policy and law enforcement methods towards cyberspace reflect fundamentally different concepts in comparison to those prevalent in the EU, particularly regarding the crucial balancing act between the interests of national security on the one hand and protection of personal data and freedom of expression on the other hand. It is obvious that the Russian policy explicitly leans towards the adoption of a sovereignty approach. Presumably, the Russian legislation lacks specific and transparent criteria determining the limits of governmental intervention into private affairs of Russian citizens and their personal data, i.e. Russian legislation and regulation can be said to lack necessity, proportionality, transparency and fairness.[16]

Overall, the Russian legislation adopted in the field of personal data protection and freedom of expression in cyberspace is perceived as under-researched, similarly to comparative research of that regulation and the rules and procedures established in the EU. Not much attention has been devoted by legal experts to the three above-mentioned Russian legislative acts that have not been extensively analyzed. In their publication, Mikhail Zhuravlev and Tatiana Brazhnik focused on the data retention requirements introduced by the 'Yarovaya' law but did not discuss the other two laws that are assessed in the current contribution.[17] Moreover, it is necessary to investigate the compliance of the new Russian legislative framework with the European human rights standards. In addition, this legislative framework should be held against the data protection requirements introduced in the General Data Protection Regulation that numerous organizations processing personal data would not be able to comply with. In general, there is thus a need to conduct deeper research of the three Russian legislative acts and to compare their compatibility with the European standards on data protection and freedom of expression. What is the essence of the recently introduced changes in the Russian legislation and do these laws clearly define conditions allowing for the restriction of individuals' human rights and freedoms under exceptional circumstances? What may be the impact of these pieces of legislation on a global scale and how can it influence the interaction in cyberspace between countries with different approaches towards the protection of the respective human rights and freedoms and safeguarding the interests of national security? What are possible procedural safeguards to ensure that the 'Yarovaya' law, the 'fake news' law and the 'disrespect' law are compatible with the European human rights standards?

3. The new Russian legislation and its complexity

3.1. *The 'Yarovaya' law*

In the recent years, Russian authorities have passed a series of laws and amendments which demonstrate their determination to significantly reinforce control over information flows in the Russian sector of the internet. These efforts are mostly justified on the grounds of countering terrorism and promoting public safety. An illustrative example of such legislation is the Federal law of 6 July 2016 No. 374-F3[18] (also known as the 'Yarovaya' law[19]) introducing amendments into the Federal law regulating counter-terrorism and public safety measures. Specifically, Article 15 of this law incorporates changes in the Federal law of 27 July 2006 No. 149-F3 'Concerning information, information technologies and the protection of information', more specifically its Article 10.1. Article 10.1 of the amended law No. 149-F3 requires distributors of information, such as internet and telecom companies, messengers, email services, forums and other platforms that allow the exchange information on the internet, to store in the territory of the Russian Federation the following information[20]:

- Information on the facts of reception, transmission, delivery and/or processing of voice information, written text, images, sounds, video or other electronic messages of internet users and information about these users for one year after the end of such actions;
- Text messages of internet users, voice information, images, sounds, video and other electronic messages of internet users up to six months from the end of their reception, transmission, delivery and/or processing.

Additionally,

- distributors of information on the internet are obliged to provide the information specified earlier to an authorized executive authority (such as the Federal Security Service

[16] OHCHR, 'Mandates of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association; and the Special Rapporteur on Freedom of Religion or Belief, Communication to the Russian Federation' (Communication, 28 July 2016), 2 <https://www.ohchr.org/Documents/Issues/Opinion/Legislation/RUS_7_2016.pdf> accessed 27 August 2020; UN Human Rights Council, 'The actions of the Russian Federation are jeopardising online freedoms everywhere' Item 4 General Debate - Oral Statement, (27 June 2018) <https://rsf.org/sites/default/files/unhrc_item_4_statement_on_russia_-270618_en.pdf> accessed 19 August 2020.

[17] Mikhail S Zhuravlev and Tatiana A Brazhnik, 'Russian Data Retention Requirements: Obligation to Store the Content of Communications' (2018) 34(3) CLSR 496.

[18] Federal law dated as of 06.07.2016 No. 374-FZ 'On the Adoption of Amendments to the Federal Law "On Countering Terrorism" and Specific Legislative Acts of the Russian Federation Regarding the Establishment of Additional Counter-terrorism Measures and Ensuring Public Security' (in Russian) (*Kremlin.ru*) <http://kremlin.ru/acts/bank/41108/page/1> accessed 25 August 2020.

[19] 'In Russia, the "Yarovaya Law" entered into force' (in Russian) (*Novaya Gazeta*, 1 July 2018) <https://www.novayagazeta.ru/news/2018/07/01/142944-v-rossii-vstupil-v-silu-zakon-yarovoy> accessed 19 August 2020.

[20] Federal law dated as of 06.07.2016 No. 374-FZ 'On the Adoption of Amendments to the Federal Law "On Countering Terrorism" and Specific Legislative Acts of the Russian Federation Regarding the Establishment of Additional Counter-terrorism Measures and Ensuring Public Security' (in Russian) (*Kremlin.ru*) <http://kremlin.ru/acts/bank/41108/page/1> accessed 25 August 2020.

(hereinafter: FSB)) that conduct operational investigative activities or safeguard the security of the Russian Federation in the cases defined by the federal laws.
- Distributors of information on the internet network are obliged, when using additional encryption of electronic messages to receive, send, deliver and/or process electronic messages of internet users, and to provide internet users with additional encryption of electronic messages, to deliver to the federal executive authority in the field of security (such as the FSB) information necessary for decoding received, transmitted, delivered and/or processed electronic messages.

According to the law, for non-performance of any of these obligations, the operators (distributors of information) may be blocked in Russia. Note that in comparison with the common Western practice of law enforcement, the Russian law grants the special services much wider powers.[21] For example, to gain access to the users' personal data, in general Western intelligence agencies need to provide a court warrant to a telecom or internet operator. Upon receiving such a document, the operator is obliged independently to convey the required information to the law enforcement agencies. However, the Russian special services operate differently. Each telecom or internet operator is obliged by law to install special software and hardware, called SORM or System for Operative Investigative Activities, which allows the FSB to gain access to users' personal data. In this case, information is accessed by special services without the knowledge of telecom or internet companies. The FSB officer simply enters the command through the SORM control panel,[22] which is connected to the operator's servers. As a result, only the FSB officer and his superiors see the warrant issued by the court permitting access to information. Considering the poor record of rule of law[23] in Russia,[24] and the de facto subordinate position of courts[25] to the executive authorities, the special services, such as the FSB, enjoy absolute freedom of action and absence of oversight. This situation is made even worse by the lack of public or parliamentary control over the work of the special services.

