Internet Censorship in Russia: The Sovereign Internet Laws and Russia's Obligations Under the European Convention on Human Rights

Erik Allerson

Author's Note

This Note was written and selected for publication in Spring 2021. In the year since it was written, Russia invaded Ukraine and was expelled from the Council of Europe. While much of this Note is premised upon Russia's membership on the Council of Europe, we have decided nevertheless to move forward with publication. The mechanisms authorized in the Sovereign Internet Laws are currently being used as part of the Kremlin's campaign to silence domestic and foreign dissent. Russia's actions have only increased concerns that it will create a splinternet as part of its push to control the online narrative. Hopefully this Note can serve as an additional resource for information on the Sovereign Internet Laws and the potential long-term implications of Russia's online censorship strategy.

INTRODUCTION

In the last decade, Russia has quietly overhauled its internet regulatory framework in order to exert subtle yet substantial control over internet access and content in the country.[1] As a member state of the Council of Europe, Russia is obligated to abide by Article 10 of the European Convention on Human Rights (Convention).[2] This Article is recognized by the Council of Europe as protecting one's ability to receive and impart information and ideas via the internet.[3] On November 1, 2019, Russia's Sovereign Internet Laws came into force.[4] They

1. *See* discussion *infra* Section I.B.

2. *See infra* Section I.A.

3. *See* Comm. of Ministers, *Declaration on Freedom of Communication on the Internet*, COUNCIL EUR., https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5 (last visited May 26, 2022).

4. FEDERAL'NYI ZAKON O VNECENII IZMENENII V FEDERAL'NYI ZAKON O SVYAZII I FEDERAL'NYI ZAKON OB INFORMATSII, INFORMATSIONNIX

consisted of three primary amendments to Russia's existing system of internet regulation: 1) they required internet service providers to install equipment for counteracting threats,[5] 2) they centralized management of networks under the federal government and implemented a control mechanism for connection lines crossing the Russian border;[6] and 3) they directed the implementation of a national Domain Name System (DNS).[7] These actions stand in stark contrast to Russia's obligations under the Convention and must be addressed accordingly.[8]

This Note outlines how Russia's Sovereign Internet Laws build upon a regulatory framework that directly contravenes Russia's obligations under the European Convention on Human Rights. Part I describes Russia's obligations under the Convention, its history of online censorship and control, how the European Court of Human Rights has responded in recent years, and Russia's new Sovereign Internet Laws. Part II analyzes how the Russian application of the Sovereign Internet Laws would compare to its past Article 10 violations, and how the Court can respond to this new legislation. This Note concludes that the Court should amend its practices to allow punitive damages to increase the monetary and political cost to Russia for its online censorship regime and deter Russia from this course of action.

I. BACKGROUND

A. THE EUROPEAN CONVENTION ON HUMAN RIGHTS

International law has been an integral part of Russian law

TECHNOLOGIYAX I O ZAZHITYE INFORMATSII [Federal Law No. 90-FZ of May 1, 2019, "On Amendments to the Federal Law," "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection"] art. 3, SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOĬ FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2019, No. 18, Item 2214, http://publication.pravo.gov.ru/Document/View/0001201905010025?index=0&rangeSize=1. *See generally* Alena Epifanova, *Deciphering "Russia's Sovereign Internet Law": Tightening Control and Accelerating the Splinternet*, GERMAN COUNCIL ON FOREIGN RELS.: DGAP ANALYSIS 2 (Jan. 2020), https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf (analyzing the Russian Sovereign Internet laws).

5. Federal Law No. 90-FZ, art. 1.
6. *Id.*
7. *Id.* art. 2.
8. *See infra* Section II.A.

since Russia adopted its 1993 Constitution.[9] Article 15(4) of the Russian Constitution establishes that the recognized norms of international law, as well as Russia's international treaties and agreements, are important components of the Russian legal system.[10] It also applies the rules of Russia's international treaties or agreements if they are different than what is envisaged by its domestic laws.[11] "This is a formulation without precedent in Imperial Russian and Soviet law and legal practice insofar as it, first, accepts generally-recognized principles and norms of international law as part of Russian law and, second, places such norms and principles side by side with norms of municipal Russian law."[12]

In this aim, Russia ratified the European Convention on Human Rights and entered it into force on May 5, 1998.[13] Doing so was the culmination of promises made as Russia transitioned from the Soviet era into the modern Russian state.[14] Among the Convention's many protections—such as the right to a fair trial and the right to freedom of thought, conscience, and religion—it also expressly protects the right to freedom of expression.[15] Article 10 states:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such

9. KONSTITUTSIIA ROSSIĬSKOĬ FEDERATSII [KONST. RF] [CONSTITUTION] art. 15(4) (Russ.).

10. *Id.*

11. *Id.*

12. WILLIAM E. BUTLER, RUSSIAN LAW 112 (3d ed. 2009).

13. *Chart of Signatures and Ratifications: Convention for the Protection of Human Rights and Fundamental Freedoms*, COUNCIL EUR. (last updated Mar. 19, 2022), https://www.coe.int/en/web/conventions/by-subject-matters?module=signatures-by-treaty&treatynum=005.

14. *See* Tatyana Beschastna, *Freedom of Expression in Russia as it Relates to Criticism of the Government*, 27 EMORY INT'L L. REV. 1105, 1105–06 (2013).

15. Convention for the Protection of Human Rights and Fundamental Freedoms arts. 6–10, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].

> formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[16]

Under Article 10, Russia is bound to protect its citizens' freedom to express themselves, receive information, and impart information, regardless of the medium, and without undue interference.[17] This duty is reinforced in Russian law under Article 15(4) of the Russian Constitution and specific language codified in federal law when the Convention was adopted.[18] "It is undoubted in Russian doctrine that the Russian Federation is bound . . . to comply with decisions of the ECHR concerning cases in which Russia is a party."[19]

The principles enumerated in Article 10 have since been further developed. On May 28, 2003, the Council of Europe's Committee of Ministers adopted the Declaration on Freedom of Communication on the Internet.[20] Principle 3 of this Declaration articulates the member states' commitment to freedom of communication on the internet:

> Public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers . . . .
>
> Provided that the safeguards or Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms are respected, measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on

16. *Id.* art. 10.
17. *Id.*
18. *See* [KONST. RF] [CONSTITUTION] art. 15(4).
19. BUTLER, *supra* note 12, at 107.
20. Comm. of Ministers, *supra* note 3.

its illegality.[21]

Despite this commitment, when a later recommendation, CM/Rec(2016)5, was adopted by the Committee of Ministers of the Council of Europe in 2016, the Russian representative reserved the right of his government to comply or not to comply with the recommendation.[22] This recommendation provided internet freedom indicators, which inform and guide member states when adopting international policy and participating in international dialogue.[23] Among its freedom indicators, it included requirements that any act to block or restrict access to internet platforms, sites, technologies, or content comply with Article 10 of the Convention.[24]

