Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context

By Oreste Pollicino[*] & Oleg Soldatov[**]

Abstract

In pursuit of solutions to curb cybercrime, legislators engage in an analysis proportionally weighing freedom of expression and other societal interests. The balance between the two concepts differs dramatically across different jurisdictions. This Article looks into a widely discussed legislative package regulating the online domain, enacted by the Sixth Convocation of the Russian Parliament (2011–2016)—the State Duma. The authors operate under the assumption that the Russian approach might have a broad spillover effect. With this in mind, the authors outline the current status quo regarding Internet regulations in the EU, disentangle and contextualize the legislation under scrutiny, emphasize Russian influence over Eastern European countries, and describe the tumultuous relationship between the Russian Federation and the European Court of Human Rights.

[*] Full Professor of Constitutional Law, Bocconi University, Milan

[**] Ph.D. candidate in Legal Studies, Bocconi University, Milan.

A. Introduction

The regulation of digital communications occurs between two extremes. At one end are proponents of making the Internet "a world where one could talk and do business without worrying about state intervention,"[1] and at the other are those who favor complete regulation of the online domain in a manner similar to, or even stricter than, the case of the traditional media; those in favor of regulation call for licensing, supervision of content production, and complete user de-anonymization.[2] After the first years of Internet development,[3] the weaknesses of the most radical[4] arguments for the presumed anarchic nature of the Internet have been exposed. Consequently, the larger issue is no longer whether it is possible to regulate the Net; rather, the issue is how to do it.[5]

In 1998, Professor Goldsmith concluded that both cyberspace and ordinary transactions involve people in real space transacting with other people in real space, which sometimes results in real world harm.[6] In pursuit of solutions to curb cybercrime, the legislative approach usually engages in a proportionality analysis between the right "to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers"[7] and other societal interests.[8] The balance struck differs dramatically across different jurisdictions.[9] Europe presents a perfect illustration of how varied Internet regulation can be within a certain geographic space, given the differences

---

[1] Henry Farrell, *Why the Hidden Internet Can't be a Libertarian Paradise*, AEON (Feb. 20, 2015), aeon.co/essays/why-the-hidden-internet-can-t-be-a-libertarian-paradise.

[2] *See* Internet Development Institute, 'Predlozhenija po formirovaniju dolgosrochnoj programmy razvitija rossijskoj chasti informacionno-kommunikacionnoj seti "Internet" i svjazannyh s nej otraslej jekonomiki' [*Suggestions on formulating the long-term development programme of the Russian Internet sector and related branches of economy*], (Draft Paper) (Sept. 29, 2015).

[3] The Internet entered the commercial phase in 1984–89, and expanded into global networks during the 1990s when business and personal computers with different operating systems joined the universal network. *See* R. Cohen-Almagor, *Internet History*, 2 INT'L J. TECHNOETHICS 45, 45–47 (2011).

[4] *See* J. P. Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUNDATION (Feb. 8, 1996), www.eff.org/cyberspace-independence.

[5] *See* Oreste Pollicino & Marco Bassini, *The Law of the Internet Between Globalization and Localization*, *in* TRANSNATIONAL LAW–RETHINKING LAW AND LEGAL THINKING 346, 348 (M. Maduro & K. Tuori eds., 2014).

[6] *See* J. L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1200 (1998).

[7] *See* European Convention on Human Rights, art. 10, Sept. 3, 1953 (defining freedom of expression).

[8] *See* Ahmet Yildirim v. Turkey, App. No. 3111/10, para. 8–9 (Dec. 18, 2012), http://hudoc.echr.coe.int/.

[9] Erik Bleich, *Freedom of Expression versus Racist Hate Speech: Explaining Differences Between High Court Regulations in the USA and Europe*, 39 J. ETHNIC & MIGRATION STUD. 283, 283 (2013).

between approaches prevailing in the EU and practices of the recent and widely discussed Russian legislative package regulating the online domain, enacted by the Sixth Convocation of the Russian Parliament (2011–2016)—the State Duma.

In this Article, the authors operate on the assumption that the Russian approach to over-regulating Internet might set a precedent for other European jurisdictions and have a broad spillover effect. This is attributed to the growing global insecurity responding to threats of terrorism,[10] and the consequential heterogeneous and sometimes disproportionate national legal responses when such a threat is presented by a "world of bits."[11]

To set the stage, this Article first describes the current status quo regarding Internet regulations in the EU, and, when appropriate, briefly highlights US practice. By its nature, this introductory part is not an all-encompassing guide to the EU and US Internet regimes. Rather, it is simply an illustrative description of the status quo, highlighting only those areas of regulation that were approached differently by Russian legislators.

In the second part of this Article, the authors present arguments supporting their assumption about the spillover effect of the Russian approach. They explore the peculiarities of the post-Soviet approach toward the freedom of speech concepts, which are well established in international law. They also discuss Russian influence over Eastern European countries and draw parallels between Russia and other European states, where terrorism has a religious and an ethnic background, and where authorities constantly seek ways to mitigate the threat of violence. The last argument in this section deals with the cross-fertilization of law in the field of technology.

The authors then move on to analyze the Russian legislative package regulating the Internet, and to present the main criticisms on its most controversial provisions.

Before reaching its conclusion, the Article describes the tumultuous relationship between the Russian Federation and the European Court of Human Rights. This includes a reference—from a state sovereignty viewpoint—to the recently enacted Federal law aimed at elevating the status of the Russian constitutional legislation above the status of opinions expressed by the Court—an act that may set a dangerous precedent.

---

[10] *See* Ulrich Beck, *The Terrorist Threat*, 19 THEORY CULTURE & SOC'Y 39, 53–54 (2009).

[11] *See generally* NICHOLAS NEGROPONTE, BEING DIGITAL (1995).

B. The Status Quo: The Legal Scenario in the European and Comparative Contexts

Although the Internet in Europe was virtually unregulated at first, the growing list of illegal activities online has given rise to mechanisms to identify liable parties with a view to holding them criminally or otherwise accountable for their actions.[12] This is nothing new under the sun, and that the current regulation of the online domain does not present any unsolvable problems to legislators across the world. Presently, in the European context, state authorities and private companies tend to respond to cybercrime using a combination of soft law and hard law instruments.[13]

Hard law instruments include EU-level legislation—applicable solely in the 28 EU member states—as well as the European Convention of Human Rights—applicable throughout the 47 Council of Europe member states. The provisions of the latter concerning freedom of expression on the Internet have been interpreted by the European Court of Human Rights—a transnational judicial body that hears applications alleging that one or more of the Council of Europe member states has breached one or more of the human rights provisions set out in the Convention and its protocols. Both EU-wide and Council-wide hard law instruments recognize the rights to privacy of communications and to freedom of expression.

These instruments can be divided into two categories: the legal obligation of Internet Service Providers (ISPs) to report and/or block certain categories of content; and criminalizing certain activities on the part of Internet users. Additionally, the EU, with a few exceptions, has not implemented content regulation, and member states are therefore free to determine their own policies, provided that they conform to Article 10 of the European Convention on Human Rights.[14] Generally speaking, the grounds for blocking online content and, in certain cases, holding its disseminators liable, include protection of national security, territorial integrity or public safety, prevention of disorder or crime, protection of health or morals, protection of the reputation or rights of others, and prevention of the disclosure of

[12] *See* Jack M. Balkin, *The Future of Free Expression in a Digital Age,* 36 PEPP. L. REV. 427, 434–35 (2009).

[13] The primary legal instruments regulating the online domain on the territory of Europe include the Council of Europe legal instruments (including but not limited to the 2001 Convention on Cybercrime with its Additional Protocol; and the 2007 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse), the European Union instruments (including, but not limited to Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market; and Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data), as well as national legislation.

[14] For a more elaborate presentation, see Oreste Pollicino & Marco Bassini, *Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis*, *in* RESEARCH HANDBOOK ON EU INTERNET LAW 508, 541 (A. Savin & J. Trzaskowski eds., 2014).

information received in confidence.[15] In older European democracies, it is only possible to block and take down illegal content on the Internet upon the issuance of case-by-case injunctions by courts, and, in fewer cases, decisions of other State authorities.[16]

In turn, soft law also includes EU initiatives such as the 2016 Code of Conduct on illegal online hate speech that was developed in cooperation with the European Commission,[17] the Council of Europe-wide tools such as the Guide to the human rights of Internet users,[18] and the codes of conduct and terms of service of ISPs and other intermediaries.[19]

On the soft law level, the human rights of Internet users recognized by the Council of Europe[20] include: The right of non-discriminatory access to the Internet; the right to seek, receive, and impart information and ideas of one's choice without interference and regardless of frontiers; the right to assemble peacefully and to associate with others using the Internet; and the right to private and family life on the Internet, which includes the protection of personal data and respect for the confidentiality of correspondence and communications.