3.2. *The 'fake news' and 'disrespect' laws*

Furthermore, on 18 March 2019 President Putin signed two additional amendments to the Federal Law which enhance governmental control over the Russian cyberspace. In Article 15 of the Federal Law of 27 July 2006 №149-FЗ[26] 'Concerning information, information technologies and the protection of information', some changes have been incorporated. To the existing legislation, an amendment has been added stressing that distribution of unreliable socially significant information distributed under the guise of reliable messages that creates a threat of harm to life and health of citizens, property, the threat of mass disturbance of public order and public safety, or the threat of interfering in the functioning or stopping of functioning of life support objects, transport or social infrastructure, credit organizations, energy, industry or communications - is defined as the offence according to the law. This law is also called the 'fake news' law. Online news outlets and users that spread 'fake news' will face fines of up to 1.5 million rubles (approximately $20.300 according to the exchange rate of August 2020).[27] Moreover, it allows Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Media – the regulator) to block media publications in the pretrial order.

The second amendment which regulates 'disrespect' of the authorities (or internet insults) says that distribution of information in telecommunication networks, including in the internet, information expressing in an indecent form that offends human dignity and public morality, obvious disrespect of society, the State, official State symbols of the Russian Federation, the Constitution of the Russian Federation or State authorities power in the Russian Federation – sets fines of up to 100.000 rubles (the equivalent of approximately 1.350 US dollars according to the exchange rate of August 2020) and 200.000–300.000 rubles (the equivalent of approximately 2.700–4.050 US dollars according to the exchange rate of August 2020) or 15 days in jail for repeat offenses.[28] However, in this case the law is relevant exclusively to the dissemination of information through informational-telecommunication networks. Printed resources are not affected by this legislation.

It must be stated that the discussed amendments raise the questions regarding their efficacy and feasibility and a collateral damage which they may cause to the development of the Russian society and economy. We suppose that in

[21] Irina Filatova, 'How the Big Brother is Following Us: Experts Explained the Methods Used by Intelligence Services' (in Russian) (*Deutsche Welle*, 30 October 2013) <https://p.dw.com/p/1A7ij> accessed 21 August 2020.

[22] Ibid.

[23] Luke Harding, 'WikiLeaks Cables Condemn Russia as "Mafia State"' (*The Guardian*, 1 December 2010) <https://www.theguardian.com/world/2010/dec/01/wikileaks-cables-russia-mafia-kleptocracy> accessed 23 August 2020.

[24] Paul Radu, 'Russia: The Cellist and the Lawyer' (*OCCPR (Organized Crime And Corruption Reporting Project)*, 26 April 2016) <https://www.occrp.org/en/panamapapers/russia-the-cellist-and-the-lawyer/> accessed 21 August 2020.

[25] Mikhail Khodorkovsky, 'Russia's Courts of Injustice: Why Only Protesters Pose a Threat to Putin's Rule' (*TIME*, 14 May 2012) <http://content.time.com/time/magazine/article/0,9171,2113854,00.html> accessed 21 August 2020.

[26] 'A Law Has Been Signed Establishing Administrative Responsibility for the Dissemination of Knowingly Inaccurate Socially Significant Information' (in Russian) (*Kremlin.ru*, 18 March 2019) <http://kremlin.ru/acts/news/60082> accessed 21 August 2020.

[27] 'Putin Signs "Fake News", "Internet Insults" Bills Into Law' (in Russian) (*The Moscow Times*, 18 March 2019) <https://www.themoscowtimes.com/2019/03/18/putin-signs-fake-news-internet-insults-bills-into-law-a64850> accessed 20 August 2020.

[28] Varvara Percova and Aleksey Sivashenkov, 'With All Due Respect. What Will the Law on Insulting Authorities Bring to Runet?' (in Russian) (*Forbes*, 18 March 2019) <https://www.forbes.ru/obshchestvo/373297-so-vsem-uvazheniem-chem-obernetsya-dlya-runeta-zakon-ob-oskorblenii-vlasti> accessed 21 August 2020.

the medium and long term, these amendments may cause more harm to public safety and Russian socio-economic development than achieve the goal of safeguarding them.

4. Privacy and data protection concerns of the 'Yarovaya' law

4.1. *Council of Europe*

Notably, the fact of existence of surveillance regimes in itself does not constitute a violation of human rights, more specifically the rights laid down in Articles 8 and 10 of the European Convention of Human Rights (hereinafter: ECHR). These are the rights to respect for private and family life, home and correspondence and to freedom of expression. Any interference with the said rights that are not be regarded as absolute can be justified when it is in accordance with the law, seeks to pursue certain legitimate aims summed up in the second paragraph of these provisions and is necessary in a democratic society for protecting any of the listed interests. Surveillance regimes can be used to achieve the legitimate aims of the Member States of the ECHR, for instance in the sphere of combating terrorism and serious crime. This conclusion can be derived from the position taken by the European Court of Human Rights (hereinafter: ECtHR) in the long awaited and recently issued *Big Brother Watch* decision from September 2018.[29] The Russian system of surveillance that was under investigation of the Court was, however, deemed to be in violation of the right to private life of Article 8 ECHR. In the *Zakharov* judgment, the ECtHR concluded that the legislation of the Russian Federation for monitoring communications of its citizens was not in line with the requirement of 'quality of law' imposed by the European human rights law and the interference was not kept to what is necessary in a democratic society.[30] It seems that unfortunately not many valuable lessons have been drawn from this judgment by the national legislator and human rights are further infringed by the adopted legal instruments.