B. RUSSIAN INTERNET

Despite its international obligations, Russia has numerous laws and programs in place to monitor, control, and block its citizens' internet activity. Although the Russian internet developed with little to no censorship throughout the 2000s, the Russian government enacted a string of legislation in the early 2010s that built upon itself to exert greater control and censorship over Russian internet.[25] This approach constituted "an alternative approach to information manipulation and control . . . that relies on a mix of less overt, more plausibly deniable, legalistic, and often non-technical mechanisms to manipulate online information flows, narratives, and framings, to affect and shape public opinion."[26]

This legislation has created a legal framework under which the Russian government can block content, systematically

---

21. *Id.*

22. Bulgakov v. Russia, App. No. 20159/15, ¶ 20 (June 23, 2020), http://hudoc.echr.coe.int/eng?i=001-203181.

23. *Id.*; Comm. of Ministers, *Recommendation CM/Rec(2016)5 of the Committee of Ministers to Member States on Internet Freedom*, 1253d mtg. (Apr. 13, 2016), https://rm.coe.int/09000016806415fa.

24. Comm. of Ministers, *supra* note 23.

25. Liudmila Sivetc, *State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners*, 27 INT'L J.L. & INFO. TECH. 28, 29–30 (2019) ("As concluded in a study conducted by the OpenNet Initiative, the regulation of the internet in Russia was done minimally and very subtly, without obvious signs of state censorship.").

26. Jaclyn Kerr, *The Russian Model of Information Control and its Significance*, *in* ARTIFICIAL INTELLIGENCE, CHINA, RUSSIA, AND THE GLOBAL ORDER 62, 65 (Nicholas D. Wright ed. 2018).

collect user data, and place liability on content intermediaries.[27] Using Russia's System for Operative Investigative Activities (SORM) program, the Russian government is able to surveil Russian citizens' telephone and internet communications.[28] Beginning with a 2012 blacklist of censored websites, Russia has expanded censorship through amending the Civil Code and the Russian Information Act[29] via its "Anti-Piracy Law," "Anti-LGBT Propaganda Law," "Law on Pre-Trial Blocking of Websites," and "Anti-Terrorist Laws."[30] The 2013 Anti-Piracy Law gave Russian authorities the power to force internet companies to cut off access to sites accused of harboring pirated media without a court order.[31] The law gives accused sites a mere 72 hours to respond before enacting a permanent ban.[32] The Anti-LGBT Propaganda Law extended the 2012 blacklist on sites pertaining to child pornography, suicide, and drug use, to also require censorship of sites providing content that could be considered propaganda directed at children advocating alternative sexual orientations.[33] The Law on Pre-Trial Blocking

27. *See id.* at 65–66.

28. *Id.* at 67.

29. *See* Veronica Fridman, *The Drive to Improve Russian Anti-Piracy Protection Intensifies*, LEXOLOGY (Jun. 8, 2020), https://www.lexology.com/library/detail.aspx?g=78a7762f-c684-4965-ae27-f4228e4d607e.

30. Kerr, *supra* note 26, at 65–66.

31. FEDERAL'NYI ZAKON O VNECENII IZMENENII V OTDEL'NYI ZAKONODATEL'NYI AKTII ROSSISKOI FEDERATSII PO VOPROSAM ZATSITII INTELLEKTURALNIKH PRAV V INFORMATSIONNO TELEKOMUNIKATSIONNIKH SETRAKH [Federal Law No. 187-FZ of July 2, 2013, "On Amendments to Certain Legislative Acts of the Russian Federation on the Protection of Intellectual Rights in Information and Telecommunication Networks"] art. 3, SZ RF 2013, No. 27, Item 3479, http://pravo.gov.ru/proxy/ips/?docview&page=1&print=1&nd=102166470&rdk=1&&empire=; *Russia Beefs Up Anti-Piracy Laws*, BBC (May 1, 2015), https://www.bbc.com/news/technology-32531275#:~:text=Russia%20is%20beefing%20up%20the,pirated%20movies%20and%20TV%20shows.

32. Federal Law No. 187-FZ, art. 3.

33. FEDERAL'NYI ZAKON O VNECENII IZMENENII V STRATIU 5 FEDERALNOVO ZAKONA O ZATSITYE DYETYEI OT INFORMATSII, PRICHINYAIASHYEI VRED IKH ZDOROVIU I RAZVITIIU I OTDELNIYE ZAKONODATELNIYE AKTI ROSSISKOI FEDERATSII V TSYELYAKH ZASHITI DETYEI OT INFORMATSII, PROPAGANDIRIUSHYEI OTRITSANIYE TRADITSIONIIKH SEMYEINIKH TSENNOSTYEI [Federal Law No. 135-FZ of June 29, 1993, "On Amendments to Article 5 of the Federal Law 'On the Protection of Children from Information Harmful to Their Health and Development' and Certain Legislative Acts of the Russian Federation in Order to Protect Children from Information that Promotes the Denial of Traditional Family Values,"] SZ RF 2013, No. 26, Item

of Websites "permitted the immediate blocking of sites deemed to contain 'incitement to extremisms or riots,' and was used to abruptly block several leading oppositional news outlets and blogs at the height of the Crimea Annexation crisis."[34] Finally, in the Anti-Terrorist Laws of 2014, *Federal Law No. 97-FZ* (better known as the "Blogger's Law") required bloggers with a daily audience of greater than 3,000 views to register on a national list and comply with fact-checking media regulations.[35]

Although SORM had previously only been monitoring internet service providers (ISPs), in 2014 the Russian government began requiring that social networks operating in Russia install SORM monitoring equipment.[36] Russia has frequently explained that its measures are required in order to combat terrorism, primarily stemming from its conflicts in Chechnya.[37] Yet, observers of Russia's actions tend to view them through one of two lenses:

> The first is that the authorities in Putin's Russia are frank and sincere fighters of terrorism and extremism.

3208, http://publication.pravo.gov.ru/Document/View/0001201306300001; Kerr, *supra* note 26, at 65.

34. Kerr, *supra* note 26, at 65; *see also* FEDERAL'NYI ZAKON O VNECENII IZMENENII V FEDERAL'NYI ZAKON OB INFORMATSIONNIKH TEKHNOLOGIYAKH I O ZASHITYE INFORMATSIN [Federal Law No. 398-FZ of December 28, 2013 "On Amendments to the Federal Law "On Information, Information Technologies and Information Protection,"] SZ RF 2013, No. 52, Item 6963, http://publication.pravo.gov.ru/Document/View/0001201312300069.