It should be reiterated that, at times, some of the rights recognized in hard and soft law, as is the case with other human rights,[21] may be temporarily or permanently restricted to prevent cybercriminal activities. The taxonomy of e-crime is varied and the most important categories of criminal activities online can be summed up as follows: (a) crimes where the computer, network, or electronic device is the target of criminal activity, for example, disrupting computer services; (b) content violation offences, for example, unauthorized possession of military secrets, intellectual property offences; (c) online fraud; and (d)

---

[15] *See* Council of Europe, *Filtering, Blocking and Take-Down of Illegal Content on the Internet* (Dec. 20, 2015), www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet.

[16] *Id.*

[17] *See* European Commission, *European Commission and IT Companies announce Code of Conduct on illegal online hate speech* (May 31, 2016), www.europa.eu/rapid/press-release_IP-16-1937_en.htm.

[18] *See* Council of Europe, *Internet Users' Rights* (April 16, 2014), www.coe.int/en/web/internet-users-rights/home.

[19] *See* DAMIAN TAMBINI, DANILO LEONARDI, & CHRIS MARDSEN, CODIFYING CYBERSPACE 28–49, 112–89 (2008).

[20] Council of Europe, *supra* note 18.

[21] For instance, the rights and freedoms guaranteed by Articles 8 (right to respect for private and family life), 9 (freedom of thought, conscience and religion), 10 (freedom of expression) and 11 (freedom of assembly and association) of the European Convention on Human Rights are qualified, and each Article contains a limitation clause. No restrictions on these rights are permitted other than those expressly listed, and such restrictions must have a legitimate aim.

improper use of telecommunications, such as cyberstalking, spamming, and conspiracy to undertake harmful or criminal activity.[22]

State security concerns stemming from a terrorist[23] threat seem to be prominent on the national and international agendas these days, and are a reason *de jure* for many governments to set limitations on online expression. In the recent words of Věra Jourová, EU Commissioner for Justice, Consumers, and Gender Equality, "the recent terror attacks have reminded us of the urgent need to address illegal online hate speech. Social media is unfortunately one of the tools that terrorist groups use to radicalise young people."[24]

Exploring the question of terrorism-related speech online, the dichotomy of "positive" and "negative" measures of curbing illegal behavior in the digital world may be introduced. "Positive" measures refer to those online initiatives that seek to make an impact through digital engagement and education and the provision of counter-narratives, while "negative" measures describe "those approaches that advocate for, or result in, the deletion or restriction of violent extremist online content and/or the legal sanctioning of its online purveyors or users."[25]

In presenting specific spheres of regulation, the authors will draw parallels with the following areas of legislative activity in Russia: modalities for removal of content; data nationalism; online anonymity; and data retention policies. This structure broadly follows the introduction timeline for the Russian anti-terrorist legislation recounted below.

First, on the EU-wide level, Directive 2000/31/EC includes a mild incentive for ISPs to take down illegal material voluntarily. This Directive stated that ISPs can have limited liability only when they do not have actual knowledge of illegal activity or information. And the damages will be limited, if they are not aware of the facts or circumstances based on which the illegal activity or information is apparent. At the same time, ISPs are not under a general obligation to monitor the information that they transmit or store, nor are they under a general obligation to actively seek facts or circumstances indicating illegal activity.

---

[22] *See* David Simms & Solange Ghernaouti, *Report on Taxonomy and Evaluation of Existing Inventories*, EUROPEAN UNION E-CRIME PROJECT (Nov. 30, 2014), www.ecrime-project.eu/wp-content/uploads/2015/02/E-Crime-Deliverable-2-1-20141128_FINAL.pdf.

[23] For the purposes of this article, this concept is defined as "the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious or social goal through fear, coercion or intimidation." Gary LaFree & Laura Dugan, *Introducing the Global Terrorism Database*, 19 TERRORISM & POL. VIOLENCE 181, 184 (2007).

[24] European Commission, *supra* note 17.

[25] Clive Walker & Maura Conway, *Online Terrorism and Online Laws*, 8 DYNAMICS ASYMMETRIC CONFLICT 156, 156 (2015).

Most commonly,[26] a court order is necessary for unconditional blocking, although, as the UK example below demonstrates, self-regulation arrangements might also be a viable solution. In the UK, the material encouraging terrorism can generally be placed on "blacklists" without court orders. According to a study commissioned by the Council of Europe,[27] in the UK, the watchdogs in charge of deciding which content to take down include various governmental agencies in charge of internet-related offenses. For instance, the Counter Terrorism Internet Referral Unit, acting in accordance with the Terrorism Act 2006 compiles the blacklist of URLs for material hosted outside of the UK that would give rise to criminal liability. The Police Intellectual Property Crime Unit are responsible for decisions to remove content or report these internet-related offenses. The former

Regardless of the hosting location, since 2013, the removal of unlawful terrorist content has been achieved through informal contact between the police and ISPs, and it has never been necessary to use formal powers under the Terrorism Act 2006. It is further noted that in the UK there are only two areas in which require statutory notice and removal procedures for scrubbing of illegal internet content: The first, in relation to material that constitutes offences under the Terrorism Act 2006, and the second, under the Defamation Act 2013.

Overseas, U.S. authorities are very reluctant to block illegal content on the Internet, given the strong protections afforded to freedom of speech under the First of the U.S. Constitution.[28] In the absence of legal regulation to remove offensive material, authorities rely on the cooperation of online platforms, whose abuse policies allow the removal of accounts flagged for promoting terrorism.[29] The 1996 Communications Decency Act and the 1998 Child Online Protection Act, which were the legislature's attempts to counter the spread of indecent information online,—were struck down by U.S. courts.[30]

---

[26] *See* Nigel Cory, *The Worst Innovation Mercantilist Policies of 2016*, INFORMATION TECH. & INNOVATION FOUND. (Jan. 9, 2017), www2.itif.org/2017-worst-innovation-mercantilist-policies.pdf; *see also* Council of Europe *supra* note 18, n. 15.

[27] Council of Europe, *supra*, note 15.

[28] *See* United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* 95–96 (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

[29] *See* Peter Neumann, *Countering Online Radicalization in America*, BIPARTISAN POLICY CENTER (Dec. 6, 2012), www.bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20_Online%20Radicalization%20Report.pdf.

[30] Oreste Pollicino & Marco Bassini, *supra* note 14, at 517–20.

Second, a growing number of policymakers in Europe seem to subscribe to the "data nationalists'" views: The belief that data are more secure when stored within a country's borders,[31] which leads to the emergence of various countries' policies that would require a certain body of the data to be stored domestically. Driven by concerns over privacy, security, surveillance, and law enforcement, some governments are erecting borders in cyberspace. Although the first generation of Internet border controls sought to keep information out of a country—for example, copyright-infringing material—the new generation of controls seeks to keep all data about individuals within a country, citing foreign surveillance as an argument.[32] Similar to the real-world border controls, data nationalist policies can be seen from two perspectives: Restrictive, where a country seeks to use data nationalism to subject stored data to overly restrictive legislation, and protective, where a country uses data nationalism to protect unsuspecting users from having their data stored in countries with either very lax or very intrusive policies. Some researchers argue that just as economic nationalism inevitably leads to lower productivity for firms and higher costs for consumers, data nationalism will similarly lead to poor economic outcomes. [33]

When it comes to the EU, there are virtually no borders between individual EU member states regarding the cross-border data flow. Nevertheless, General Data Protection Regulation 2016/679 will enter into force on May 25, 2018, and will allow companies to transfer data outside the European Union, only if appropriate safeguards are in place to ensure a level of protection for the rights of data subjects equal to that envisaged by the General Data Protection Regulation. Many countries, such as Germany and France, are at the center of efforts to force companies to store data only in the European Union or even in-country, such as through a "Bundescloud" (a cloud for government data) in Germany, where on July 1, 2017 a law requiring local data storage for telecommunications metadata will enter into force.[34]

Third, when it comes to the question of online anonymity, it is observed that in both the EU and the U.S., the anonymity of Internet users remains protected by default for those who do not wish to disclose their identity. Nevertheless, the right to privacy often must be reconciled with conflicting policy objectives, such as the fight against illegal or harmful content. The European Commission's long-held view on this issue, generally supported by the case-law of the European Court of Human Rights,[35] is that "the ability of governments and public

[31] Daniel Castro, *The False Promise of Data Nationalism*, INFO. TECH. & INNOVATION FOUND. (Dec. 9, 2013), www2.itif.org/2013-false-promise-data-nationalism.pdf.

[32] *See* Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 679 (2015).

[33] Castro, *supra* note 31.