The decision in the *Zakharov* case was without doubt a remarkable one given that the applicant could not prove the fact of surveillance and of being personally affected by it and that the Court went as far as to examine the relevant Russian domestic laws *in abstracto*. Although, the Russian surveillance system, more specifically SORM, was concluded by the Court to violate Article 8 of the Convention, Zakharov was not able to effectuate the ECtHR's judgement in Russia. Shortly after this judgment was issued, in Russia an amendment was introduced to the Federal Constitutional Law that was based on the decision of the Russian Constitutional Court from July 2015 allowing the country to abstain from implementation of judgments of international human rights courts if they are considered as contradicting the Russian Constitution.[31] This law confers the power to the Constitutional Court to review any international human rights judgments and in fact invalidate them by declaring these decisions as impossible to execute. As a matter of fact, the court has already made use of this review power on several occasions, for instance, in relation to the ECtHR's judgment in the case of Anchugov and Gladkov against Russia.[32]

While there is a national legislation in Russia that allows the above-mentioned surveillance measures to be taken for achieving the legitimate aims of fighting serious crime and terrorism and protecting public security, it is to be stressed that the Russian data retention legislation fails to meet the quality of law requirement reconsidered by the ECtHR in the *Zakharov* case.[33] Although it is true that the national authorities have a certain margin of appreciation when they decide on the means for attaining the legitimate aims outlined above, this margin of appreciation is subjected to European supervision determining whether there are guarantees against possible abuse.[34] This abuse of power can be prevented if a set of minimum requirements is introduced in the law: 'the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed'.[35] The quality of law requirement means that the law must not only be accessible to individuals who should be able to foresee how it would apply in practice but also ensure that measures of secret surveillance are only used when it is necessary in a democratic society and establish safeguards and guarantees against abuse that are both adequate and effective.[36] In the Russian legislation, it is not specified what the nature of the offences is that give rise to the application of the data retention rules. The procedure for examining, storing and processing personal data is far from clear, it is not defined who the authorities are that are authorized to get access to the information in question and which bodies supervise the exercise of these powers. There should also be national remedies provided for by the law against the use of the said measures that are open to individuals subjected to this form of surveillance. The 'Yarovaya law' cannot be said to meet the requirement of quality of law and does not manage to limit the interference strictly to what is necessary in a democratic society. Introducing the data retention obligations and allowing access of national authorities to this data do not constitute a restriction of the human right to privacy and data protection laid down in Article 8 ECHR and may be said to violate this provision.

[29] *Big Brother Watch and Others v. the United Kingdom* App no 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018), para 386.

[30] *Zakharov v. Russia* App no 47143/06 (ECtHR, 4 December 2015), paras 302-305.

[31] Federal Law of 14 December 2015 on Amendments to the Federal Constitutional Law 'On the Constitutional Court of the Russian Federation' (in Russian) (*RG.ru*, 16 December 2015) <https://rg.ru/2015/12/15/ks-site-dok.html> accessed 20 August 2020.

[32] *Anchugov and Gladkov v. Russia* App no 11157/04 and 15162/05 (ECtHR, 4 July 2013); Constitutional Court of the Russian Federation 16 April 2016 <https://rg.ru/2016/05/05/sud-dok.html> accessed 20 August 2020.

[33] *Zakharov v. Russia* App no 47143/06 (ECtHR, 4 December 2015), para 231.

[34] Ibid., para 232.

[35] Ibid., para 231.

[36] Ibid., para 236.

4.2. *EU and Data Retention Directive*

One should observe that the new Russian legislation is also clearly at variance with the EU legal regime on privacy and data protection, more specifically rules on the retention of data. Data retention is associated with the process of storing and holding communication data for certain purposes, including those of law enforcement.[37] In the EU, the Court of Justice of the European Union (hereinafter: CJEU) has taken a firm stance against the data retention practices of the Union based on the Directive 2006/24 or the Data Retention Directive from 2006.[38] Article 3 Paragraph 1 of this Directive required EU Member States to introduce in their national jurisdiction an obligation aimed at providers of publicly available electronic communications services or public communications networks to retain data regarding their users or subscribers that are generated or processed by these providers. The retained information included traffic and location data and other data that are necessary to identify subscribers and registered users. The content of electronic communications was however not retained.

By using the stored data, it was possible to establish and identify a source, destination, date, time, duration and type of a communication.[39] In addition, the retention of data allowed identification of the equipment used and the location of mobile devices.[40] In accordance with Article 6 of the Directive, all this data could lawfully be retained for the period of 6–24 months counting from the date of the communication. In its preliminary ruling *Digital Rights Ireland,* the CJEU declared the Directive invalid on 8 April 2014.[41] The Court found that the spectrum of data retained by providers of public communications networks and publicly available electronic communications services was significantly wide and allowed for drawing very precise conclusions regarding the private life of the individuals concerned.[42] Among other things, one could learn a great deal about their habits, places of residence and social relationships.[43] Although, the content of communications was not retained, the retention of data falling under the scope of the Directive had an impact on the use of the means of communication by persons and could have a negative effect on the exercise of their freedom of expression found in Article 11 of the EU Charter of Fundamental Rights (hereinafter: the Charter).[44]

Under the reach of the Data Retention Directive, the data in question could be collected and processed without notifying the concerned users and subscribers meaning that they lived with a constant feeling of being secretly surveilled and monitored.[45] In addition, the far-going data retention practices required by the Directive seriously interfered with the rights to privacy and data protection laid down in Articles 7 and 8 of the Charter.[46] This interference was not deemed to be in line with the principle of proportionality, as stressed by the Court.[47] The Data Retention Directive concerned all persons, all possible means of communication and all traffic data and interfered with fundamental rights of almost all European citizens.[48] Additionally, no relationship between the retained data and threats to public security was required, the scope of application of the Directive was not limited, there were no objective criteria for establishing the limits of the access of national authorities to the collected data and its processing and no substantive and procedural conditions for granting this access and further use.[49] Also, the data could be retained for at least 6 months without any distinction made between different categories of data and the determination of this retention period was not based on objective criteria.[50] There were no safeguards regarding security and protection of data, it did not have to be deleted after the retention period and there was no requirement for retaining data in the EU.[51]

While the Russian Federation is of course not an EU Member State and the EU's legal regime does not impose direct legal obligations on Russia, it can be argued that even under the Strasbourg human rights framework there would be an incompatibility of the Russian surveillance system with the ECHR's standards. Drawing inspiration from the work of the CJEU, the ECtHR has referred several times to the *Digital Rights Ireland* decision when it analyzed surveillance measures taken in some Member States of the Council of Europe (hereinafter: CoE).[52] Similarly to the Russian laws, the invalidated Directive had an objective of contributing to the fight against serious crime and terrorism and protecting public security.[53] While in the EU, the data retention obligation was applicable to the providers of publicly available electronic communications services or public communications networks, in Russia its scope is broadened to include all possible distributors of information