35. Oreste Pollicino & Oleg Soldatov, *Striking the Balance Between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context*, 19 GERMAN L.J. 85, 98 (2018); FEDERAL'NYI ZAKON O VNECENII IZMENENII V FEDERAL'NYI ZAKON OB INFORMATSII, INFORMATSIONNIKH TEKHNOLOGIYAKH I O ZASHITYE INFORMATSII I OTDELNIYE ZAKONODATELNIYE AKTI ROSSIISKOI FEDERATSII PO VOPROSAM UPORYADOCHENIYA OBMYENA INFORMATSIYE S ISPOLZOVANIYEM INFORMATSIONNO TELEKOMMUNIKATSIONNIKH SYETYEI [Federal Law No. 97-FZ of May 5, 2014 "On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection' and Certain Legislative Acts of the Russian Federation on Regulating the Exchange of Information Using Information and Telecommunication Networks"] art. 1, SZ RF 2014, No. 19, Item 2302, http://ips.pravo.gov.ru:8080/default.aspx?pn=0001201405050068. These regulations as applied to bloggers were repealed in 2017. FEDERAL'NYI ZAKON O VNECENII IZMENENII V FEDERAL'NYI ZAKON OB INFORMATSII, INFORMATSIONNIKH TEKHNOLOGIYAKH I O ZASHITYE INFORMATSIN [Federal Law No. 276-FZ of July 29, 2017, "On Information, Information Technologies and Information Protection"] art. 1, SZ RF 2017, No. 31, Item 4825, https://rg.ru/2017/07/30/fz276-site-dok.html.

36. Kerr, *supra* note 26, at 67.

37. *See* Pollicino & Soldatov, *supra* note 35, at 97–98.

> 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.[38]

No matter the inspiration behind these laws, the method by which they have been wielded has had a direct impact on ordinary Russians. Russian social network users, such as 23-year-old Maria Motuznaya, have faced criminal charges for posting controversial content, such as "memes."[39] After sharing satirical memes about the Russian Orthodox Church on her VKontakte account (Russia's largest social media site), Maria was added to Russia's official list of extremists and terrorists and was charged with "hate speech and offending religious believers' feelings – both criminal offences in Russia."[40] She faced up to six years in prison for these charges.[41] After she fled Russia, the case against her was eventually discontinued.[42] Although VKontakte claims that it only provides user information to the authorities in response to requests that comply with the law, critics say it actively cooperates with Russian authorities.[43] Some of the laws VKontakte is referring to are the Yarovaya amendments, which were passed in 2016.[44] The Yarovaya amendments required telecom providers, social

---

38. *Id.* at 98.

39. *See* Olga Robinson, *The Memes That Might Get You Jailed in Russia*, BBC (Aug. 23, 2018), https://www.bbc.com/news/blogs-trending-45247879. A meme is "a cultural item in the form of an image, video, phrase, etc., that is spread via the internet and often altered in a creative or humorous way." *Meme*, DICTIONARY.COM, https://www.dictionary.com/browse/meme# (last visited May 26, 2022).

40. Robinson, *supra* note 39 ("One of the offending memes shows women dressed as nuns smoking cigarettes and urging each other to be quick 'while God isn't looking.'").

41. *Id.*

42. Anton Starkov, *Maria Motuznaya: I Want to Delete All Social Networks and Disappear Forever*, DAILY STORM (Jan. 11, 2019), https://dailystorm.ru/obschestvo/mariya-motuznaya-hochetsya-udalit-vse-socseti-i-propast-navsegda (Russ.).

43. *See* Robinson, *supra* note 39.

44. Alina Polyakova & Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, BROOKINGS: DEMOCRACY & DISORDER 9 (Aug. 2019), https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

media platforms, and messaging services to store user data for three years and provide Russia's security service, the FSB, access to the information.[45]

Russia then "began blocking virtual private networks (VPN) that allow access to banned content," and enacted legislation "allowing the Russian government to designate media organizations as 'foreign agents'" if they receive funding from abroad.[46] This also allowed the government to block online content such as social media websites that hosted activities declared "undesirable" or "extremist."[47] After many amendments, the government may now block access to any distributed information that appeals for public protest, so long as it designates the information as "undesirable" or "extremist."[48]

C. THE EUROPEAN COURT OF HUMAN RIGHTS

The European Court of Human Rights is no stranger to addressing Russian Article 10 violations or its human rights violations in general.[49] Despite the promises Russia made in its Constitution and in its ratification of the European Convention on Human Rights, it has repeatedly been found in violation of its obligations as a member of the Council of Europe by the Court.[50] In 2019, Russia had the most adverse judgments against it by the Court with 186 out of a total 198 judgments finding at least one violation of the Convention.[51] This substantially outnumbered the second-highest, Ukraine, with 109 adverse

45. *Id.*

46. *Id.* A virtual private network is "a private computer network that functions over a public network (such as the internet) and usually utilizes data encryption to provide secure access to something (such as an internal business server or private network)." *Virtual Private Network*, Merriam-Webster, https://www.merriam-webster.com/dictionary/virtual%20private%20network (last visited May 26, 2022).

47. Polyakova & Meserole, *supra* note 44, at 9.

48. *Id.* at 9–10.

49. *See, e.g.*, Kharitonov v. Russia, App. No. 10795/14, ¶ 6 (June 23, 2020), http://hudoc.echr.coe.int/eng?i=001-203177 (addressing Russian wholesale blocking of websites by IP address).

50. *See* Yuri Dzhibladze, *The Council of Europe Must React to Violations by Members – Starting with Russia*, OPENDEMOCRACY (June 24, 2021), https://www.opendemocracy.net/en/odr/the-council-of-europe-must-react-to-violations-by-members-starting-with-russia/.

51. *Violations by Article and by State*, EUR. CT. HUM. RTS. (2019), https://www.echr.coe.int/Documents/Stats_violation_2019_ENG.pdf.

judgments.[52] Nineteen of Russia's 2019 judgments concerned violations of Article 10.[53]

The European Court of Human Rights is commonly and internally described as the "conscience of Europe."[54] Starting in 1998, with the adoption of Protocol No. 11, any individual may bring a complaint directly to the Court after exhausting their domestic remedies.[55] After an adverse judgment from the Court, a violating state has three obligations: cease the violation, make reparations for the violation, and ensure non-repetition of similar future violations.[56] In this pursuit, the Court affords compensatory payments as well as non-pecuniary damages.[57] Punitive damages are not permitted.[58] Unlike non-pecuniary damages in the United States, the Court guides judges' non-pecuniary awards with a standardized but secret table.[59] Judges are not bound to follow this table.[60] Compensatory damages may be far larger than the relatively modest non-pecuniary damages awarded by the Court; the largest judgment ever awarded by the Court was 1.8 billion Euros in *OAO Neftyanaya Kompaniya Yukos v. Russia* in 2014.[61]

The Court faces inherent challenges when imposing such large sanctions. In *Yukos*, Russia immediately declared that it was unwilling to pay the full amount of damages.[62] Instead, only 300,000 Euros were paid by Russia for costs and expenses.[63]

---

52. *Id.*

53. *Id.*

54. ANGELIKA NUSSBERGER, THE EUROPEAN COURT OF HUMAN RIGHTS xxxv (2020).

55. Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Restructuring the Control Machinery Established Thereby art. 35, *opened for signature* May 11, 1994, E.T.S. 155 (entered into force November 1, 1998).