[34] Cory, *supra* note 26.

[35] *See generally* European Court of Human Rights, *Internet: Case-law of the European Court of Human Rights* (June 16, 2015), www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.

authorities to restrict the rights of individuals and monitor potentially unlawful behavior should be no greater on the Internet than it is in the outside, off-line world."[36] The Ministerial Declaration of the Ministerial Conference in Bonn on Global Information Networks, July 6–8, 1997, declared a formula that continues to be "where the user can choose to remain anonymous off-line, that choice should also be available on-line."[37]

Meanwhile, in the recent case, *Delfi AS* v. *Estonia*, the European Court of Human Rights supported the proposition of holding online intermediaries responsible for the content published by third parties.[38] In this case, the Court decided that the civil liability imposed by the Estonian courts on *Delfi*, an Internet news portal and an applicant in the case, for defamatory comments posted by anonymous readers below one of *Delfi*'s online articles was compatible with guarantees provided by the Convention, and did not constitute a disproportionate restriction on the applicant company's right to freedom of expression. This decision is considered to push online intermediaries toward a strategy of gradual de-anonymization of online users that actively participate in online discussion. Of course, it is premature to draw conclusions from *Delfi*, as the mechanisms for such de-anonymization, for example updating terms of service of online intermediaries, as well as other repercussions of this judgment, need to be analyzed further, based on subsequent case law developments.[39]

The United States Supreme Court has ruled that the right to speak anonymously is protected by the First Amendment because anonymity is "a shield from the tyranny of the majority" that protects "unpopular individuals" from retaliation at the hands of an intolerant society.[40]

It is obvious that in response to a wider adoption of tools that make discovery of the real identity of a given user more difficult, such as data encryption, virtual private networks,[41] and onion routing,[42] more effective monitoring tools are being introduced by investigative

---

[36] European Commission, *Anonymity on the Internet* (Dec. 3, 1997), ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp6_en.pdf.

[37] European Union Ministers Bonn Declaration, July 8, 1997.

[38] *See* Delfi AS v. Estonia, App. No. 64569/09 (June 16, 2015), http://hudoc.echr.coe.int/.

[39] *See* Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, App. No. 22947/13 (Feb. 2, 2016), http://hudoc.echr.coe.int/.

[40] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

[41] A Virtual Private Network extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. *See* Melanie Pinola, *Virtual Private Network (VPN) Definition and Examples*, LIFEWIRE (Oct. 14, 2016), www.lifewire.com/what-is-a-vpn-2377977.

[42] The most well-known application of onion relaying is *Tor*, a software that protects a user by bouncing his/her communications around a distributed network of relays run by volunteers all around the world, thereby preventing

authorities. In particular, the deep packet inspection, a technology for scanning and analyzing Internet traffic and making decisions about how to handle it in real time, has emerged.[43] Some countries are choosing to enact mandatory key disclosure legislation, which requires individuals to surrender their cryptographic keys to law enforcement.[44]

Last, but not least, the post-9/11 era "can be characterized by the desire and ability of governments to develop a global mass surveillance system, largely unseen and until recently unsuspected," and "a common trend can be discerned whereby governments monitor the communications and online behavior of the vast majority of ordinary citizens."[45] Whereas the European Court of Human Rights has often extended a margin of appreciation to Member States when privacy rights have clashed with national security concerns,[46] at the EU level, the attempt to codify data retention rules in an overly wide manner was denied by the European Court of Justice. The events unfolded as follows. The 2006 EU Data Retention Directive[47] prescribed the storage of EU citizens' telecommunications metadata for a minimum of 6 months and at most 24 months, and allowed the investigative authorities access to details such as IP addresses and times of use with regard to every email, phone call, and text message sent or received, conditional upon court approval. The retention of data was used to serve the purpose of preventing, investigating, detecting, and prosecuting serious crimes, such as organized crime and terrorism. On April 8, 2014, the Court of Justice of the European Union declared the Directive invalid on the grounds that interference with the fundamental rights to respect for privacy and the protection of personal data was not limited to strictly necessary materials.[48] In December 2016, the Court further elaborated that EU law precludes national legislation that prescribes the general and indiscriminate

third parties from monitoring a user's Internet connection and learning what sites he/she visits, as well as preventing the sites from learning the user's physical location. *See Tor FAQ*, TOR PROJECT www.torproject.org/docs/faq.

[43] *See* Ebenezer Duah, *Internet Service Providers' Monitoring Obligation*, 6 MASARYK UNIV. J.L. & TECH. 207, 208 (2012).

[44] *See* Regulation of Investigatory Powers Act 2000 (Eng.), and subsequent amendments.

[45] Arianna Vedaschi & Valerio Lubello, *Data Retention and its Implications for the Fundamental Right to Privacy*, 20 TILBURG L. REV. 14, 15 (2015).

[46] *See* Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RTS. J. 65, 69 (2015).

[47] *See* Council Directive 2006/24/EC, 2006 O.J. (EC) (explaining the retention of data generated or processed related to the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC).

[48] *See* Judgment of the Court (Grand Chamber), 8 April 2014

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Joined Cases C‑293/12 and C‑594/12

retention of data.[49] It appears that, following these developments, the European Court of Human Rights supported the conclusion concerning the illegality of indiscriminate data collection and retention.[50] Unlike the EU Data Retention Directive, the United States does not have ISP-level mandatory data retention laws.[51]

C. Russian Legislative Approach and its Potential to Inspire other European Countries

There are several factors that can explain the peculiarities of the Russian approach toward these concepts that are well established in international law: Including the country's unique, periodically hostile relationship with Europe and the West in general, its historically established tendency toward an authoritarian government, and the relative weakness of the rule of law inside the country along with an emphasis on preserving the territorial integrity of Russia as the world's largest territorial state.[52]

There is "a distinctively Russian tradition of thought and argument about human rights" that can be traced back to the imperial and Soviet roots of the Russian Federation and to the long history of serfdom in pre-Soviet Russia.[53] The particular traits of Russian legal thought arguably have spillover effects toward countries that once shared the communist ideology with the Russian Federative Socialist Republic under the umbrella of the Soviet Union and the Eastern Bloc. Decades after the collapse of the Union, the political, cultural,[54] and religious[55] ties with a number of Central and Eastern European nations, as well as its strong position as an exporter of energy resources,[56] the Russian Federation still has significant influence over Soviet successor states currently not in the EU—namely, Azerbaijan, Armenia,

[49] *See* Case C-203/15 & Case C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of St. for the Home Dep't v. Tom Watson and Others, 2016 E.C.R.

[50] *See* Roman Zakharov v. Russia, App. No. 47143/06 (Dec. 4, 2015), http://hudoc.echr.coe.int/.

[51] *See* CHRISTINA AKRIVOPOULOU & ATHANASIOS PSYGKAS, PERSONAL DATA PRIVACY AND PROTECTION IN A SURVEILLANCE ERA 257 (2011).

[52] *See* LAURI MÄLKSOO, RUSSIAN APPROACHES TO INTERNATIONAL LAW 3 (2015).

[53] Bill Bowring, *Russia and Human Rights: Incompatible Opposites?*, 1 GÖTTINGEN J. INT'L L. 257, 262 (2012).

[54] *See* Stefan Meister & Jana Puglierin, *Perception and Exploitation: Russia's Non-Military Influence in Europe*, 10 DGAPKOMPAKT 4 (2015).

[55] *See* Daniel Washburn, *Religious Tradition and Innovation in the Post-Soviet World: A Case of Revival of Rejection*, CUMBERLAND LODGE (Feb. 2, 2007), https://www.cumberlandlodge.ac.uk/sites/default/files/public/Religious%20Tradition%20and%20Innovation%20in%20a%20Post%20Soviet%20World.pdf.

[56] *See* Ekaterina Demakova & Jakub M. Godzimirski, *Russian External Energy Strategy: Opportunities and Constraints*, *in* DYNAMICS OF ENERGY GOVERNANCE IN EUROPE AND RUSSIA 149, 150–51 (C. Kuzemko et al. eds., 2012).