[37] Ian Lloyd, 'Data Retention' (2018) 34(2) CLSR 405, 407.
[38] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 (Data Retention Directive).
[39] Article 5(1)(a), 5(1)(b), 5(1)(c) and 5(1)(d) Data Retention Directive.
[40] Article 5(1)(e) and 5(1)(f) Data Retention Directive.
[41] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others* [2014] ECLI:EU:C:2014:238, para 71.
[42] Ibid., paras 26-27.
[43] Ibid., para 27.
[44] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others* [2014] ECLI:EU:C:2014:238, para 28.
[45] Ibid., para 37.
[46] Ibid.
[47] Ibid., para 69.
[48] Ibid., paras 56-57.
[49] Ibid., paras 59-61.
[50] Ibid., paras 63-64.
[51] Ibid., paras 66-68.
[52] *Szabó and Vissy v. Hongary* App no 37138/14 (ECtHR, 12 January 2016); *Zakharov v. Russia*. 47143/06 (ECtHR, 4 December 2015).
[53] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others* [2014] ECLI:EU:C:2014:238, para 41.

including communication services provided over the internet, such as Skype. Another notable difference of the Russian surveillance system with the European regimes that were based on the Directive is the fact that in Russia not only metadata but also the content of communications is being stored in an indiscriminate manner and subsequently monitored, which is an uncommon practice in Europe. The authorities of the Russian Federation that get access to all communications of internet users can collect significant amounts of information regarding their private life. It is not required to indicate a link between the retained data and the threats posed to national security. Metadata is stored for a period of 12 months while the content is held for a period of up to 6 months: both types of data must be retained on the territory of the Russian Federation. The law does introduce measures for achieving an appropriate level of security of communication data held by the respective entities and there is no clearly outlined obligation to delete this information after the retention period.

The considerations made above lead to the conclusion that the Russian legal framework is clearly not in line with the Directive that was declared to be invalid and would certainly not be compatible with the EU legal regime. Under the CoE's human rights framework, this would also be seen as an interference that is incompatible with the conventional human rights standards.

At the same time, low efficacy and feasibility of the legislation have been demonstrated by the mostly failed efforts of Roskomnadzor to enforce the 'Yarovaya' Law. This scenario played out in the case of the 'Telegram Messenger LLP' company, which rejected implementation of the 'Yarovaya' law (10.1 No. 149-F3 with amendments according to No. 374-F3).[54] Namely, Telegram rejected the requirement of the FSB to transfer keys to decrypt users' messages, because the company considers it its duty to keep users' correspondence[55] secret. As a result, based on Article 15.4 of the Federal Law 'On Information, Information Technologies and Information Protection', on 6 April 2018 Roskomnadzor filed a lawsuit demanding that access to the information resources of Telegram Messenger LLP be limited (i.e. blocked) in Russia. However, for technical reasons the regulator's efforts[56] to block Telegram have succeeded only partially,[57] while causing significant collateral damage. Instead of preventing the operation of Telegram, the Russian authorities blocked users' access to unrelated online services. At the same time, *de facto*, Telegram continues to carry out its activities on the territory of the Russian Federation.[58]

Eventually, in June 2020, the Roskomnadzor announced that it would lift the ban on Telegram's operations in Russia. This is to greater extent due to the Roskomnadzor's failure to block Telegram in Russia.[59] Pavel Durov, the founder of the Telegram mentioned that:

> 'In April 2018, Russia's telecom regulator Roskomnadzor blocked Telegram on the country's territory. We knew it was coming, so by the time the block went live, we had already upgraded the Telegram apps with support for rotating proxy servers, ways to hide traffic and other anti-censorship tools. We were joined by thousands of Russian engineers that set up their own proxies for Telegram users, forming a decentralised movement called Digital Resistance. As a result, Telegram's user base in Russia hasn't decreased – in fact, it has doubled since 2018. In May 2020, out of 400 million monthly active users of Telegram, at least 30 million were from Russia. It means that our growth in Russia has been in line with our growth in other countries. To put it simply, the ban didn't work… we have decided to direct our anti-censorship resources into other places where Telegram is still banned by governments – places like Iran and China.'[60]

Furthermore, the Russian authorities also demonstrate inability to enforce the national laws as applicable to the major Western companies such as Google,[61] Facebook or Twitter[62] (for example) that are required to fulfill the 'Yarovaya' law's requirements regarding the databases localization in Russia. This entails the localization of personal data of Russian users on the territory of the Russian Federation. Russian courts issued a number of resolutions against such companies as mentioned above according to the 'Yarovaya' law, while the companies were fined for being non-compliant with the Russian legal instruments. Up until now, the companies have failed to comply with the rules imposed on them in Russia.

It is obvious that the Russian authorities demonstrate an uncompromising will to establish control over information flows in the Russian section of the internet, despite significant economic and reputational costs and technological

[54] 'A Few Steps from Blocking: Roskomnadzor Filed a Lawsuit against Telegram' (in Russian) (*RBC*, 6 April 2018) <https://www.rbc.ru/technology_and_media/06/04/2018/5ac726039a794701e9f0c01c> accessed 27 August 2020.

[55] 'Roskomnadzor Gave Telegram 15 Days to Transfer Encryption Keys to the FSB' (in Russian) (*RBC*, 20 March 2018) <https://www.rbc.ru/rbcfreenews/5ab0e3b99a79477cf2540d32> accessed 27 August 2020.

[56] Nikita Batalov, 'Opposite Effect: Why Has the Blocking of Telegram Failed?' (in Russian) (*Deutsche Welle*, 21 July 2018) <https://p.dw.com/p/31qEi> accessed 26 August 2020.

[57] 'The Blocking Has Failed: Why Telegram Still Works' (in Russian) (*Gazeta.ru*, 15 May 2018) <https://www.gazeta.ru/tech/2018/05/15/11751535/telega.shtml> accessed 26 August 2020.

[58] Matt Burgess, 'This is Why Russia's Attempts to Block Telegram Have Failed' (*Wired*, 28 April 2018) <https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google> accessed 26 August 2020.