56. NUSSBERGER, *supra* note 54, at 161; *see also* ECHR, *supra* note 15, art. 46 ("The High Contracting Parties undertake to abide by the final judgment of the Court in any case to which they are parties.").

57. NUSSBERGER, *supra* note 54, at 161–62; ECHR, *supra* note 15, art. 50.

58. EUR. CT. HUM. RTS., RULES OF COURT 67 (2022), https://www.echr.coe.int/Documents/Rules_Court_ENG.pdf (practice note for just satisfaction claims).

59. NUSSBERGER, *supra* note 54, at 162.

60. *Id.*

61. *Id.* at 163. *See also* OAO Neftyanaya Kompaniya Yukos v. Russia, App. No. 14902/04, ¶¶ 574–75 (Jan. 17, 2012), http://hudoc.echr.coe.int/eng?i=001-145730 (holding that Russia had violated Article 1 of Protocol No. 1 through its application of unlawful tax penalties).

62. NUSSBERGER, *supra* note 54, at 164.

63. *Id.* at 179.

However, this is not the norm. "[W]ith the prominent exception of the *Yukos* case—Russia, as a rule, pays the awards of damages. The sums are considerable; in the years between 2011 and 2017 they range between 4.1 million and 14.6 million Euros."[64]

D. THE RUSSIAN SOVEREIGN INTERNET LAWS

In 2019, Russia enacted legislation dubbed "The Sovereign Internet Laws" by the media which consisted of a series of amendments to existing federal law.[65] As previously discussed, the Russian model of online control depends on a "legal regime coupled with tightening information control and intimidation of internet service providers (ISPs), telecom providers, private companies, and civil society groups" rather than filtering information before it reaches Russian citizens.[66] The Sovereign Internet Laws represent a shift to a more centralized approach with the aim of ending "the country's dependence on systems from abroad, which Russia fears could be shut down by a foreign government."[67] The Laws do so through three important changes to the Russian legal regime:

- The compulsory installation of technical equipment for countering threats[.]
- Centralized management of telecommunication networks in case of a threat and a control mechanism for connection lines crossing the border of Russia[.]
- The implementation of a national Domain Name System (DNS)[.][68]

These three amendments build directly upon Russia's existing legislative framework, providing increased control over

64. *Id.* at 178–79.

65. Epifanova, *supra* note 4, at 2.

66. Polyakova & Meserole, *supra* note 44, at 7.

67. Nadezhda Tsydenova, *Russia Plans "Sovereign Internet" Tests to Combat External Threats*, REUTERS (Dec. 19, 2019, 9:47 A.M.), https://www.reuters.com/article/us-russia-putin-internet/russia-plans-sovereign-internet-tests-to-combat-external-threats-idUSKBN1YN23Z.

68. Epifanova, *supra* note 4, at 2. *See generally What is DNS?*, AMAZON WEB SERVICES, https://aws.amazon.com/route53/what-is-dns/ (last visited May 26,S 2022) ("A DNS service . . . is a globally distributed service that translates human readable names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. The Internet's DNS system works much like a phone booth by managing the mapping between names and numbers.").

the Russian internet landscape.

First, the amendment to Article 46, clause 5 requires ISPs to install in their networks as a means to "counter threats to the stability, security and integrity of the functioning of the Russian Federation and public communications networks" and provide the federal government with information.[69] The Russian government can then use this technology "to track, filter, and reroute internet traffic."[70] "It can delay the flow of certain types of network packets while prioritizing others, giving them better performance."[71] It can thus control information and prevent its dissemination. Further, when combined with existing legislation it can "curtail opposition activity on social media sites, helping it to prevent protests such as those in 2011 through 2013 ahead of elections to Russia's parliament, the State Duma, scheduled for 2021 and the presidential election scheduled for 2024."[72]

Second, the laws amend Article 65 which covers management of public communications networks in emergencies, adding a section titled Article 65(1) which focuses on the centralization of telecommunication management under the federal government.[73] This allows the state regulatory control over internet infrastructure crossing Russian borders.[74] Critics claim this "is an attempt to enable the isolation of a national network from the global internet – for which the state can open and close 'digital borders' and determine the flow of information as it sees fit."[75] This centralized approach stands in contrast to the decentralized approach of countries like the United Kingdom and India, shifting Russia's approach further

69. FEDERAL'NYI ZAKON O VNECENII IZMENENII V FEDERAL'NYI ZAKON O SVYAZII I FEDERAL'NYI ZAKON OB INFORMATSII, INFORMATSIONNIX TECHNOLOGIYAX I O ZAZHITYE INFORMATSII [Federal Law No. 90-FZ of May 1, 2019, On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection"] art. 1(3), SZ RF 2019, No. 18, Item 2214, http://publication.pravo.gov.ru/Document/View/0001201905010025?index=0&rangeSize=1.

70. Laurel Wamsley, *Russian Lawmakers Pass Bills that Could Block Social Media Sites – and Stifle Dissent*, NPR (Dec. 23, 2020, 1:12 P.M.), https://www.npr.org/2020/12/23/949608378/russian-lawmakers-pass-bills-that-could-block-social-media-sites-and-stifle-diss.

71. Epifanova, *supra* note 4, at 3.

72. *Id.* at 2.

73. Federal Law No. 90-FZ of May 1, 2019, art. 1(5).

74. Epifanova, *supra* note 4, at 2.

75. *Id.*

toward the Chinese model of state control.[76] The law creates a control mechanism for lines crossing Russia's border, giving the state the potential to create a kill-switch, a mechanism that could isolate and shut down parts of the Russian internet and silence dissent.[77]

Finally, the addition of Article 14(2) calls for the creation of a national DNS.[78] This would provide Russia with its own internet infrastructure and domain names, regulated by the Russian government through Roskomnadzor, its federal agency overseeing media, information technology, and telecommunications.[79] This is an unprecedented step which if fully implemented would make Russia the first country with its own proprietary DNS, independent from the International Corporation for Assigned Names and Numbers (ICANN). As explained by Alena Epifanova, "A national DNS would only make sense if a country opts for a long-term and complete isolation of its internet."[80] If this were to come to fruition, Russian websites would be segregated from the international DNS.[81] Russian websites would be unavailable internationally, and Russians would likely not have access to the global DNS.[82]

The Chairman of Russia's Committee on Informational Policy, Leonid Levin, disagrees with the media's "sovereign internet" label, stating, "It's more about creating a reliable internet that will continue to work in the event of external influences, such as a massive hacker attack."[83] Russia has also cited what it calls the "aggressive nature" of the United States' cyber security strategy.[84] President Vladimir Putin himself addressed this issue, claiming that a free internet and a sovereign internet were not contradictory.[85] He stated, "The law is aimed at just one thing – preventing negative consequences of being disconnected from the global network, the management of which is mostly abroad . . . .We are not moving toward closing

