THE EUROPEAN COURT OF HUMAN RIGHTS: INTERNET ACCESS AS A MEANS OF RECEIVING AND IMPARTING INFORMATION AND IDEAS

Gergely Gosztonyi

Eötvös Loránd University (ELTE), Hungary
E-mail: gosztonyi@ajk.elte.hu

Received: 1 November 2020; accepted: 16 November 2020
DOI: http://dx.doi.org/10.13165/j.icj.2020.12.003

Abstract. "The Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas." (European Court of Human Rights, cited in Cengiz and Others v. Turkey). Are these rights merely window dressing for some countries? Perhaps the most important question is what lies behind this so-called Potemkin village that is very much in evidence? For example, in 2019 there were at least 213 documented internet shutdowns around the world, with the number of countries experiencing shutdowns increasing from 25 in 2018 to 33 in 2019 – or 17% of the countries in the world today. In this respect, Russian and Turkey are standouts as landmark cases that have come before the European Court of Human Rights (ECtHR). Here, the fundamental issue is blocking access to the Internet, regardless of the methods used by each State. This paper examines the use of shutdowns in Russia and Turkey with a view to understanding how these States in particular are responding to the propagation of fake news, hate speech, content that promotes violence, and how to balance drastic measures (shutdowns) with the need to ensure public safety and/or national security and freedom of expression.

Keywords: freedom of expression, media, human rights, internet shutdown, collateral blocking, excessive blocking, wholesale blocking

Introduction

It is generally accepted that the Internet has impacted our lives in many different ways, and not only in providing ready access to an astonishing amount of information, but also in dislodging old notions of the State, the economy, education, and our personal relations and anxieties about the world today. "Out of all the plethora of communication opportunities that the Internet has opened up, I would highlight the emergence of social media and the way they have intricately melded into our daily lives. Social media have changed our personal space, altering the way we interact with our loved ones, our friends, and our sexual partners; they have forced us to rethink even basic daily processes like studying and shopping; they have affected the economy by nurturing

---

1 Ph.D., Hungarian lawyer and media researcher. He was awarded a Ph.D. in Media Law from the Faculty of Law, Eötvös Loránd University (ELTE) Budapest, where he has taught since graduation. Particular research interests are censorship, alternative media and the liability of intermediaries. He studied sociology and political sciences for one year in Finland and media law for six months in Denmark. Between 2000-2004 he was the office coordinator of the Hungarian Federation of Free Radios and between 2004-2006 he was the managing director of Civil Radio FM98, a community radio in Budapest. From 2010-2017 he was the Head of the Rector's Cabinet of Eötvös Loránd University. He is a member of the European Communication Research and Education Association. Since 2015 he has been the coach of the Hungarian Team for the yearly Monroe E. Price Media Law Moot Court Competition.

2 Any literal or figurative construction whose purpose is to provide an external façade to a country which is faring poorly, the intention being to make people believe that the country is better. The term comes from stories of a fake portable village built solely to impress Empress Catherine.
business startup culture and electronic commerce; they have even given us new ways to form broad-based political movements." (Dentzel, 2014; Gelernter et al., 2014).

The Internet has also raised numerous legal questions concerning media law, security, big data, fake news, privacy, and human rights. How can people feel protected against the threats posed by the Internet when they go online? As ECtHR stated in Cengiz and Others v. Turkey: "the Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas." (Cengiz and Others v. Turkey, 2015, 49). Indeed, the Internet has become not only the primary tool used to communicate, but also a platform where (at least it seemed at first glance) the ideas espoused by the nineteenth century English economist, John Stuart Mill, in his 'Marketplace of Ideas' (Gordon, 1997) would become reality. Again, according to ECtHR, "the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. User generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression." (Cengiz and Others v. Turkey, 2015, 52).