[59] 'Russia lifts ban on Telegram messaging app after failing to block it' (*Reuters*, 18 June 2020) <https://www.reuters.com/article/us-russia-telegram-ban/russia-lifts-ban-on-telegram-messaging-app-after-failing-to-block-it-idUSKBN23P2FT> accessed 2 August 2020.

[60] Pavel Durov, 'Durov's Channel' (*Telegram*, 22 June 2020) <https://t.me/durov/117> accessed 26 August 2020.

[61] 'Company Google Received a Fine Worth 700.000 Rubles for Non-compliance with the Russian Law' (in Russian) (*Roskomnadzor*, 18 July 2019) <https://rkn.gov.ru/news/rsoc/news68466.htm> accessed 26 August 2020.

[62] Mark Bennetts, 'Facebook and Twitter Could Be Blocked in Russia in Data Storage Row' (*The Guardian*, 17 April 2019) <https://www.theguardian.com/world/2019/apr/17/facebook-and-twitter-face-russian-sanctions-in-data-storage-row> accessed 26 August 2020.

problems of implementing the new legislation.[63] According to various assessments and estimates, such as those concerning equipment and operational costs, even implementation of the 'Yarovaya' law by the distributors of information may cost 2–10 trillion rubles[64] in the coming years (27–135 billion US dollars according to the exchange rate of August 2020).

Moreover, the said legislation creates the possibility for the Russian special services to have almost unrestricted access to a significant portion of private and commercial information which circulates in the Russian segment of cyberspace. Considering the opacity[65] and corruption[66] of the Russian governmental structures,[67] including the security services,[68] many of those who operate in Russian cyberspace should worry about how the collected information will be used. Another issue is the safety of the collected and stored information. Will telecom and internet companies be able to provide the necessary level of data security and prevent the theft of valuable information by hackers or other malicious actors?

For example, in the end of the 2018, for a small sum of money a journalist bought[69] from a Russian official information from a classified Russian database regarding the real identities of the two Russian GRU officers who poisoned the Skripals in Salisbury UK.[70] Thus, it can be assumed that if the Russian authorities are unable to keep secretly information about their intelligence officers, the mentioned kind of collected information is also not stored securely and can in theory be obtained by others.

Acting according to the Russian laws, all entities that can be qualified as 'distributors of information' will fail to meet the requirements for data retention practices clarified by the CJEU and the ECtHR. As stated above, the amended law is not up to the quality standard that a legal measure constituting an interference with the right to privacy ex Article 8 ECHR is supposed to satisfy. This standard cannot be met without adequate safeguards and guarantees against possible abuse of the powers of the authorities that access communications of Russian users. The law in question does not constitute a necessary measure that must be taken in a democratic society in order to achieve the legitimate aims of protecting the interests of national security and, in contrast to the EU, in Russia the balance between the protection of human rights and national security interests seems to be shifted to the latter.[71]

4.3. *EU and General Data Protection Regulation*

In the modern globalized world, corporations offer services over the world wide web reaching their customers located far beyond the national territorial boundaries. Many of such companies have an establishment in the EU and have to comply – among other things – with the requirements set by the General Data Protection Regulation. If these companies acting as data controllers and determining the purposes and means of the processing of personal data or operating as data processors and handling personal data on behalf of controllers deal with personal information relating to Russian users, they will have to act in accordance with the Russian amended law No. 149-F3. Essentially, they would be obliged to establish databases containing personal data of Russian nationals on the territory of the Russian Federation and disregard their GDPR obligations in relation to Russian and EU users, for instance, those relating to the exercise of certain data subjects' rights, such as the right to be forgotten.[72]

The wording of the new legislative act implies the inability of data controllers to comply with their data protection obligations under the GDPR. How can EU data subjects, for instance, make use of the essential right to be forgotten if the companies are obliged to store their personal data in Russia and are not allowed to delete it? This would become a problematic issue that needs to be dealt with. Similarly, Russian companies, which are involved in the processing of personal data of persons located in the EU, will have to use double standards for the two groups of users: individuals from the EU and Russia. Instead of following the practice of safeguarding human rights and fundamental freedoms promoted by the EU, such corporations established in Russia will be obliged to grant GDPR rights to persons that are in the Union and treat Russian nationals differently in accordance with the Russian domestic legislation. Finally, the obligation of cooperating with the Russian authorities on decrypting communications of internet users may lead the introduction of backdoors in the platforms of information distributors allowing governmental agencies to access these communications. This could entail not only violation of GDPR rights of data subjects but also more generally their rights to privacy and freedom

[63] Mikhail S Zhuravlev and Tatiana A Brazhnik, 'Russian Data Retention Requirements: Obligation to Store the Content of Communications' (2018) 34(3) CLSR 496, 497

[64] 'Rostec" Calculated the Cost of Equipment for Implementing the "Yarovaya Law' (in Russian) (*Lenta.ru*, 5 September 2016) <https://lenta.ru/news/2016/09/05/rostech/> accessed 26 August 2020.

[65] 'Putin and the Proxies' (*OCCRP*, 24 October 2017) <https://www.occrp.org/en/putinandtheproxies/#infographic> accessed 26 August 2020.

[66] Transparency International, 'Corruption Perceptions Index 2017' (Survey, 21 February 2018) <https://www.transparency.org/news/feature/corruption_perceptions_index_2017> accessed 26 August 2020.

[67] 'Putin's Bodyguards Rewarded with Land and Power' (*OCCRP*, 19 November 2018) <https://www.occrp.org/en/28-ccwatch/cc-watch-indepth/8922-putin-s-bodyguards-rewarded-with-land-and-power> accessed 25 August 2020.

[68] Roman Anin, 'Palaces under Guard' (in Russian) (*Novaya Gazeta*, 19 November 2018) <https://www.novayagazeta.ru/articles/2018/11/19/78623-dvortsy-pod-ohranoy> accessed 26 August 2020; Pol Rodin, 'Corruption in the Central Apparatus of the FSB of the Russian Federation. What Was It?' (in Russian), (*Regnum*, 19 July 2017) <https://regnum.ru/news/2302756.html> accessed 26 August 2020.