76. *Id.* at 3–4.
77. *Id.* at 6–7.
78. Federal Law No. 90-FZ of May 2, 2019, art. 2.
79. *See* Epifanova, *supra* note 4, at 7.
80. *Id.* at 8.
81. *Id.*
82. *Id.*
83. Jan Lindenau, *Russia's Sovereign Internet Law Comes into Force*, MOSCOW TIMES (Nov. 1, 2019), https://www.themoscowtimes.com/2019/11/01/russias-sovereign-internet-law-comes-into-force-a68002.
84. Tsydenova, *supra* note 67.
85. *Id.*

the internet and do not intend to do so."[86] Despite their assurances, these laws represent a substantial development in a repressive legal regime that has already been found to be in violation of Article 10 of the European Convention on Human Rights.[87] They will undoubtedly need to be addressed by the European Court of Human Rights.

II. ANALYSIS

A. COMPLIANCE WITH RUSSIA'S OBLIGATIONS UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS

If implemented as written, the Sovereign Internet Law would almost certainly be viewed as an Article 10 violation by the European Court of Human Rights. In 2020, the Court found in multiple cases that Russia had violated Article 10 through blocking internet content and regulating social media.[88] The Court's most recent decisions on Russian internet censorship are best illustrated through examination of four cases: *Bulgakov v. Russia*, *Engels v. Russia*, *Kharitonov v. Russia*, and *Kablis v. Russia*.

In the 2020 case *Bulgakov v. Russia*, a Russian court had implemented a blocking order in 2012 targeting "extremist content" that had the effect of blocking access to the entire website of a Russian national, Yevgeniy Vladimirovich Bulgakov.[89] Citing Russia's anti-extremist laws, specifically section 10(6) of the Information Act, the Russian court required the regional ISP to block Bulgakov's site as it contained a pamphlet and an e-book in its file section, and both had previously been categorized as extremist content.[90] Bulgakov was not a party to that suit.[91] Once he discovered that the local ISP had blocked access to his site by order of the local court, Bulgakov removed the files and appealed in an attempt to regain access to his website.[92] Ultimately, and without examining his evidence, the appellate court dismissed his appeal and held that

86. *Id.*
87. *See, e.g.*, *Kharitonov*, App. No. 10795/14, ¶ 47.
88. *See, e.g.*, *id.*; *Bulgakov*, App. No. 20159/15, ¶ 40.
89. *Bulgakov*, App. No. 20159/15, at 1.
90. *Id.* ¶ 5.
91. *See id.* ¶ 6.
92. *Id.*

it had not been shown that the e-book had been removed.[93] After exhausting his domestic legal options, Bulgakov took his case to the European Court of Human Rights.

In its analysis of whether Russia had violated Article 10, the Court made plain that Article 10's guarantee of the freedom to receive and impart information and ideas applies not only to the content of information, but to the means by which it is disseminated.[94] In doing so, it stated "that measures blocking access to websites are bound to have an influence on the accessibility of the Internet and, accordingly, engage the responsibility of the respondent State under Article 10[.]"[95] As such, the prevention of visitors from visiting Bulgakov's website constituted interference by a public authority with the right to receive and impart information under Article 10 § 1, and was thus subject to analysis under Article 10 § 2.[96] The Court explained, "Interference will constitute a breach of Article 10 unless it is 'prescribed by law,' pursues one or more of the legitimate aims referred to in Article 10 § 2 and is 'necessary in a democratic society' to achieve those aims."[97]

The Court interpreted the "prescribed by law" standard of Article 10 § 2[98] to require not only that an action have a statutory basis, but that it is both "accessible and foreseeable" enough that an individual is able to ascertain the consequences an action may entail.[99] It would be contrary to this standard for a law to grant the executive "unfettered power . . . the law must provide protection against arbitrary interference by public authorities[,]" as well as indicate the scope of authorities' discretion the manner of their exercise.[100] Although the Russian court order had a basis in domestic law, it did not restrict its blocking order to the banned content, but instead blocked the entire IP address.[101] Despite having no basis in law, this method has been used in thousands of Russian cases.[102]

The Court compared the act of banning access to an entire

93. *Id.*
94. *Id.* ¶ 28.
95. *Id.* ¶ 29.
96. *Id.* ¶¶ 29–30.
97. *Id.* ¶ 30.
98. ECHR, *supra* note 15, art. 10.
99. *Bulgakov*, App. No. 20159/15, ¶ 31.
100. *Id.* at 9.
101. *Id.* ¶ 33.
102. *Id.*

website to banning an entire newspaper or television station, and explained that "[s]uch a measure deliberately disregards the distinction between the legal and illegal information the website may contain, and renders inaccessible large amounts of content which has not been designated as illegal."[103] This directly reflects the Council of Europe's discouragement of general blocking or filtering measures in The Declaration on Freedom of Communication on the Internet.[104] Further, the law did not provide necessary protections to protect individuals from excessive and arbitrary effects of blocking orders, as it did not require the website owner's involvement in blocking proceedings, did not require he be provided with advance notice, did not afford him the opportunity to remove the illegal content, and did not invite him to intervene or make submissions in the action between the prosecutor and local ISP.[105] The law did not meet the Court's transparency standard, and the Russian court did not properly "consider whether the same result could be achieved through less intrusive means."[106] For these reasons, the Court held that the application of the law, section 10(6) of the Information Act, did not meet the "prescribed by law" standard and thus the action constituted a violation of Article 10 of the Convention.[107]

When the Court employed the same standard and line of analysis in the 2020 case *Engels v. Russia*, it provided additional commentary on what constitutes an "arbitrary effect in practice," in violation of the "prescribed by law" standard and thus Article 10 of the Convention.[108] Here, in 2015 Roskomnadzor had threatened to block the IP address of an internet freedom activist in Russia who provided news, information, and research regarding freedom of online expression in Russia, because one page of his site contained information on tools to bypass internet restrictions, such as VPNs.[109] Engels was forced to remove the page, as the government deemed that the VPNs could be used to access

103. *Id.* ¶ 34.
104. Comm. of Ministers, *supra* note 3.
105. *Bulgakov*, App. No. 20159/15, ¶ 35.
106. *Id.* ¶ 37.
107. *Id.* ¶ 40.
108. Engels v. Russia, App. No. 61919/16, ¶¶ 24–34 (June 23, 2020), http://hudoc.echr.coe.int/eng?i=001-203180.
109. *Id.* ¶¶ 4–7.

extremist content on other pages.[110] The Court found that this justification illustrated the manner in which the law was capable of producing an arbitrary effect in practice.[111] Finding a violation, the Court made clear that VPNs provide a host of legitimate purposes, and that information technologies are content-neutral and cannot be equated with the content they are used to store and access.[112]