Such a worthy and honourable vision of what might have been has turned out to be something else. In 2017 Nils Mužnieks, who was then Commissioner for Human Rights for Council of Europe, wrote that "Internet blocking is a widespread phenomenon in Council of Europe Member States." (Council of Europe, 2018) Over the last three years the situation has continued to deteriorate, hence it is useful to examine to what extent it is possible to enjoy freedom of access to Internet as a mean of receiving and imparting information and ideas. Further, what legal avenues are available to resist the growing incidence of the use of this measure by certain States to block their own citizens from accessing information?

1. Overview of Historical and Technical Background

In the UNHRC 2011 annual report, the UN Special Rapporteur spoke on the promotion and protection of the right to freedom of opinion and expression: "some of the ways in which States are increasingly censoring information online, namely through: arbitrary blocking or filtering of content; criminalization of legitimate expression; imposition of intermediary liability; disconnecting users from Internet access, including on the basis of intellectual property rights law; cyber attacks; and inadequate protection of the right to privacy and data protection." (UNHRC, 2011, Summary) The report mentioned various measures and attempts by States to prevent contents from reaching the end user, which includes:

- denying users access to specific websites, Internet Protocol (IP) addresses, domain name extensions
- removing websites from the web server where they are hosted
- using filtering technologies to exclude pages containing keywords or prevent specific content from loading.

Removing or preventing access to existing content is problematic and just one aspect of the question. We should state that without Internet connection the marginalised groups of any given society remain even more marginalised and this one also applied to less-developed States. "The Internet offers a key means by which such groups can obtain information, assert their rights, and participate in public debates concerning social, economic and political changes to improve their situation." (UNHRC, 2011, Summary) How to manage the digital divide among States in the world (and also among different groups in a State) is a vexed question and has caught the attention of world leaders. For example, see the Plan of Action adopted at the 2003 Geneva World Summit on the Information Society, and Connect the World adopted at the 2005 International Telecommunication Union's Forum.

Perhaps the most pressing question is what is the reality behind the Potemkin-village that some countries have adopted? The #KeepItOn report (AccessNow, 2020) on internet shutdowns in 2019 is cause for concern. “From
Bolivia to Malawi, India, Sudan, and beyond, 2019 was a difficult year, both online and off. The #KeepItOn coalition has documented an increase in shutdowns in 2019, as well as a trend toward sustained and prolonged shutdowns, and targeted internet shutdowns.” (AccessNow, 2020, 1.) In fact, around the world in 2019 there were at least 213 documented shutdowns, with the number of countries involved rising from 25 in 2018 to 33 in 2019. This figure represents 17% of the world's countries, which begs the question: how many countries are there in the world today that used this measure, as of 2020? The top three on the list comprise India, Venezuela and Yemen, yet not only authoritarian regimes or countries in transition blocked the Internet. In 2019 there were at least five Internet shutdowns in Europe (AccessNow, 2020, 2.) It is well to remember that the aforementioned instances of shutdown is not only of short duration; 16% of the documented 213 cases lasted for more than seven days.

Even where a State has been unable to shut down the Internet within its geographical borders, it has used other means to achieve much the same. One avenue is to restrict bandwidth which effectively slows down Internet traffic, while others target only social media sites, both methods disrupting the free flow of information. Ascertaining the real number of shutdowns and/or slowdowns is almost impossible. In 2019, the governments that form the subject of this study acknowledged only 116 shutdowns from a monitored 213, or 54%. Their stated legal aims included: "fighting fake news, hate speech, or content promoting violence, public safety, national security, third-party actions, school exams." (AccessNow, 2020, 13.) The States also used the excuse of the growing number of technical problems, although observers and critics dispute this assertion, believing that the real reasons are quite different, and relate mainly to: protest, violence, and elections or political instability. According to the report it seems that in exceptional circumstances, e.g. elections, military actions, religious holidays, visits by government officials, the States tend to use extraordinary (non-regular) measures to thwart open criticism of real and/or imagined problems. Precautionary measures, a somewhat bureaucratic term, "are almost always used by the Indian government to justify shutting down the Internet in situations of military action, such as in Jammu and Kashmir" (AccessNow, 2020, 13.).