[69] 'The Insider Learned the Real Name of the GRU Colonel, Acting Under the Name of Ruslan Boshirov' (in Russian) (*NEWSru.com*, 26 September 2018) <https://www.newsru.com/russia/26sep2018/boshirovchepiga.html> accessed 27 August 2020.

[70] 'Solberetsky, Part Three. "Boshirov" Turned Out to Be "the Hero of Russia", GRU Colonel Anatoly Chepiga' (in Russian) (*The Insider*, 26 September 2018) <https://theins.ru/politika/118927> accessed 27 August 2020.

[71] Mikhail S Zhuravlev and Tatiana A Brazhnik, 'Russian Data Retention Requirements: Obligation to Store the Content of Communications' (2018) 34(3) CLSR 496, 506.

[72] See Article 17 GDPR.

of expression. The Russian special services will be able to access a wide spectrum of information regarding natural and legal persons, including sensitive personal data and financial information, and process it for their own purposes without having obtained consent from the persons concerned or having another legal ground for such processing. In addition, this practice could create a possibility for various third parties to exploit backdoors and other intentionally introduced vulnerabilities and get unauthorized access to stored data meaning that internet users would not be able to securely engage in communications online, as indicated by the UN Special Rapporteurs.[73] This is something Western internet users, businesses and respective governments should be aware of and consider in their data sharing practices.

Finally, one should note that there are adequacy decisions taken by the European Commission on the basis of Article 45 GDPR with regard to a number of third countries allowing personal data to be shared with those countries without any additional requirements to be met. While there are adequacy decisions for Israel, the United States of America, Japan and a few other countries, Russia cannot be found in this list.[74] After the adoption of the 'Yarovaya' law amendments, natural and legal persons established in the EU that transfer personal data to Russia should now be more careful with processing this data in such a manner. If this information falls under the scope of the new Russian legislation obliging their distributors to store, process and share it with the authorities, this will make compliance with data protection obligations of those persons and entities handling personal data impossible and probably infringe rights and freedoms of concerned data subjects.

5. Freedom of expression and other complications of the 'fake news' and 'disrespect' laws

The 'fake news' and 'disrespect' ('internet insults') amendments should be said to be rather directed at the prevention of criticism towards the Russian government than at the protection of public order and public well-being. These amendments can be used to intimidate the dissent and suppress the freedom of speech since the 'fake news' law outlaws the dissemination of what the government deems to be 'fake news' – i.e. any information undesirable by the government can potentially be deemed as such. In the same way justified and fair criticism of the authorities can be defined as an insult according to the law.

Due to their vagueness, bias of the Russian judicial system and its dependence on the executive authority, these amendments increase the risk of selective and arbitrary justice. For instance, how is one supposed to establish that disrespect towards authorities found its expression in indecent form and what is the standard for measuring this indecent form? Such vague definitions used in the law could lead to erratic and arbitrary implementation and enforcement that should ideally be prevented. This is a highly evaluative concept, which makes objective enforcement of the law quite difficult. Therefore, these laws help cultivating some kind of self-censorship among the citizens because any article, post or picture on social media platforms or internet media can be defined as violating the law. Thus, a fear of selective and arbitrary violence reinforces a feeling of insecurity that ultimately leads people trying to avoid any expression of their opinion and consequently confrontation with the authorities.

The developments in Russia clearly contradict the principles of the Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda adopted by the United Nations Human Rights Office of the High Commissioner, OSCE and several additional organizations in Vienna on 3 March 2017.[75] Paragraph 1(a) of the General Principles reveals that States are allowed to introduce restrictions on the right to freedom of expression only in accordance with the test used for imposing such restrictions under international law. They must be introduced in a national law, seek to achieve one or more legitimate interests that may be pursued under international law and need to be necessary and proportionate in the protection of those interests. Furthermore, Paragraph 1(b) specifies that restrictions of the freedom of expression may also be used to prohibit advocacy of hatred, which constitutes incitement to violence, discrimination or hostility in line with Article 20(2) of the International Covenant on Civil and Political Rights.

Moreover, the use of the law on 'fake news' will increase pressure on those media outlets[76] that have remained independent and impartial and are trying to participate in some competition with the major pro-Kremlin mass media in the field of distribution of information. These still independent mass media outlets are mostly small ones, such as different online media and Telegram channels. Also, in this regard, the policy of the Russian government contradicts the principles of the Joint Declaration, more specifically its Paragraphs 3(a) and 3(b). These stress that States are under a positive obligation to ensure promotion of 'a free, independent and diverse communications environment, including media diversity' and are required to create 'a clear regulatory framework for broadcasters which is overseen by a body which is protected against political and commercial interference or pressure and which promotes a free, independent and diverse broadcasting

[73] OHCHR, 'Mandates of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association; and the Special Rapporteur on Freedom of Religion or Belief, Communication to the Russian Federation' (Communication, 28 July 2016), 2 <https://www.ohchr.org/Documents/Issues/Opinion/Legislation/RUS_7_2016.pdf> accessed 27 August 2020.

[74] European Commission, 'Adequacy Decisions' <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 27 August 2020.

[75] OSCE, Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda (OSCE, 3 March 2017) <https://www.osce.org/fom/302796> accessed 27 August 2020.

[76] These media outlets basically operate only in cyberspace (most of the independent TV channels were eliminated by the authorities in the 2000s).

sector'.[77] In essence, the policy of the Roskomnadzor clearly contradicts the said principles.

Eventually, the discussed legislation will inevitably lead to violations of the basic citizens' rights such as the freedom of expression and the freedom of receiving and disseminating information. Thus, 'fake news' and 'internet insults' laws complement the 'Yarovaya' law in the Russian government's efforts to prevent dissemination of unsolicited information. Overall, criticism of the authorities on the web is perceived as a great danger to the stability of the regime.

It should be observed that on the side of relatively low efficacy of the new legislation and regulation, it contains major threats to development of the Russian society and economy. As mentioned above, from the human rights perspective the amendments introducing the prohibition of the distribution of fake news and disrespect towards the authorities are also far from unproblematic. They seem to significantly limit the scope of the right to freedom of expression of Russian nationals who would be less willing to contribute to the flow of information on the internet and share their opinions on certain events or on the governmental structures. In this context, the Russian civil society and the basic human rights and fundamental freedoms, including the freedom of speech, are the primary victims of the new legislation triggering the chilling effect and posing significant threats to these human rights and freedoms.