Belarus, Georgia, Moldova, and Ukraine[57]—as well as those post-Eastern Bloc counties that joined the EU—in particular Bulgaria,[58] Hungary,[59] and Romania.[60] Ideologically, the Russian Federation spares no resources when it comes to promoting its geopolitical idea of "Eurasianism" with a center of gravity in Moscow.[61]

One of the hopes associated with the collapse of the Soviet Union in 1991 and the transition to a "New" Russia was the establishment of new human rights standards, including the fundamental right to freedom of expression.[62] Thus, at least on paper, the democratic aspirations of the 1993 Russian Constitution are "beyond question."[63] In this regard, Article 17 of the Constitution of the Russian Federation provides guarantees for the rights and freedoms according to the universally recognized principles and norms of international law.[64] Article 29 bans censorship and provides for universal freedom of speech, with the caveat of banning propaganda that instigates social, racial, national, or religious supremacy or hatred.[65] In accordance with Articles 23 and 24, limits on the right to privacy of correspondence shall only be allowed by a court decision, while the collection and storage

---

[57] *See generally* Joan DeBardeleben, *The Impact of EU Enlargement on the EU-Russian Relationship*, *in* A RESURGENT RUSSIA AND THE WEST: THE EUROPEAN UNION, NATO, AND BEYOND 93 (R. E. Kanet ed., 2009).

[58] *See* Dimitar Bechev, *Russia's Influence in Bulgaria*, NEW DIRECTION (May 12, 2015), www.europeanreform.org/files/ND-report-RussiasInfluenceInBulgaria-preview-lo-res_FV.pdf.

[59] *See* Daniel Hegedűs, *The Kremlin's Influence in Hungary*, 8 DGAPKOMPAKT 1 (2016).

[60] *See* Nadezda Feyt, *Russian-Romanian Relations in the 21st Century*, 11 POL. SCI. INT'L REL. 53 (2014).

[61] Vladimer Papava, *The Eurasianism of the Russian antiwesternism and the concept of Central Caucasia*, 3 IDEOLOGY & POL. 68, 69–70 (2013).

[62] Tatyana Beschastna, *Freedom of Expression in Russia as it Relates to Criticism of the Government*, 27 EMORY INT'L L. REV. 1105 (2013).

[63] Bowring, *supra* note 53, at 258.

[64] *See* KONSTITUTSIIA ROSSIISKOI FEDERATSII [KONST. RF] [CONSTITUTION] (Russ.).

[65] This article, in its entirety, states the following:

> 1. Everyone shall be guaranteed freedom of ideas and speech; 2. Propaganda or agitation instigating social, racial, national or religious hatred and strife shall not be allowed. Propaganda involving social, racial, national, religious or linguistic supremacy shall be banned; 3. No one may be forced to express his or her views and convictions or to reject them; 4. Everyone shall have the right to look freely for, receive, transmit, produce and distribute information by any legal means. The list of data comprising state secrets shall be determined by a federal law; 5. The freedom of mass communication shall be guaranteed. Censorship shall be banned.

KONSTITUTSIIA ROSSIISKOI FEDERATSII [KONST. RF] [CONSTITUTION] art. 29 (Russ.).

of information about the private life of a person shall not be allowed without his or her consent.[66] The rights guaranteed by the Articles mentioned above may be limited by Federal law only to the degree necessary for the protection of fundamental principles of the constitutional system, which include morality, health, the rights and lawful interests of other people, or for ensuring the defense of the country and the security of the State or in a state of emergency, captured in Articles 55 and 56 of the Constitution of the Russian Federation.[67]

As previously mentioned, terrorism is often cited by legislators as a reason for limiting the scope of human rights protections, and, as a result, digressing from the highest freedom of expression standards. Research in the field of political science supports the hypothesis that countries with ethnic minority groups geographically concentrated in one part of the country, and ethnic groups with kin in other countries, are more likely to experience terrorism.[68] Because of the history and ethnic composition of the North Caucasus region,[69] Russia joins the United Kingdom,[70] the Netherlands,[71] Turkey,[72] France, and Spain[73] on the long list of European states where political violence and terrorism have a religious and an ethnic basis; and where the authorities are constantly seeking ways to mitigate the threat of a terrorist attack.

Since the 1990s, the Chechen movement in the North Caucasus has shifted from being a nationalist agenda with the goal of achieving Chechnyan independence to that of embracing radical Islam.[74] After the Chechens' top commander, Dokku Umarov, proclaimed an Islamic state in the North Caucasus—the Caucasus Emirate—in October 2007, militants continued to attack Russians, developing a clear terrorist strategy and attacking civilians on the Russian

---

[66] Papava, *supra* note 61.

[67] *Id.*

[68] *See* Bryan J. Arva & James A. Piazza, *Spatial Distribution of Minority Communities and Terrorism*, 27 DEF. & PEACE ECON. 1, 3 (2016).

[69] *See generally* Monica Duffy Toft & Yuri Zhukov, *Denial and Punishment in the North Caucasus: Evaluating the Effectiveness of Coercive Counter-insurgency,* 49 J. PEACE RES. 785 (2012).

[70] *See* RICHARD ENGLISH, ARMED STRUGGLE 3–4 (1st ed., 2005).

[71] *See* Maria M. Komen, *Homegrown Muslim Extremism in the Netherlands: An Exploratory Note,* 7 J. STRATEGIC SEC. 47 (2013).

[72] *See* YONAH ALEXANDER ET AL., TURKEY: TERRORISM, CIVIL RIGHTS AND THE EUROPEAN UNION (2008).

[73] *See* Teresa Whitfield, *The Basque Conflict and ETA, United States Institute of Peace* (Dec. 2015), cic.nyu.edu/sites/default/files/whitfield_basque_conflict_eta_dec2015.pdf.

[74] *See* ANDREI SOLDATOV & IRINA BOROGAN, THE RED WEB 246 (2015).

mainland. The insurgents continued their activities even after the official end of the decade-long Second Chechen War in 2009.[75]

In response, the Sixth Convocation (2011–2016) of the Russian Parliament, the State Duma, passed a long list of laws regulating the Internet with the principal rationalization of curbing the terrorist threat. In 2013, *Federal Law No. 398-FZ* came into force, allowing state Internet watchdog Roskomnadzor[76] to block websites disseminating statements calling for riots or containing other "extremist" information with immediate effect and without any warning or court decision. In 2014, this law was joined by *Federal Law No. 97-FZ,* which required the registration of all bloggers with more than 3000 visits a day with Roskomnadzor, and by *Federal Law no. 242-FZ*, which decreed that databases containing the personal data of Russian citizens be stored on servers that are physically located on the territory of the Russian Federation. Finally, in 2016, *Federal Laws Nos. 374-FZ* and *375-FZ*, also known as Yarovaya's Laws, further increased the state's surveillance discretion in the domain of digital communications by mandating blanket data storage by ISPs, allowing investigative authorities to access such data retroactively, and by legally obliging ISPs to help the investigative authorities decipher encrypted messages sent by users.

It is difficult to determine the genuine driving force behind all these precautions. The legislative package in question can be viewed through two different lenses. The first is that the authorities in Putin's Russia are frank and sincere fighters of terrorism and extremism. The second is that the Russian Federation is becoming an increasingly authoritarian state where anti-terrorism concerns are a smoke-screen for politicians to gain legitimacy with the aim of further reducing freedom of expression in order to fortify their authoritarian political system.[77] The United Nations Special Rapporteur on freedom of expression, David Kaye, reports that efforts to counter violent extremism can be the "perfect excuse" for both democratic and authoritarian governments around the world to restrict free expression and to seek to control access to information.[78]

The last argument concerning the potential of Russian legislation in the field of online regulation to influence other European legislators include the trends of transnational

---

[75] *See* Cerwyn Moore, *Foreign Bodies: Transnational Activism, the Insurgency in the North Caucasus and Beyond*, 27 TERRORISM & POL. VIOLENCE 395, 406 (2015).

[76] Roskomnadzor is the Russian Federal Surveillance Service for Mass Media and Communications, an executive structure within the Ministry of Communications and Mass Media and the federal body responsible for supervision and surveillance of the media in Russia, including electronic media. *See* REGULATION OF ONLINE CONTENT IN THE RUSSIAN FEDERATION 6–8 (2015).

[77] *See generally* NATE ANDERSON, THE INTERNET POLICE (2013).

[78] U.N. High Commissioner for Human Rights, *Countering Violent Extremism, a "Perfect Excuse" to Restrict Free Speech and Control the Media* (May 3, 2016), www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=19916&LangID=E#sthash.yNerWwqD.dpuf.

convergence and the cross-fertilization of technology-related legislation.[79] One of the recent examples of such convergence is the migration of European judicial ideas concerning jurisdiction on the withdrawal of information after the European Court of Justice delivered its seminal Google Spain[80] judgment.[81] Another illustration of this phenomenon is the withdrawal of several non-EU countries, including Israel and Switzerland, from respective safe harbor data transfer agreements with the U.S. following[82] the invalidation of the EU-US safe harbor agreement in the *Shrems* judgment.[83]

When considering concrete examples of other Easter European states following the Russian lead on restricting access to certain web resources without judicial review, a recent Ukrainian block of certain—ironically Russian, websites—springs to mind. In 2017, this block was considered a tit-for-tat Ukrainian Presidential decision taken in the context of the "anti-terrorist" operation against pro-Russian separatists in the Eastern Ukraine.[84]

Armenia presents a second, more straightforward illustration of the spillover effects of Russian Internet censorship. Due to the fact that some Armenian Internet users receive filtered traffic from Russian ISPs, there have been reports of cases where a website blocked in Russia also became unavailable to Armenian users. [85]

---

[79] *See* Justin Hughes, *The Internet and the Persistence of Law*, 44 B.C. L. REV. 1, 37 (2003); *see also* DIANE ROWLAND & UTA KOHL, INFORMATION TECHNOLOGY LAW 3 (2012).