2. Landmark Cases of the European Court of Human Rights

Article 10 of the European Convention on Human Rights (Council of Europe, 1952) states that "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." Article 10 goes on to say that this right may be subject to formalities, conditions, restrictions or penalties, yet it should be compatible with the three-part-test of the ECtHR. That means that the contested measures should not be arbitrary: the interference "(a) should be suitable to achieve the legitimate aim pursued (suitability or legitimacy), (b) should be the least intrusive instrument (necessity), and (c) should be strictly proportionate to the legitimate aim pursued (proportionality sensu stricto)." (Oster, 2015).

In this particular matter, the landmark cases of the ECtHR apply to two countries: Russia and Turkey (Ahmet Yildirim v. Turkey, 2012); (Akdeniz v. Turkey, 2014); (Bulgakov v. Russia, 2020); (Cengiz and Others v. Turkey, 2015); (Elvira Dmitriyeva v. Russia, 2019); (Engels v. Russia, 2020); (Kablis v. Russia, 2019); (OOO Flavus and Others v. Russia, 2020); (Vladimir Kharitonov v. Russia, 2020). The basic issue in all these cases is the blocking of access to the Internet, although the States used different methods. In some cases, we find collateral blocking (several sites including the one targeted shared the IP address that was blocked), excessive blocking (the entire website was blocked due to a single page or file deemed unacceptable), or wholesale blocking (all, or part of the Internet was blocked). In most instances, the ECtHR found that the measure taken

---

3 That is still an increase from the number of 81 in 2018.
4 It should be noted that a different aspect to examine the question would be the restrictions placed on prisoner's access to the Internet, see (Kalda v. Estonia, 2016); (Jankovskis v. Lithuania, 2017).
violated Article 10 of the European Convention on Human Rights (ECHR) as they mostly failed the necessity and/or the proportionality part of the above-mentioned test.

2. 1. Akdeniz v. Turkey

Somewhat different from other cases that follow in this paper is the matter of Akdeniz v. Turkey, 2014), although since it pertains to admissability we will describe it first. Thus, in June 2009 the media division of Turkey’s public prosecutor's office ordered the blocking of access to the websites myspace.com and last.fm on the grounds that these sites were in breach of copyright through the dissemination of musical works. The applicant had lodged their application as a user of those websites, the main question being: who could be a 'victim' of an internet blocking? In 2014 the ECtHR declared the application inadmissible (incompatible ratione personae) on the grounds that since the applicant had been indirectly affected by a blocking measure, there was insufficient evidence they could be regarded as a 'victim'. As the ECtHR stated "the fact that the applicant had been deprived of access to those websites had not prevented him from taking part in a debate on a matter of general interest" (Akdeniz v. Turkey, 2014), which means that if one could obtain the needed information (in this particular case, music) from different sources, it might justify the State’s use of some form of restrictions.

2. 2. Ahmet Yildirim v. Turkey

The Denizli Criminal Court of First Instance blocked all access to Google sites under the Turkish law, and this interim injunction was promulgated in a criminal proceeding against the owner of a website hosted by Google (Ahmet Yildirim v. Turkey, 2012). The problem was that this given site contained content that was alleged by the State found offensive to the memory of the father of the nation, Mustafa Kemal Atatürk, who established the modern State of Turkey in 1923. Ahmet Yildirim, a Turkish student, also ran a website at Google, so that the above-mentioned blocking also affected his domain. The ECtHR found this to be a violation of Article 10 of the European Convention on Human Rights, the main reason being that the measure taken by Turkey was not the least intrusive method, and also that the State did not try to find a better way to reach its goals, such as blocking the specific site at Google. The ECtHR also found that there was no strict legal framework in domestic law regulating the scope of the ban and the guarantee of judicial review. "In the Court's view, they should have taken into consideration, among other elements, the fact that such a measure, by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect.” (Ahmet Yildirim v. Turkey, 2012, 66.)