As Article 10(1) of the ECHR provides, everyone is entitled to the right to freedom of expression forming an essential foundation of a democratic society.[78] This right includes freedom of holding opinions and receiving and imparting information and ideas without interference by public authorities. This does not mean, however, that this right cannot be restricted. The second paragraph of the same provision stipulates that possible restrictions must be prescribed by law and must be necessary in a democratic society for achieving the legitimate goals of among other things national security, public safety and protection of morals.

It is obvious that there are national laws in Russia allowing for an interference with the said human right in the form of prohibitions of fake news and internet insults. These laws seem to pursue the legitimate aims of protecting national security, territorial integrity and public safety and preventing crime and disorder. The laws in question, however, also need to meet the qualitative standards that have been outlined by the ECtHR. The norms laid down in these laws must be formulated as precisely and clearly as possible in order for the individuals falling under the scope of these norms to be able to foresee what the consequences are of certain behavior.[79] Of course, achieving the highest degree of foreseeability is impossible in practice but taking into account the content of the 'fake news' and 'disrespect' laws, the fields they are covering and the number and status of those who are addressed by them,[80] it should be argued that the national authorities are expected to attain a significantly high level of precision of this legislation. As the laws stand now, they include rather vague and undefined terms that can be used by national authorities for prosecuting those who are appealing to their freedom of expression for criticizing these authorities. There are no adequate safeguards for ensuring that the interference is justified by the public interest. Both legislative acts can be concluded to be in violation of Article 10 ECHR.

Apparently, without freedom of speech and viable and functional civil society, transformation of the Russian deeply corrupted and ineffective governmental structures, and especially modernization of the Russian economy, are impossible. Thus, in the medium and long perspective the mentioned legislation will undermine Russian economy and Russia's competitive potential in comparison with other major countries. At the same time, the process of deepening Russian socio-economic difficulties will eventually undermine the stability of the regime itself.

Through lawmaking and regulation, Moscow strives to restrict any undesired activity in Russian cyberspace while undermining the freedom of speech, privacy, data protection and the confidentiality of correspondence. Consequently, these efforts also have had a significant negative impact on Russia's business climate, and generally on investments and the potential development of entire sectors of the Russian economy. These negative consequences of the strategy chosen by the lawmakers of the Russian Federation constitute a logical result of having a certain vision on the role of State in the regulation of cyberspace and the methods of safeguarding its own interests.

6. Conclusion

In sum, Russia serves as an intriguing case where an authoritarian regime's efforts to preserve its stability lead to damage to its reputation inside and outside the State, significant direct and indirect economic damage, as well as uncontrolled access by the security services to sensitive private and commercial information with wide opportunities for misuse.[81]

Clearly, the new Russian laws on data retention are not compatible with the EU and ECHR standards and may lead to violations of essential human rights, including the rights to privacy and data protection. They place Russian nationals under constant surveillance by the authorities who are in a position to access the content of their online communications and associated metadata that are stored by distributors of information on the internet. Such practices can result in various data security threats, for instance, when several third parties would be able to access the stored personal data and use it for a variety of malicious purposes. Also, there is a possibility of abuse by the authorities that are in a position

[77] OSCE, Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda (OSCE, 3 March 2017) <https://www.osce.org/fom/302796> accessed 27 August 2020.

[78] *Big Brother Watch and Others v. the United Kingdom* App no 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018), para 487.

[79] *Centro Europa 7 S.R.L. and Di Stefano v. Italy* App no 38433/09 (ECtHR, 7 June 2012), para 141.

[80] Ibid., para 142.

[81] Vladimir Kara-Murza, 'What's Really Behind Putin's Obsession with the Magnitsky Act' (*The Washington Post*, 20 July 2018) <https://wapo.st/2uM9CDO> accessed 28 August 2020.

to obtain massive amounts of information on internet users. In addition, the amendments concerning fake news and disrespect towards the authorities sacrifice the freedom of expression of individuals and affect their freedom of receiving and disseminating information. This is undoubtedly an alarming development that will endanger the protection of crucial human rights and fundamental freedoms in Russia.

Some might be inclined to argue that other countries can choose to follow the Russian approach in the future.[82] If these prediction materialize, this will most probably create an even bigger gap between such counties – together with Russia – and the West, where the adopted policy generally speaking favors a delicate balance between the protection of these rights and freedoms and the national security interests. The Russian authorities seem to be willing to sacrifice human rights and fundamental freedoms to stimulate the creation of such a gap by isolating Russia from the rest of the world in the digital domain. On 1 May 2019, Russian President had signed the 'Law on Sovereign Internet' that entered into force on 1 November 2019.[83] This law creates a possibility for disconnecting the Russian segment of the internet from the world wide web and filtering the traffic of this segment. The adoption of this piece of legislation is a matter of great concern given that one of the notable victims of such a program based on the principles of 'authoritarianism and [S]tate control'[84] will be the right to freedom of expression protected by international and national legal instruments.

Moreover, the efficacy of the described legislation and the measures aimed at total control and preservation of the regime's stability are highly questionable. Such measures may achieve some of the State's short-term goals but will presumably in the long run cause damage to State development and its relations with the rest of the international community, thereby upsetting the stability of the said regime.

Acceptance of the addressed Russian regulatory amendments by the collective 'West' and transnational IT companies will provide a degree of legitimacy to the Russia's efforts to undermine basic human rights and freedoms in cybersphere and encourage other non-democratic and semi-democratic governments[85] to continue their assaults on democracy and its core values. At the same time, it will also undermine the foundation of liberal-democratic values and norms and their further development on a global level and potentially in the Western societies.

Moreover, the Western and particularly European response to the introduced Russian laws should take into account not only necessity to protect the basic human rights according to the ECHR principles and rule of law, but also the fact that the new Russian legislation and especially potential compliance of the transnational IT companies with it give Russia a certain degree of obvious superiority over the open democratic Western societies in the field of information warfare. Consequently, this could potentially undermine the stability of Western democracies. Thus, the abovementioned Russian legislative framework violates not only the ECHR principles and the GDPR, but also contains security threats to the collective West. It is not a secret that the Russian leadership defines cyberspace as one of the major fields of asymmetric military conflict with the West.[86] By doing so, it seeks to compensate for its conventional and economic inferiority in comparison to the collective West. Consequently, it is essential to oppose the examined Russian legislation not only from the legal and human rights perspective, but also from the national security standpoint of the Western countries.