[80] *See* Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, 2014 E.C.R.

[81] *See* Krystyna Kowalik-Bańczyk and Oreste Pollicino, *Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information*, 17 GERMAN L.J. 315, 319, 330–37 (2016).

[82] *See* Oreste Pollicino, *Bridge Is Down, Data Truck Can't Get Through . . . A Critical View of the Schrems Judgment in the Context of European Constitutionalism*, 26 ITYIL (forthcoming 2017).

[83] *See* Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015 E.C.R.

[84] Oleg Soldatov, *Is the Ukrainian Ban on Russian Social Media Justified?,* EUROPEAN CTR. FOR PRESS & MEDIA FREEDOM (Aug. 1, 2017), www.rcmediafreedom.eu/Tools/Legal-Resources/Is-the-Ukrainian-ban-on-Russian-social-media-justified.

[85] *See* Sanja Kelly et al., *Freedom on the Net 2015*, FREEDOM HOUSE (Oct. 2015), www.freedomhouse.org/sites/default/ files/FOTN%202015%20Full%20Report.pdf.

D. The Russian Way: Departure from the Status Quo?

The first wave of legislative rulings relates to blocking and removing illegal content. Dated December 28, 2013, *Federal Law No. 398-FZ* "*On amending the Federal Law* '*On Information, Information Technologies and Protection of Information,*'" also known as Lugovoy's Law,[86] builds on earlier legislation[87] that created a blacklist of banned Russian websites. This law, effective immediately, allows the state Internet watchdog Roskomnadzor to block websites that disseminate statements calling for riots or that contain other "extremist" information, without a warning and without a court decision. The blocking measure is based simply on the order of the State Prosecutors' Service. Furthermore, blocking takes place at the ISP level, and the owner of the site is informed of the fact that his or her content has been blocked *post factum*.[88] The owner of the website can do nothing to prevent blockage, and his role is completely passive.

The absence of a judicial review mechanism means that website blocks are entirely discretionary on the part of the State Prosecutors' Service, and depend on the service's decision to classify certain content as "calling for riots or containing extremist information." The arbitrary nature of the State Prosecutor's decisions can serve to silence opposition, especially in light of the fact that the definition of "extremist" information stems from *Federal Law No. 114-FZ* '*On Combating Extremist Activity*' *dated 25 July 2002 (as amended),* which was heavily criticized by the Venice Commission for its imprecision. The Commission held that:

> The Extremism Law, on account of its broad and imprecise wording, particularly insofar as the "basic notions" defined by the Law—such as the definition of "extremism," "extremist actions," "extremist organizations" or "extremist materials"—are concerned, gives too wide discretion in its interpretation and application, thus leading to arbitrariness . . . the activities defined by the Law as extremist and enabling the authorities to issue preventive and corrective measures do not all contain an element of violence and are not all defined with sufficient precision to allow an individual to regulate his or her conduct or the activities

[86] *Roskomnadzor Warned Media About Blocking for Extremism*, LENTA (Jan. 31, 2014), www.lenta.ru/news/2014/01/31/extreme/.

[87] Namely, Federal'nyi zakon (federal law) July 27, 2006, No. 149.

[88] *See* Ivan Ivanov, *Internet: Use and keep in check*, OTRASLI PRAVA (Apr. 7, 2015), www.отрасли-права.рф/article/110.

> of an organization so as to avoid the application of such measures.[89]

Note that Russian legislation choose to speak of "extremism," a much broader concept than "terrorism." In contrast, for instance in the UK, while the State authorities do often mention "extremism" in official documents,[90] they usually revert to the definition of "terrorism" whenever discussing criminally prosecutable activities. Finally, the fact that over the last few years in Russia "thousands of sites were blocked by mistake"[91] also shows the ineptitude of those with access to the blocking mechanism.

The second wave of legislation calls for a complete de-anonymization of bloggers.[92] Dated May 5, 2014, *Federal Law No. 97-FZ* "*On amending the Federal Law 'On information, information technologies and protection of information'*" and certain legislative acts of the Russian Federation on streamlining the exchange of information using information and telecommunication networks, known as the "Blogger's Law,"[93] require that all bloggers with more than 3000 visits a day register with Roskomnadzor and disclose their real identity. Bloggers will have to follow the same rules as journalists working in conventional State-registered mass media. The restrictions include, among other things, obligations to (a) verify information before publishing it; (b) abstain from releasing reports containing slander, hate speech, extremist calls, or other banned information such as, for example, advice regarding suicide; (c) abstain from using obscene language; and (d) follow electoral agitation guidelines.

---

[89] Venice Commission Opinion on the Federal Law on Combating Extremist Activity, no. 660/2011.

[90] *See* Prime Minister's Task Force on Tackling Radicalization and Extremism, *Tackling Extremism in the UK*, U.K. GOVERNMENT (Dec. 4, 2013), https://www.gov.uk/government/publications/tackling-extremism-in-the-uk-report-by-the-extremism-taskforce.

[91] Soldatov & Borogan, *supra* note 74, at 313.

[92] In the end of July 2017, after this manuscript was accepted for the publication, a new Law prohibiting anonymizer and VPN usage and superseding Federal Law No. 97-FZ, was signed. Namely, Federal Law No. 276-FZ dated July 29, 2017 was enacted on November 1, 2017. This new piece of legislation prohibits usage of software and hardware solutions that facilitate access to the Internet resources blocked in Russia. The providers of such solutions will have to either voluntarily cooperate with Roskomnadzor, or face the prospect of unconditional ban on the Russian territory. It should also be observed that Federal Law No. 276-FZ only specifies the obligations of VPN service providers and website owners; ordinary Internet users would not, in principle, be prosecuted for using VPNs and anonymizers. *See* Oleg Soldatov, *The Russian VPN Ban: Another Round in the Battle for a Free Internet*, EUROPEAN CENTRE FOR PRESS AND MEDIA FREEDOM (Sept. 20, 2017), www.rcmediafreedom.eu/Tools/Legal-Resources/The-Russian-VPN-ban-another-round-in-the-battle-for-a-free-Internet.

[93] Neil McFarquhar, *Russia Quietly Tightens Reins on Web With "Bloggers Law"*, N.Y. TIMES (May 6, 2014), www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html.

Non-compliance with the Blogger's Law is punishable by substantial administrative fines, which were up to $14,000 at the time the law was passed.[94] The law also places ISPs under obligation to store the data, correspondence, and content of the hosted blogs for six months, and to provide such information to the investigative authorities upon request.

The number of bloggers affected by the law is significant. In 2014, the independent web counter LiveInternet estimated that there were about 500 independent Russian bloggers with an audience exceeding 3,000 unique daily visitors. Regarding social networks, the LiveInternet owner German Klimenko estimated that approximately 1,500 Russian-speaking Facebook users had audiences of 3,000 visitors or more.[95] These influential Internet personalities are now being scrutinized by the government. While the bloggers' new obligations may appear to further the balance between freedom of expression and other fundamental rights on the surface, the legislation's reliance on such vague concepts as "extremism" and "obscene language" make it overly broad. Other criticisms of this law can be summarized in three points.

First, while the discussion about the existence of a legal right to online anonymity is still inconclusive,[96] the law makes anonymous and pseudonymous blogging an impossible undertaking in Russia. If there is even a remote possibility that a blogger's daily audience will overshoot 3,000 viewers, he is under an obligation to register and provide real-world contact details online. Pseudonymous blogging should not be seen as a tool employed solely by marginalized elements of society; it is also, for example, a tool used by those members of academia who do not want their blogging activities to affect their academic standing.[97]

Second, an accurate assessment of the number of visitors is obviously a weak link in the law, because the figure can be inflated by counting visits from search engine bots, repeat visits from the same users, and DDoS attacks on blogs; incidentally, these attacks have become an easy way of framing a user for non-registration with the Roskomnadzor. Collective blogs remain in an unregulated grey area.

Third, regarding verification of information the law places bloggers under the same restrictions as officially employed journalists, but without providing them with the same level of protection. Primarily, such protection concerns what is termed the "journalist's

---

[94] *See* PETER B. MAGGS ET AL., LAW AND LEGAL SYSTEM OF THE RUSSIAN FEDERATION 372 (2015).