2.3. Cengiz and Others v. Turkey

In another case, the Ankara Criminal Court argued that a post on YouTube had infringed the country’s criminal law which prohibited insulting the memory of Mustafa Kemal Atatürk. The court ordered that YouTube be completely blocked (Cengiz and Others v. Turkey, 2015), which prompted Serkan Cengiz, a law professor, and other law professors from various Turkish universities, to respond. They claimed that as they were unable to use YouTube for a longer period, their human rights were infringed. In this case, the ECHR found that the measures taken by Turkey violated Article 10 of the European Convention on Human Rights. Meanwhile, the ECtHR acknowledged that YouTube was an important means by which the applicants exercised their right to receive and impart information and ideas through the Internet, and that both the damage and its effect were also collateral (Cengiz and Others v. Turkey, 2015, 64.) The Honourable Court had more to say, questioning the legal framework in Turkey’s domestic laws regulating the scope of the ban. And - as a new element to consider – the Court also found important that the block was upheld for a lengthy period of time.
2. 4. Kablis v. Russia, Elvira Dmitriyeva v. Russia

In this Russian case, (Kablis v. Russia, 2019), Kablis informed the Syktyvkar Town Administration of his intention to organise a protest. His request was refused, whereafter he criticised the decision on his social networking blog site, Vkontakte, and as a consequence his account was blocked. The case of Dmitriyeva is similar (Elvira Dmitriyeva v. Russia, 2019). Not a single court order was issued in either case, and therefore the Russian Prosecutor's measures amounted to a prior restraint. In the Dmitriyeva case, both Article 10 and Article 11 were examined. In both cases, the European Court of Human Rights ruled that the Russian state was in violation of Article 10 of the ECHR. The Honourable Court reiterates that the Russian "Information Act lacks the necessary guarantees against abuse required by the Court's case-law" (Kablis v. Russia, 2019, 97.).

2. 5. Wikimedia Foundation Inc. and Others v. Turkey

The third case in which Turkey sought to block differs in the outcome from the previous examples of Ahmet Yıldırım v. Turkey, 2012, and Cengiz and Others v. Turkey, 2015. In the case of Wikimedia Foundation Inc. ve Diğerleri Başvurusu, 2019, the ECHR did not find the organisation had violated Article 10 of the ECHR. The background is as follows: in 2017, all foreign (non Turkish) language editions of Wikipedia were blocked by the Turkish Information and Communication Technologies Authority on the grounds that Wikipedia had refused its request to remove content which asserted that Turkey was a sponsor of ISIS and other terrorist organisations. At this point, it should be underlined that by 2019 "more than 15 institutions and organizations are authorized to issue or request access-blocking orders under various regulations and most of these powers are exercised by submitting administrative blocking orders (...) without the need for judicial approval." (Akdeniz & Güven, 2020) Following Turkey's failure in the ECHR, it then claimed that Wikipedia was part of a 'smear campaign' against the country. As the blocking remained intact, Wikipedia filed an application in the ECHR in 2019. Not long after, the Turkish Constitutional Court concluded that the wholesale blocking violated the right to freedom of expression guaranteed under Article 26 of the Turkish Constitution. It also found the Turkish interpretation of the grounds for the interference was overly broad, making the legal basis unforeseeable and could have a substantial chilling effect.\(^5\)

2.6. Vladimir Kharitonov v. Russia, OOO Flavus and Others v. Russia, Bulgakov v. Russia, Engels v. Russia

Russia was the respondent in the most recent cases of website blocking, which includes: Bulgakov v. Russia, 2020; Engels v. Russia, 2020; OOO Flavus and Others v. Russia, 2020; Vladimir Kharitonov v. Russia, 2020.\(^6\) All of these cases have similarities, the European Court of Human Rights having ruled on the same day (23 June 2020), although the applications were lodged between 2013 and 2015. Vladimir Kharitonov found the IP address of his website was blocked because the Russian Federal Drug Control Service wanted to deny access to another website which had the same hosting company and IP address. In the case of OOO Flavus and Others, website access was blocked at the request from the Russian Prosecutor General without having first obtained a court order. Russia failed to identify the applicants of the specific offending material, so they could not even remove it in order to restore their access. Bulgakov's access was denied based on a court order, because his website stored an electronic book in the extremist publication section of the website. Even after he deleted the given book, the Russian Court upheld its decision stating that the block was a wholesale block, and not only for the material itself. Engels found himself in a very similar situation because his website contained information on how to bypass content filters. The blocking was decided even if the information did not violate domestic law. In all court cases, the ECtHR was unanimous in finding a violation of Article 10 of the European Convention on Human Rights, and clearly stated that the proceedings lacked the well-needed legitimacy because the provisions of