The Court in the 2020 case *Kharitonov v. Russia* assessed an action with broader effect than *Bulgakov* or *Engels*: in 2012 the Russian government blocked a cluster of multiple websites hosted under the same IP address due to the content of one.[113] In this case, an electronic publishing website was blocked as it was hosted on the same United States-based web-host—and thus had the same IP address—as a website called "The Rastaman Tales" which hosted a collection of cannabis-themed folk stories.[114] The Court held that the enabling law, Section 15.1 of the Information Act, had failed to "require Roskomnadzor to check whether [the] address was used by more than one website or to establish the need for blocking by IP address."[115] Noting that millions of websites in Russia have remained blocked solely for sharing an IP address with another website containing illegal conduct, the Court found that the law was not sufficiently foreseeable in its effects and did not "afford the applicant the degree of protection from abuse to which he was entitled by the rule of law in a democratic society."[116]

Finally, in the 2019 case *Kablis v. Russia*, surrounding the decision by his town to deny his permit to hold a protest, Mr. Kablis made three blog posts and a VKontakte post calling for a public assembly and public discourse.[117] By government order, his VKontakte account and his three blog posts were blocked.[118] Assessing his Article 10 claims, the Court focused on the phrase "necessary within a democratic society" within Article 10 § 2, and stated that it implied a "pressing social need."[119] The Court

110. *Id.* ¶ 6.
111. *Id.* ¶ 28.
112. *Id.* ¶¶ 29–30.
113. *Kharitonov*, App. No. 10795/14, ¶ 5.
114. *Id.* ¶¶ 5–6.
115. *Id.* ¶ 41.
116. *Id.* ¶ 46 (citation omitted).
117. Kablis v. Russia, App. Nos. 48310/16 & 59663/17, ¶¶ 6–9 (June 23, 2020), http://hudoc.echr.coe.int/eng?i=001-192769.
118. *Id.* ¶¶ 12–14.
119. *Id.* ¶ 82.

found no pressing social need to block the content, as the aim of the event was to express an opinion on an issue of public interest, the event permit was denied on formal grounds rather than due to a risk of public safety, and the posts did not contain calls for violence or disorderly acts.[120]

The Sovereign Internet Laws consist of three amendments to Russian law: 1) compulsory installation of threat-countering equipment, 2) centralized federal management of telecommunication networks and a control mechanism for connection lines crossing Russia's border, and 3) implementation of a national DNS.[121] These changes would only serve to heighten its ability to inhibit Russian inhabitants' access to information on the internet.[122] If fully exercised, the Sovereign Internet Laws would prevent visitors from accessing information on the internet, much like the aforementioned cases, but on a much larger scale.[123] Preventing internet users within Russia from accessing information would constitute interference by a public authority and bring the action within the domain of Article 10.

The actual application of the Article 10 standard as applied in the aforementioned cases would inherently depend on how the Russian authorities employed the Sovereign Internet Laws. This has not prevented experts in Russia and abroad from recognizing the amendments' potential for abuse. The amendment to Article 46 clause 5,[124] which provides for the compulsory installation of threat countering equipment, would provide Roskomnadzor with greater ability to track, filter, and reroute internet traffic.[125] By "delay[ing] the flow of certain types of network packets[,]"[126] the technology enables the authorities to prevent the dissemination of information and "curtail

120. *Id.* ¶¶ 104–07.

121. FEDERAL'NYI ZAKON O VNECENII IZMENENII V FEDERAL'NYI ZAKON O SVYAZII I FEDERAL'NYI ZAKON OB INFORMATSII, INFORMATSIONNIX TECHNOLOGIYAX I O ZAZHITYE INFORMATSII [Federal Law No. 90-FZ of May 1, 2019, "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection"], SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOĬ FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2019, No. 18, Item 2214, http://publication.pravo.gov.ru/Document/View/0001201905010025?index=0&rangeSize=1.

122. *See* Epifanova, *supra* note 4, at 9.

123. *See id.*

124. Federal Law No. 90-FZ, art. 1.

125. *Id.*; Wamsley, *supra* note 70.

126. Epifanova, *supra* note 4, at 3.

opposition activity on social media[.]"[127] If used in this manner, the Court would likely assess such actions under the "pressing social need" standard demonstrated in *Kablis v. Russia*.[128] In that case, the Court demonstrated its commitment to public discourse and peaceful assembly and found a violation for filtering content aimed at organizing events to express opinions on topical issues of public interest.[129]

The amendment to Article 65 allows the state regulatory control over internet infrastructure crossing Russian borders, and creates a legal basis to refuse to direct traffic through it.[130] The creation of this control mechanism provides the state with the potential to create a "kill-switch, a . . . mechanism that could" isolate and "shut down most of the Russian internet" and silence dissent.[131] As evidenced by the Court's application of the "prescribed by law" standard in *Bulgakov*, *Engels*, and *Kharitonov*, this would likely constitute a violation for lack of protections against arbitrary enforcement.[132] Much like Russia's application of the Information Act in these cases, Article 65 does not require prior notice or involvement of affected individuals in any proceedings before their access is blocked.[133] A kill-switch would also run directly contrary to the Council of Europe's discouragement of general blocking or filtering measures in The Declaration on Freedom of Communication on the Internet.[134]

These issues are only exacerbated if the Sovereign Internet Laws' final amendment is fully implemented: the addition of Article 14(2) which calls for the creation of a national DNS.[135] This would provide Russia with its own internet infrastructure and domain names, regulated by the Russian government through Roskomnadzor, and separate from ICANN.[136] Russian websites would be unavailable internationally, thereby preventing Russian citizens from imparting information.[137]

---

127. *Id.* at 2.
128. *See Kablis*, App. Nos. 48310/16 & 59663/17, ¶ 82.
129. *See id.* ¶ 104.
130. *See* Epifanova, *supra* note 4, at 2; Federal Law 90-FZ, art. 1.
131. Epifanova, *supra* note 4, at 7.
132. *See, e.g.*, *Bulgakov*, App. No. 20159/15, ¶ 35.
133. *See* Federal Law 90-FZ, art. 1.
134. *See* Comm. of Ministers, *supra* note 3.
135. Federal Law 90-FZ, art. 2.
136. Epifanova, *supra* note 4, at 7–8.
137. *See* ECHR, *supra* note 15, art. 10 ("This right shall include freedom to hold opinions and to receive and *impart information* and ideas without interference by public authority and regardless of frontiers.") (emphasis added).

If, as a result, Russians were to lose access to the global DNS, this would not only restrict their freedom to impart information, but their freedom to receive it from the global community as well. As the Court has found violations of Article 10 § 2's "prescribed by law" and "necessary in a democratic society" standards for Russian blocking of lone IP addresses,[138] blog posts, and social media accounts,[139] a blocking and filtering regime of this scale would almost certainly run afoul of Article 10's protections. Thus, if Russia implements the Sovereign Internet Laws in a similar manner to how it has utilized prior legislation, these acts would likely be viewed as an Article 10 violation by the Court.