[95] *See Legislative Restrictions on Popular Bloggers Come Into Force in Russia*, RUSS. TODAY (Aug. 1, 2014), www.rt.com/politics/177248-russia-bloggers-law-restrictions/.

[96] *See* Evgeni Moyakine, *Online Anonymity in the Modern Digital Age: Quest for a Legal Right*, 1 J. INFO. RTS., POL'Y & PRAC. 5 (2016).

[97] *See* Daniel W. Drezner, *So You Want to Blog . . . , in* APSA GUIDE TO PUBLICATIONS 181, 190 (2008).

privilege," which protects journalists from being compelled to disclose confidential information or sources.[98]

The third wave of legislation deals with data nationalism. Enacted on July 21, 2014, *Federal Law no. 242-FZ* **"***On amending the Federal Law 'On personal data' and the Federal Law 'On information, information technologies and protection of information'"* ("Database Law") prescribes that databases containing the personal data of Russian citizens shall be stored on servers that are physically located in the territory of the Russian Federation. According to this law, every legal entity or any individual collecting or processing personal data falls under the definition of the "operator." Therefore, each of these users has reporting obligations, such as informing Roskomnadzor—which keeps a special register of personal data "operators"—of the physical location of databases.[99]

Companies that violate the aforementioned legal requirements are placed on the Register of infringers of the rights of personal data subjects,[100] after which their access to websites, IP addresses or domains in violation of the law may be blocked, and persons responsible may face fines or even criminal sentences for the "illegal collection of personal data," pursuant to Article 137 of the Russian Criminal Code. Article 137 was already in place when *Federal Law no. 242-FZ* was enacted.[101]

As a side note, a recent non-binding interpretation provided by the Russian Ministry of Telecom and Mass Communication sheds some light on the possibility of backing up or processing personal data abroad. Specifically, "[p]ersonal data initially collected and stored in Russia can be transferred abroad or processed in databases located abroad. The key issue here, in order to protect the subject of personal data, is the initial location."[102]

---

[98] V. Sazonoiv, *The Law on Giving the Mass Media Status to Bloggers*, RADIO EKHO MOSKVY (May 7, 2014), echo.msk.ru/blog/advokat_sazonov/1315532-echo/.

[99] Mikhail Chentsov et al., *Personal Data Storage in Russia*, EAST-WEST DIGITAL NEWS (Sept. 2015), www.ewdn.com/files/personaldatastorage.pdf.

[100] *See* Anne Fiero, *Russia's Federal Law No 242-FZ—Where Does it Leave us on Data Retention and Sharing*, LINKEDIN (Oct. 1, 2015), www.linkedin.com/pulse/russias-federal-law-242-fz-where-does-leave-us-data-anne-fiero.

[101] Maggs et al., *supra* note 94.

[102] *Id.*

Basically, the law challenges the concept that the Internet is borderless[103] by forcing all social networking sites and online platforms to store personal data in Russia. On November 17, 2016, following a first-instance court decision and an unsuccessful appeal,[104] Roskomnadzor began to enforce a Russia-wide block of LinkedIn—the world's biggest business- and employment-oriented social network and the fourteenth most popular website at the time.[105] The LinkedIn application is also no longer available for download to mobile devices via the Apple App Store and Google Play.[106] In March 2017, LinkedIn wrote an official letter to Roskomnadzor and reaffirmed its unwillingness to store personal data on the servers located in Russia.[107]

Critics of this legislation oppose it because sorting and storing data based on the citizenship of data subjects may be overly expensive, a waste of time and computational power, and infeasible for many online platforms. Instead, platforms may choose to leave the country altogether, thereby cutting Russian citizens off from a significant portion of the Internet. Indeed, this law led a number of major international companies to consider leaving the Russian market because of the associated legal complexities.[108] Companies dependent on borderless cloud technologies will be forced to reassess their business models as well.[109]

The fourth wave of legislation concerns data retention and the further criminalization of certain online behavior. Dated July 7, 2016, *Federal Laws Nos. 374-FZ and 375-FZ*—also known as "Yarovaya Laws"[110]—expand on already existing legislative mechanisms mandating cooperation between ISPs and telecoms on the one hand and investigative authorities on the other. These laws further increase the state's surveillance discretion in the domain of digital communications. The law requires, among other things, that, as of July 1, 2018, ISPs and other telecommunications companies store all telephone conversations, text messages, videos, and picture messages for six months. In addition, telecom companies must retain customers' metadata—that is, information regarding with whom, when, for how

[103] *See* Oreste Pollicino & Marco Bassini, *supra* note 5, at 348–49.

[104] *See LinkedIn to be Blocked by Telecom Providers*, ROSKOMNADZOR (Nov. 17, 2016), rkn.gov.ru/news/rsoc/news41615.htm.

[105] *See* LinkedIn Traffic Statistics, ALEXA (Jan. 12, 2018), www.alexa.com/siteinfo/linkedin.com.

[106] *See* Cecilia Kang and Katie Benner, *Russia Requires Apple and Google to Remove LinkedIn from Local App Stores*, N.Y. TIMES (Jan. 6, 2017), www.nytimes.com/2017/01/06/technology/linkedin-blocked-in-russia.html.

[107] *See LinkedIn refused to eliminate violations of Russian legislation*, ROSKOMNADZOR (Mar. 7, 2017), rkn.gov.ru/news/rsoc/news43486.htm.

[108] Maggs et al., *supra* note 94.

[109] Fiero, *supra* note 100.

[110] Ivan Nechepurenko, *Russia Moves to Tighten Counterterror Law*, N.Y. TIMES (June 24, 2016), www.nytimes.com/2016/06/25/world/europe/russia-counterterrorism-yarovaya-law.html.

long, and from where they communicated—for three years. Investigative authorities can access such data retroactively. Providers of telecommunication services are also legally obliged to help investigative authorities decipher encrypted messages sent by users. In addition, expressing "justification" for terrorism online are criminally punishable by a prison sentence of up to seven years. According to Russian case-law, "justification" for terrorism does not have to be direct—the portrayal of a fictional terrorist character in a positive light would suffice for qualification of the behavior as "justification" for terrorism.[111] These provisions build on previous legislation[112] criminalizing "extremism"-related speech on the Internet.

In short, the legislation creates a precedent for the storage of personal data on a previously unseen scale, and makes criminally punishable the expression of a wider range of opinions on the Internet, further eroding online freedom of expression in Russia. The approach to data retention taken by the Russian legislature is in stark contrast to the position recently expressed by the European Court of Justice in its rulings in Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd* and *Seitlinger* and others, as well as the previously described Joined Cases C-203/15 and C-698/15 *Tele2* and *Watson*.

The laws under scrutiny have been criticized not only by journalists and human rights advocates,[113] but also by Russian state-funded experts.[114] First, the legislation creates a precedent for the storage of personal data on a hitherto unseen scale, making any security breaches a non-trivial event from the perspective of data protection.[115] Second, the representative of the biggest[116] Russian telecom operator, MTS, pointed out that, given MTS's current income figure, they would have to put all of their profits into the data center infrastructure for the next 100 years to fully implement data storage provisions and ensure compliance with Yarovaya's Laws.[117] The fact that most Russian telecoms will not be able to

---

[111] Postanovlenie Plenuma Verkhovongo Suda Rossiiskoi Federatsii [Russian Federation Supreme Court Plenary Ruling of Feb. 9, 2012] BIULLETEN' VERKHOVNOGO SUDA RF [BVS] [Bulletin of the Supreme Court of the Russian Federation] 2012, No. 1.

[112] Federal'nyi zakon (federal law) July 21, 2014, No. 274.

[113] *See* Ronald Bailey, *I Learned It By Watching You!*, REASON 18 (Nov. 2016).

[114] *See* Tamara Morschakova et al., *Zakonoproekty Ozerova i Yarovoj ne snizjat terroristicheskoj i jekstremistskoj ugrozy i nuzhdajutsja v pererabotke [Draft laws prepared by Ozerov and Yarovaya will not decrease the terrorist and extremist threat, and need to be reworked]*, HUMAN RIGHTS COUNCIL (Apr. 16, 2016), www.president-sovet.ru/presscenter/news/read/3151/.

[115] *See* S. Potresov, *"Popravki Yarovoj i Ozerova," tsena voprosa* [*Ozerov's and Yarova's Drafts, Amounts Involved*], MOBILE-REVIEW (June 24, 2016), www.mobile-review.com/articles/2016/data-storage.shtml.

[116] *See* V. Savitskiy, *Kvartalnyy Podschet* [*Quarterly Results*], COMNEWS (Sept. 1, 2016), www.comnews.ru/content /103556/2016-09-01/kvartalnyy-podschet.