At the same time, the fact remains that the Western countries are unable to directly force the current Russian government to cardinally change its legislative framework in the field of privacy, data protection and freedom of expression in accordance with the ECHR standards and requirements. The EU may try, however, to encourage European transnational IT companies working in Russia to operate according to the GDPR standards and the principles defined in the ECHR. This could entail sanctions against IT companies which adhere to the respective Russian laws (for example, the 'Yarovaya' law) explicitly contradicting the GDPR and ECHR rules and norms. Thus, IT companies could be required to choose between, for instance, the Western market and the Russian market, which is a dozen times smaller than the Western one. Consequently, the Russian authorities would be forced to adjust and recalibrate Russian data protection legislation (at least with respect to the Western IT companies) in such a way that this legislation will be made compliant with the European standards.

When it comes to the amendments addressed in this contribution, it is to be observed that there is a need to substantially improve their quality aspect by clearly defining the scope of their application and the terms used. Instead of prohibiting all forms of expression that could be qualified as 'fake news', more attention should be paid to precisely defining the incorporated notions in addition to creating and enforcing data protection rules that deal with the processing of special categories of personal data, regulate profiling and automated decision-making and ensure the basic principles of the processing, as noted by the European Data Protection

[82] Oreste Pollicino and Oleg Soldatov, 'Striking the Balance Between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context' (2018) 19(1) GLJ 85.

[83] Yulia Krivoshapko, 'RU – and Full Stop: The Law about Runet Enters Into Force' (in Russian) (*RG.ru*, 31 October 2019) <https://rg.ru/2019/10/31/zakon-o-suverennom-runete-vstupaet-v-silu.html> accessed 27 August 2020; 'Russia's Sovereign Internet Law Comes Into Force' (*The Moscow Times*, 1 November 2019) <https://www.themoscowtimes.com/2019/11/01/russias-sovereign-internet-law-comes-into-force-a68002> accessed 28 August 2020.

[84] 'The Authoritarian Assault on Internet Freedom is on the Move in Russia and India' (*The Washington Post*, 20 February 2019) <https://wapo.st/2T23aHd> accessed 28 August 2020.

[85] In this regard, the recent legal amendments accepted in Turkey can be mentioned. They resemble the Russian 'Yarovaya' law and prescribe IT companies to open offices in Turkey and store metadata and the content of communications on the territory of Turkey; 'Turkey Passes Law Extending Sweeping Powers Over Social Media' (*The New York Times*, 29 July 2020) <https://www.nytimes.com/2020/07/29/world/europe/turkey-social-media-control.html> accessed 28 August 2020.

[86] Ofer Fridman, 'The Russian Perspective on Information Warfare: Conceptual Roots and Politicization in Russian Academic, Political, and Public Discourse' 2017(2) Defence Strategic Communications: The official journal of the NATO Strategic Communication Centre of Excellence 61-86.

Supervisor.[87] Furthermore, it is a crucial task for the regulators in such fields as data protection and consumer protection to cooperate, to establish the scope of the problem posed by fake news and to understand the involved practices.[88] Of course, one should not forget about the importance of self-regulation for addressing this problem and the right of individuals to an effective remedy that they should be able to exercise.[89]

A softened and streamlined Russian approach regarding data protection could be based on a set of clear and objective criteria for access of national authorities to the collected big data; more explicit distinction between different categories of data; a well-defined connection between the retained data and the threats posed to the national security; and a clear obligation to delete retained data after a certain period of time. Moreover, the 'Yarovaya' law could be reshaped and modified so that only metadata will be stored in the territory of the Russian Federation and will remain in the possession of the corresponding IT companies. At the same time, this information could be delivered to the Russian authorities only following the availability of sufficient evidence acquired by the appropriate and competent Russian authorities that the requested information is necessary for prevention/investigation of terrorist and criminal activities, and is not only associated with political activities or business interests. Additionally, requests to deliver to the federal executive authority in the field of national security information necessary for decoding received, transmitted, delivered and/or processed electronic messages should be abolished. A requirement of the installation of SORM system connected to the Russian branches of Western IT companies should be unequivocally rejected. At the same time, the recent example of the Telegram Messenger LLP demonstrates that the adamant position of an IT company rejecting the 'Yarovaya' law may cause the Russian government to retreat from applying this law in practice. It remains, however, unclear whether the European authorities will be willing and able to implement the discussed measures against IT companies, which comply with the 'Yarovaya' law and in this way undermine the ECHR principles, freedom of expression, privacy, data protection and security interests of their consumers in the Western countries.

In sum, the Russian example again raises the question of where the borderline between necessary and excessive control over cyberspace by State authorities should be drawn, in order to be able to ensure the unobstructed development of economic and civil society and the essential in this day and age protection of human rights and fundamental freedoms. Only time will tell whether and how these challenges will be addressed and one can only hope that a fair balance would be struck between the often conflicting but undeniably crucial interests at stake.

Data Availability

No data was used for the research described in the article.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work was supported by the Center for Cyber Law & Policy (CCLP) at the University of Haifa in conjunction with the Israel National Cyber Directorate in the Prime Minister's Office. It has been written as part of research conducted by the authors who would like to thank anonymous reviewers for their assessment and insightful comments. The views provided in the article are entirely those of the authors and shall not be associated with TLS, CCLP, the Israel National Cyber Directorate or any other entity or person. The authors and the above-mentioned entities or persons cannot be held responsible for any use of the information included in this article.

Author information

Dr. E. Moyakine is an Assistant Professor at the Transboundary Legal Studies (TLS) Department of the Faculty of Law of the University of Groningen, the Netherlands, and a Research Fellow at the Center for Cyber Law & Policy of the University of Haifa, Israel.

Dr. A. Tabachnik is a Postdoctoral Researcher at the School of Political Sciences of the Faculty of Social Sciences of the University of Haifa, Israel, and a Research Fellow at the Center for Cyber Law & Policy of the same university.

[87] European Data Protection Supervisor, *EDPS Opinion on Online Manipulation and Personal Data*, Opinion 3/2018 (19 March 2018), 18, <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf> accessed 30 August 2020.

[88] Ibid., 18-20.

[89] Ibid., 20-22.