B. HOW THE EUROPEAN COURT OF HUMAN RIGHTS MAY ADDRESS RUSSIA'S ACTIONS.

The European Court of Human Rights has multiple options regarding how to address the Russian government's growing censorship of the internet: it could choose to continue with its current system of enforcement, reform its remedy rules to raise the cost of violations or suspend Russia's membership rights to the Council of Europe.

Its current system of enforcement is by no means sympathetic to Russia. The Court has already dedicated a large portion of its focus to addressing Russian human rights issues; in 2019, the Court levied more adverse judgments against Russia than it did against any other member state.[140] Further, its awards of monetary damages to the victims of these violations are largely paid by Russia.[141] Yet, the damage awards in online freedom of expression cases are by their nature often limited to non-pecuniary damages[142] which are guided by a secret but standardized table maintained by the Court.[143] The aforementioned cases *Bulgakov* and *Engels* each resulted in a non-pecuniary damage award for their applicant of 10,000 Euros.[144] Nearly eight years after his website was blocked, the

138. *See Bulgakov*, App. No. 20159/15, ¶ 34.
139. *See Kablis*, App. No. 48310/16, ¶ 84.
140. *Violations by Article and by State*, *supra* note 51.
141. NUSSBERGER, *supra* note 54, at 178–79.
142. *E.g.*, *Kharitonov*, App. No. 10795/14, ¶ 61.
143. NUSSBERGER, *supra* note 54, at 162.
144. *Bulgakov*, App. No. 20159/15, ¶ 53; *Engels*, App. No. 61919/16, ¶¶ 46–48.

Kharitonov applicant was also awarded 10,000 Euros in non-pecuniary damages, supplemented by a 2,000 Euro award for costs and expenses.[145] The largest award among the four, the *Kablis* case resulted in a 12,500 Euro non-pecuniary damage award for its applicant, supplemented by a 2,500 Euro award for costs and expenses.[146]

Any proposed reform to the Court's current remedy system would thus need to deal with a key policy issue: weighing the competing priorities of affording individual applicants with some measure of just compensation, or further deterring Russian human rights violations.[147] The Court's adverse judgments against Russia for its attacks on internet freedom have not stopped Russia from implementing laws that are directly contrary to the obligations of the Convention. Despite the repeated adverse judgments against Russia in 2019,[148] it still enacted the Sovereign Internet Laws.[149] Although an extreme example, Russia's unwillingness to pay a 1.8 billion Euro damage award in *Yukos* indicated that there is an upper limit to what Russia is willing to pay in the event of an adverse judgment, and has raised questions about precisely how high that limit is.[150] Further, there has been debate among member states about whether to withdraw from the Convention, viewing the Court as intruding upon national sovereignty.[151]

Still, the Sovereign Internet Laws carry with them far-reaching implications for the future of Russian internet, that unless curbed before fully implemented could potentially result in Russian citizens being completely cut off from the greater

145. *Kharitonov*, App. No. 10795/14, ¶ 61.

146. Kablis v. Russia, App. Nos. 48310/16 & 59663/17, ¶¶ 111, 114 (June 23, 2020), http://hudoc.echr.coe.int/eng?i=001-192769.

147. *See generally* Veronika Fikfak, *Changing State Behaviour: Damages Before the European Court of Human Rights*, 29 EUR. J. INT'L L. 1091, 1097–1102 (2018) (discussing the tension between just satisfaction and the enforceability of the Court's judgments).

148. *Violations by Article and by State*, *supra* note 51.

149. *See* FEDERAL'NYI ZAKON O VNECENII IZMENENII V FEDERAL'NYI ZAKON O SVYAZII I FEDERAL'NYI ZAKON OB INFORMATSII, INFORMATSIONNIX TECHNOLOGIYAX I O ZAZHITYE INFORMATSII [Federal Law No. 90-FZ of May 1, 2019, "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection"] art. 3, SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOĬ FEDERATSII SZ RF 2019, No. 18, Item 2214, http://publication.pravo.gov.ru/Document/View/0001201905010025?index=0&rangeSize=1.

150. *See* NUSSBERGER, *supra* note 54, at 163–64.

151. *See id.* at 2–3 n.9 (explaining that Switzerland and the United Kingdom have contemplated effectively leaving or denouncing the Convention).

World Wide Web, "in whole or in parts."[152] According to Alena Epifanova, if the laws were fully realized, Russia could potentially partner with China, or other states, and create a "splinternet," where parts of the internet are controlled and regulated by different states.[153] Even if its bid for a national DNS proves unsuccessful, its system of tightening information control, repressive legal regime, and willingness to intimidate ISPs and private companies[154] is very much operational.[155] If left unchecked, this low-cost alternative to China's heavy-handed approach may prove to be a model for other authoritarian regimes around the globe.[156] The Russian model of internet control is well-suited for other countries where a more robust censorship approach may not be feasible.[157]

The Court should therefore prepare itself now by strongly adjusting its internal damage calculations when addressing Russian internet censorship in order to reflect Russia's increasingly authoritarian measures.[158] Although there are valid questions regarding their limits, monetary damages have largely been the tool that has elicited the most compliance among the member states, as the Court's attempts to go beyond monetary damages have been commonly met with non-compliance.[159] The Court is presently limited by its practice directions, which ban punitive damages.[160] Practice directions are issued by the President of the Court, and may be amended

152. Polyakova & Meserole, *supra* note 44, at 7.

153. Epifanova, *supra* note 4, at 3, 9.

154. Dylan Myles-Primakoff & Justin Sherman, *Russia's Internet Freedom Shrinks as Kremlin Seizes Control of Homegrown Tech*, FOREIGN POL'Y (Oct. 26, 2020, 1:58 P.M.), https://foreignpolicy.com/2020/10/26/russia-internet-freedom-kremlin-tech/ (explaining how Russia has worked to pressure private companies such as VKontakte, Facebook, and Twitter).

155. *See* Polyakova & Meserole, *supra* note 44, at 8–10.

156. *Id.* at 7.

157. *See* Kerr, *supra* note 26, at 71.

158. *See* Pollicino & Soldatov, *supra* note 35, at 98.

159. *See* Fikfak, *supra* note 147, at 1094 ("Although no similar study has been undertaken for the ECtHR, which issues non-monetary remedies much more reluctantly than the IACtHR, judges themselves insist that the Court faces the same issue with compliance as its inter-American counterpart.").