[117] Potresov, *supra* note 115.

comply with this legislation may in fact be beneficial for the government; those companies will become *de facto* criminals, giving the state authorities "the leverage to extract from them any other concession it desires."[118]

Recent Russian case-law corroborates the fact that newly introduced criminal sentences, in accordance with both Yarovaya's law and *Federal Law No. 274-FZ*, can be imposed for an offense as minor as reposting or retweeting content that is critical of Russia's external policy in Ukraine or Syria.[119]

E. Tumultuous Relationship Between Russia and the European Court of Human Rights

The changes introduced by the legislation packages described above appear to be even more disturbing given the emergent problems with the international overview of the situation regarding human rights standards in Russia. Europe may be on the brink of changes signifying the Russian departure from one of the most effective,[120] and active,[121] local mechanisms of human rights protection. The European Court of Human Rights, which, as stated above, has jurisdiction to adjudicate over the applications alleging that one or more of the 47 Council of Europe member states that have breached one or more of the human rights provisions set out in the Convention and its Protocols. At the time of its ratification by Russia in 1998, the Convention was seen by many new democracies "as a document they should subscribe to, to demonstrate the seriousness of their break with their pasts and their commitment to a democratic future."[122] Some researchers go as far as to claim that the strength of the protection of human rights in Europe today derives partly from their enforcement by the European Court of Human Rights.[123]

In principle, by ratifying the Convention, the Russian Federation has undertaken to comply with final judgments of the European Court of Human Rights in instances of finding violations of the Convention—see Article 46—along with other Council of Europe member states.

---

[118] Bailey, *supra* note 113.

[119] *See Vkontakte so sledovatelyami* [*On-line with Prosecutors*], MEDUSA (July 5, 2016), www.meduza.io/feature/2016/ 07/05/vkontakte-so-sledovatelyami.

[120] *See* European Commission on Human Rights, *High Level Conference on the Future of the European Court of Human Rights,* Brighton Declaration (Apr. 19, 2012), www.echr.coe.int/Documents/2012_Brighton_FinalDeclaration_ ENG.pdf (last visited April 7, 2017).

[121] *See* Alec Stone Sweet, *On the Constitutionalisation of the Convention: The European Court of Human Rights as a Constitutional Court*, 71 FAC. SCHOLARSHIP SERIES 4 (2009).

[122] Ed Bates, THE EVOLUTION OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS: FROM ITS INCEPTION TO THE CREATION OF A PERMANENT COURT OF HUMAN RIGHTS 22 (2010).

[123] Sionaidh Douglas-Scott, *A Tale of Two Courts: Luxembourg, Strasbourg and the Growing European Human Rights Acquis*, 43 COMMON MKT. L. REV. 629, 631 (2006).

Indeed, "[a] judgment of the European Court of Human Rights is not an end in itself, but a promise of future change, the starting point of a process which should enable rights and freedoms to be made effective."[124]

As the Council of Europe's decision-taking body, the Committee of Ministers supervises execution of the judgments of the Court. It not only ensures that damages awarded by the Court are paid but it also assists the respondent State in finding suitable measures to comply with all other demands made by the European Court of Human Rights. The latter can be challenging whenever the Court places on the member state an obligation to prevent certain human rights violations from happening again, which can often only be accomplished by making changes to the national legislation.[125] The Committee of Ministers has made it clear that respecting the Court's judgments is one of the conditions of membership in the Council of Europe.[126] Recently, the Committee of Ministers has also been taking steps to ensure the enforcement of judgments dealing with Article 10 violations online. For instance, it was applied in the course of an enhanced supervision procedure concerning the execution of *Ahmet Yildirim* v *Turkey*, a 2012 judgment dealing with the restriction of access to the Internet.[127]

Broadly speaking, adjudication before the Strasbourg-based court has proven to be an effective and popular instrument for mitigating human rights abuses in Council of Europe member states, to the point of the Court becoming "a victim of its own success,"[128] and being considerably overloaded by incoming applications.[129] Historically, Russia has been the leader in generating the Court's workload, and "has experienced a turbulent relationship with the European Court of Human Rights ever since it joined the Council of Europe."[130] In 2013, following a number of high-profile cases that the country lost in the Strasbourg Court, the

---

[124] Francoise Tulkens, *Execution and Effects of Judgments of the European Court of Human Rights: The Role of the Judiciary*, *in* DIALOGUE BETWEEN JUDGES 9, 12 (2006).

[125] *See Supervision of the execution of judgments and decisions of the European Court of Human Rights: 9th Annual Report of the Committee of Ministers*, COUNCIL OF EUROPE 21 (2016).

[126] *See* Elisabeth Lambert Abdelgawad, THE EXECUTION OF JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS 6 (2006) (citing interim resolutions in cases of *Loizidou* v *Turkey*, and *Ilaşcu and others* v *Moldova and the Russian Federation*).

[127] COUNCIL OF EUROPE, *supra* note 125, at 101.

[128] Laurence R. Helfer, *Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime*, 19 EUR. J. INT'L L. 125, 125 (2008).

[129] *High Level Conference on the Future of the European Court of Human* Rights, Brighton Declaration, *supra* note 120.

[130] William E. Pomeranz, *Uneasy Partners: Russia and the European Court of Human Rights*, 19 HUMAN RTS. BRIEF 17, 17 (2012).

Chairman of Russia's Constitutional Court openly expressed his dissatisfaction with the outcome of several cases before the Court.[131]

The turbulence reached its peak on July 14, 2015, when Russia's Constitutional Court ruled that the Constitution of the Russian Federation, as well as those laws that had already been declared constitutional by the country's Constitutional Court, should take precedence over decisions of the European Court of Human Rights.[132] The mechanism of establishing such a precedence, laid down in *Federal Law No. 7-FKZ* passed in December 2015, operates through adjudication by the Constitutional Court of the Russian Federation.[133] It should be further noted that in its decision, the Russian Constitutional Court referred to several European Court of Human Rights judgments that, in the view of the Constitutional Court, did not conform with principles of the legal order of the Russian Federation and, ultimately, should not be executed.[134]

Essentially, the ruling and the federal law in question gave Russian authorities the right to ignore judgments of the European Court, based on the views expressed by the country's Constitutional Court. On April 19, 2016, the Constitutional Court of the Russian Federation ruled for the first time that a decision of the Strasbourg Court of Human Rights could not be implemented in Russia because the measures aimed at its implementation would contradict the Constitution.[135]

The decision of the Russian Constitutional Court rekindled discussion on the clash between constitutional law and international human rights law, two leading systems for protecting the fundamental rights of individuals.[136] As Alec Stone Sweet argued, the scope of the European Court's authority is indeed comparable to that of national constitutional and supreme courts, and it is well positioned to exercise a decisive influence on the development

---

[131] *See* Lauri Mälksoo, *Russia's Constitutional Court Defies the European Court of Human Rights*, 12 EUR. CONST. L. REV. 377, 380 (2016).

[132] Postanovlenie Konstitutsionnogo Sudaa Rossiiskoi Federatsii ot 14 июль 2015 [Decision of the Constitutional Court of the Russian Federation of July 14, 2015], ROSSIISKAIA GAZETA [ROS. GAZ.] 2015, No. 21-П [hereinafter Decision of the Constitutional Court of the Russian Federation].

[133] This law was criticized by the Venice Commission. *See* Venice Commission Interim Opinion on the Amendments to the Federal Constitutional Law on the Constitutional Court of the Russian Federation no. 832/2015, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)005-e.

[134] Decision of the Constitutional Court of the Russian Federation, *supra* note 132.

[135] Postanovlenie Konstitutsionnogo Sudaa Rossiiskoi Federatsii ot 19 апрель 2016 [Decision of the Constitutional Court of the Russian Federation of Apr. 19, 2016], ROSSIISKAIA GAZETA [ROS. GAZ.] 2016, No. 12-П [Decision of the Constitutional Court of the Russian Federation of Apr. 19, 2016].

[136] *See* Gerald L. Neuman, *Human Rights and Constitutional Rights: Harmony and Dissonance*, 55 STAN. L. REV. 1863, 1863 (2003).

of a rights-based, pan-European constitutionalism. As his article points out, there are precedents of conflicts between the legal systems of the Council of Europe member states, particularly referring to the infamous *Hirst* v *United Kingdom* judgment, and the framework of the European Convention on Human Rights.[137] Another example of the unpredictability of the relationship between the Strasbourg Court and national constitutional courts comes from Italy, where the Constitutional Court concluded that the privileged constitutional status enjoyed by the tenets of international law as generally recognized rules cannot extend to the country's international obligations under an international treaty, such as the European Convention on Human Rights.[138] In turn, in Germany and Spain the constitutional courts considered the interpretation of the European Convention on Human Rights through the lens of the Court's case-law should be as narrow as possible.[139]

As seen from these examples, constitutional courts are quite often constrained by the imperative not to lose their privileged position as arbiters of fundamental rights "at the crossroads between the domestic and the international legal orders."[140] At the same time, the codification of differences between national constitutional law and the Convention as interpreted by the European Court of Human Rights, and not just the acknowledgment of such differences in the ruling of the constitutional court, is exceptional. It provides evidence of the Russian Federation's unwillingness to give up a part of its constitutional sovereignty unconditionally, and might set a troubling precedent for other Council of Europe member states.

At the moment, in the European Court of Human Rights there are more than 5,000 pending cases against Russia, classified as potentially admissible and assigned to a Chamber, and in which the Court has communicated its questions to the parties.[141] Almost 100 of these cases deal with Article 10 (freedom of expression), and more than 200 deal with Article 8 of the European Convention on Human Rights (private life). A substantial portion, 26 percent, of applications, as of April 2017, including cases by opposition leaders and Non-Governmental Organizations,[142] concern various Internet-related issues, and it remains to be seen how the

---

[137] Sweet, *supra* note 121, at 6.

[138] *See* Oreste Pollicino, *The European Court of Human Rights and the Italian Constitutional Court: No "Groovy Kind of Love"*, *in* THE UK AND EUROPEAN HUMAN RIGHTS: A STRAINED RELATIONSHIP? 361, 363 (K. Siegler ed., 2015).

[139] *See* M. Kanetake and A. Nollkaemper, *The Rule of Law at the National and International Levels* 215 (Hart Publishing 2016).

[140] Pollicino, *supra* note 138, at 377.

[141] European Court of Human Rights HUDOC Database Search, hudoc.echr.coe.int/eng#{%22respondent%22:[%22RUS%22],%22documentcollectionid2%22:[%22CHAMBER%22,%22COMMUNICATEDCASES%22]} (last visited January 17, 2018).

[142] European Court of Human Rights HUDOC Database Search, hudoc.echr.coe.int/eng#{%22fulltext%22:[%22internet%22],%22respondent%22:[%22RUS%22],%22article%22:[%228%22,%228-1%22,%228-

Russian Federation will react to the potentially unfavorable outcomes of proceedings before the Court. It should be noted that some of the recent case-law developments concerning privacy and freedom of expression are found in judgments against Russia. For instance, according to Judge Robert Spano, "the case of *Roman Zakharov v. Russia* is the Court's current most elaborate judgment on the issue of interception of data by police for law enforcement purposes."[143]

Other examples of relatively recent conclusions reached by the Court in contentious cases against Russia include the State's obligation to protect freedom of expression against attacks coming from private individuals, covered in *Shabanov* v. *Russia*.[144] The idea that political controversy contributes, by its very nature, to general interest debates, reached in *Filatenko* v. *Russia*;[145]and the unlawfulness of police databases tracking train and air travel about the country, commented upon in *Shimovolos* v *Russia,*[146] and so on.

Whenever dealing with countries that have generic domestic problems of a legal order, the last resort technique employed by the European Court of Human Rights includes indication of general measures in the operative part of its judgments. In doing so, the Court not only points out the underlying problem a respondent state faces, but also proposes a solution. For example, the Court introduced effective domestic remedies in certain situations on a legislative level.[147] If the authors' pessimistic view with regard to recent developments in Russia concerning regulation of the Internet proves to be true, the Court would, for the foreseeable future, experience an influx of cases dealing with the alleged incompatibility of the above-mentioned legislation with the Convention. Should the Court choose to side with

2%22,%2210%22,%2210-1%22,%2210-2%22],%22documentcollectionid2%22:[%22COMMUNICATEDCASES%22]} (last visited Jan. 17, 2018).

[143] Oleg Soldatov, *Data Retention Under the 2016 Yarovaya Law in Russia*, MEDIALAWS (March 2, 2017), www.medialaws.eu/data-retention-under-the-2016-yarovaya-law-in-russia-disrupting-the-european-status-quo/.

[144] Shabanov & Tren v. Russia, App. No. 5433/02 (Dec. 2006), http://hudoc.echr.coe.int/. In this case, the Court explored, *inter alia,* the journalistic duties to cover stories of general interest and to avoid gratuitous attacks on public personalities' reputations.

[145] Filatenko v. Russia, App. No. 73219/01 (June 3, 2004), http://hudoc.echr.coe.int/. In this case, the Court reached the conclusion that opinions and information aired during an electoral campaign should be considered as part of a debate on issues of public interest and that there is little scope under Article 10 for restrictions on such a debate.

[146] Shimovolos v. Russia, App. No. 30194/09 (June 21, 2011), http://hudoc.echr.coe.int/. In this case, the Court noted that the existence of the "surveillance database" containing the information about the applicant's travel amounted to an interference with his private life, given the fact that the creation and maintenance of the database and the procedure for its operation were governed by a ministerial order, which had never been published or otherwise made accessible to the public.

[147] Olga Dubinska & Oleg Soldatov, *Fighting the Lernaean Hydra—General Measures in the Operative Part of the European Court of Human Rights Judgments: Broad Context and Ukrainian Perspectives*, 1 KYIV-MOHYLA L. & POL. J. 176, 179–80 (2015).

critics of the Russian regulatory approach, such an influx is likely to lead to adoption of the judgment containing the general measures in its operative part. This judgment, at odds with current Russian policy, could in turn trigger the mechanism of overruling the European Court of Human Rights by the Russian Constitutional Court. Of course, such a mechanism can also be triggered by a single judgment examining a one-off case dealing with Russian violations of Article 8 or 10.

Consequently, the authors do not hold out hope that the contentious legislation presented in this Article may be annulled by the Russian legislature even after being criticized by the European Court of Human Rights, either on a case-by-case basis or by adopting umbrella judgments related to the general measures. To recapitulate, the current attitudes of Russian authorities towards the European Court of Human Rights can be summed up by the words of President Vladimir Putin, in whose view "[the European Court] does not regulate legal relations, does not protect rights, but simply executes some kind of political function."[148]

F. Conclusion

Recent terrorist attacks, coupled with the fact that the online domain is one of the tools that terrorist groups use, have reminded Europeans of the need to address illegal online speech. The problem of how to balance state security with online freedom of expression and privacy requires an urgent solution. In this respect, however, the roles of judges, legislators and, international institutions, remain disputed.

Within its geographical borders, the "wider" Europe, which includes Russia, presents a perfect illustration of how divergent any effective regulation of the Internet can be. Due to the ethnic composition of the North Caucasus region, and to historical events in that area, Russia is similar to many other European countries in which political violence and terrorism have religious and ethnic foundations—for example, the United Kingdom, the Netherlands, Turkey, France, and Spain. Nevertheless, the approach taken by Russian legislature with the rationalization of curbing the terrorist threat is markedly different from that of many European countries.

The Sixth Convocation (2011–2016) of the Russian Parliament passed a long list of laws regulating the Internet. These laws provide State authorities with a wide set of measures to control online communication, and are among the most radical on the continent. The genuine driving force behind all these precautions is difficult to determine, as the legislative package in question can be seen through two different lenses. The first is that authorities in Putin's Russia are frank and sincere fighters against terrorism and extremism. The second is

[148] *Putin: vyhod Rossii iz-pod jurisdikcii ESPCh vozmozhen, no vopros na povestke ne stoit* [*Putin: Russia Can Leave the Jurisdiction of the European Court of Human Rights, but the Question is not on the Agenda*], TASS (Aug. 14, 2015), www.tass.ru/politika/1380242.

that the Russian Federation is demonstrating politically an increasingly authoritarian state in which anti-terrorism concerns are a smoke-screen used by politicians with the aim of further reducing freedom of expression in order to fortify their subservient political system. It remains to be seen whether legislators in other European countries will be tempted to follow the example of any of Russia's novel Internet-related legislation, especially given Russia's influence over many of its Eastern European neighbors that were part of the former Soviet Bloc.

Moreover, the 2015 codification in a federal law regarding Russia's unwillingness to give up part of its constitutional sovereignty to the Strasbourg Court within the framework of the European Convention on Human Rights might also establish a dangerous precedent for other Council of Europe member states. The codification rekindles the debate on the relationship between international and national mechanisms of human rights protection, and may prevent the effective intervention by the European Court of Human Rights in the situation regarding online regulation in Russia.

The authors believe this topic will be well worth revisiting when more empirical data becomes available concerning real-life consequences of the discussed legislation, and after the highly probable examination of matters under consideration by the European Court of Human Rights.