160. EUR. CT. HUM. RTS., *supra* note 58, at 67 ("The purpose of the Court's award in respect of damage is to compensate the applicant for the actual harmful consequences of a violation. It is not intended to punish the Contracting Party responsible. The Court has therefore, until now, considered it inappropriate to accept claims for damages with labels such as 'punitive', 'aggravated' or 'exemplary.'").

as they see fit.[161] Through its ban on punitive damages, the Court is preventing itself from raising the monetary cost of violations and is limiting its ability to express righteous anger through punishment.[162] Both increased monetary costs and the expressive power of adjudication are powerful incentives for cooperative state behavior.[163]

As compliance with Court decisions is voluntary, if the practice directions were reformed to increase damage awards through punitive damages, it may not always result in paid damages, but "may nevertheless encourage states to conduct a cost-benefit analysis and conclude that it is best to get rid of structural/systemic problems than to continue the violation."[164] This proposal is not without support among members of the Court. In a concurring opinion in *Cyprus v. Turkey*, Judge Pinto De Albuquerque explained:

> [T]he Court has been at the forefront of an international trend, using just satisfaction to prevent further violations of human rights and punish wrongdoing governments. The acknowledgment of punitive or exemplary damages under the Convention is essential in at least three cases: (1) gross violations of human rights protected by the Convention or the additional Protocols, especially when there are multiple violations at the same time, repeated violations over a significant period of time or a single continuing violation over a significant period of time; (2) prolonged, deliberate non-compliance with a judgment of the Court delivered with regard to the recalcitrant Contracting Party; and (3) the severe curtailment, or threat thereof, of the applicant's human rights with the purpose of avoiding, impairing or restricting his or her access to the Court as well as the Court's access to the applicant.[165]

He also noted that an openness to punitive damages has been similarly signaled in statements by the Council of Europe's

---

161. EUR. CT. HUM. RTS., RULES OF COURT 32 (2022), https://www.echr.coe.int/documents/rules_court_eng.pdf.

162. *See* Fikfak, *supra* note 147, at 1106.

163. *See id.* at 1102–07.

164. *Id.* at 1125.

165. Cyprus v. Turkey, 2014-II Eur. Ct. H.R. 245, 287 (citations omitted).

Committee of Ministers.[166] The Parliamentary Assembly of the Council of Europe also considered imposing punitive fines on states that "persistently fail to execute judgments of the Court."[167] Although these recommendations have not yet resulted in a change to the Court's practices, they reflect a political appetite for such an amendment.

For now, Russia is able to pay the Court's low fees and treat the issues as resolved.[168] "Russian legislation explicitly requires that the country's annual budget contains a part intended to pay off ECHR violations. Between 2010 and 2016, the amount 'reserved' for ECHR compensation was respectively 114 million rubles (US$1.7 million) and 500 million rubles (US$7.6million)."[169] With Russia able to predict the monetary cost of its human rights violations, it has little incentive to change its conduct.

There is still time for the Court to act; although the Sovereign Internet Laws took effect on November 1, 2019, they have had a limited direct effect on Russian internet users because the technology to fully implement them had not been fully developed at time of passage.[170] A stronger stance on damages would signal to Russia that its legal trajectory would have real political consequences in the international community. If Russia were to then fail to abide by the Court's final judgments, it could be subjected to an Article 46 procedure, whereby the Committee of Ministers would refer to the Court the question of whether Russia failed to fulfill its obligations.[171] This rarely-used procedure could be understood as a precursor to suspension of membership rights under Article 8 of the

166. *Id.* at 286 ("In the Council of Europe, the Committee of Ministers noted that 'the setting up of a merely compensatory or acceleratory remedy may not suffice to ensure rapid and full compliance with obligations under the Convention, and . . . further avenues must be explored, e.g. through the combined pressure of various domestic remedies (punitive damages, default interest, adequate possibility of seizure of state assets, etc.) . . . .' This clear stance in favour of punitive damages taken by the highest political body of the Council of Europe was not an isolated case.'").

167. Paulo Pinto de Albuquerque & Anne van Aaken, *Punitive Damages in Strasbourg*, *in* THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND INTERNATIONAL LAW 230, 239 (Anne van Aaken & Iulia Motoc eds., 2018).

168. *See* Veronika Fikfak, *Non-Pecuniary Damages Before the European Court of Human Rights: Forget the Victim; It's All About the State*, 33 LEIDEN J. INT'L L. 335, 361 (2020).

169. *Id.*

170. *See* Lindenau, *supra* note 83.

171. *See* ECHR, *supra* note 15, art. 46.

Statute of the Council of Europe.[172]

However, suspending Russia's membership rights would be a drastic political move with consequences for human rights in the country. Consistent with Russia's explicit obligation under the Russian Constitution to comply with the decisions of the European Court of Human Rights,[173] the Court has had real success with influencing human rights conditions in Russia. On the 20th anniversary of Russia's membership in the Council of Europe in 2018, the Council published a list of 20 important cases that had changed the Russian legal system.[174]

Among them was the 2005 case of *Greenberg v. Russia* in which the Court found an Article 10 violation after an individual was held liable for expressing a value judgment: an opinion that could neither be proven or disproven with facts.[175] This distinction influenced subsequent Russian Supreme Court rulings, "evolve[ing] towards greater respect of value judgments in public debate."[176] Rather than alienate Russia through the removal process, the Court should instead maintain its influence in the country yet further challenge Russia to reverse its course of action.

CONCLUSION

Since the early 2010s, Russia has crafted a legislative framework that subtly undermines the ability of Russian citizens to impart and receive information through the internet. When it enacted the Sovereign Internet Laws in 2019, Russia signaled its intent to take a large step forward on the path to an authoritarian level of online content and access control. By installing ISP devices that can sever connections, controlling the flow of digital information at the country's border, and developing a global DNS, Russia is positioning itself to have complete control over its citizens' online connectivity, and potentially cut them off from the global DNS entirely.

---

172. *See* NUSSBERGER, *supra* note 54, at 160.

173. BUTLER, *supra* note 12, at 107; *see also* KONST. RF art. 15(4).

174. *See* Yu Berestnev, *Russia and the European Convention on Human Rights: 20 Years Together: 20 Cases that Have Changed the Russian Legal System*, 2018 CASE-L. EUR. CT. HUM. RTS., Special Issue 5'2018, https://rm.coe.int/russia-and-the-european-convention-on-human-rights-20-years-together-b/16808b3b38.

175. *Id.*

176. *Id.*

The European Court of Human Rights has directly addressed Russian online censorship in the past; yet its condemnations have done little to deter Russian development on this front. The Court's adverse judgments against Russia for its attacks on internet freedom have not stopped Russia from implementing laws that are directly contrary to the obligations of the Convention. This Note proposes that the Court amend its internal practices in order to raise the monetary damages for violations of Article 10 through the use of punitive damages and increase the cost to Russia for its repeat transgressions. Should Russia utilize the Sovereign Internet Laws to further censor online expression in the country, the Court should recognize these acts as a violation of Article 10 and apply these punitive damages accordingly.