---

\(^5\) More on chilling effect, see (Fatullayev v. Azerbaijan, 2010, 102; Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt.v. Hungary, 2016, 86.; UNHRC, 2011, 28)

\(^6\) Note: the request for referral to the Grand Chamber is pending at the moment.
Russia's Information Act used to block the websites had excessive and arbitrary effects, and had not provided proper safeguards against abuse. The Honourable Court also declared that "the wholesale blocking of access to an entire website is an extreme measure which has been compared to banning a newspaper or television station." (Vladimir Kharitonov v. Russia, 2020, 38).

Conclusions

In conclusion, during the last decade almost all media outlets have made explicit on their news sites that the "UN declares Internet (access) a human right" (Kravets, 2011; Velocci, 2016; Jackson, 2011). However, the exact wording of the UNHRC documents did not go as far as to say that. Despite having stated that "for the Internet to remain global, open and interoperable, it is imperative that States address security concerns in accordance with their international human rights obligations, in particular with regard to freedom of expression, freedom of association and privacy" (UNHRC, 2016), this is not as stating the Internet to be a human right.7

The threat of State action to prevent access to the Internet remains. In 2020, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression raised concerns about "governments increasingly resort to shutting down the Internet, often for illegitimate purposes but in all cases having a disproportionate impact on the population." (UNHRC, 2020, 25.) It has become increasingly apparent that the COVID-19 pandemic is exposing more and more examples of limitations on free expression and the right to obtain information worldwide. In their July 2020 report (Mapping Media Freedom, 2020) the European Federation of Journalists and the International Press Institute showed that from March to June 2020 there had been a wide range of threats against media freedom (e.g. "during this time, Turkish authorities continued to use media regulators to shut down outlets broadcasting critical or sensitive topics.") (Mapping Media Freedom, 2020, 19.)

It would appear from decisions made by ECtHR that Internet blocking could be compatible with human rights only if it complies with some requirements. All three parts of the ECtHR's test (legitimacy, necessity and proportionality) should be addressed carefully, yet the States considered in this article usually fail to comply with the requirements of the necessity part of the above-mentioned test (e.g. there are less intrusive methods) and/or the proportionality part (e.g. there are collateral damages as such websites are taken down or blocked that has nothing to do with the targeted materials).

What is a possible way forward? Article 19 articulates the requirements. First, law must provide for blocking measures. A legal provision must establish clear and predictable rules concerning what content can be blocked, and to what extent. When it comes to assessing what content can be blocked, domestic legislation should follow the standards set by international human rights law. Secondly, a court or an independent adjudicatory body must issue blocking measures. Non-independent government agencies are likely to enforce overly restrictive measures, as their primary goal is to protect interests that conflict with freedom of expression. Thirdly, Internet users and Internet service providers (ISPs) must be allowed to challenge blocking measures. To that end, they must be given sufficient information on how to mount that challenge whenever they attempt to access a blocked site. Finally, blocking measures should be strictly targeted in order to avoid blocking lawful content. IP-address technologies should only be implemented in order to target non-shared IP servers." (Article-19, 2020).

Given that the Internet has become the tool for so many people to enjoy and express their human rights, to receive and impart information and ideas, and to fight against the marginalisation of States and groups in different societies, the growing number of cases sound a clear warning. Landmark cases ruled on by the ECtHR's show the different approaches of States in trying to block the Internet and make materials unreachable for end-users. Regardless, the mechanism of international jurisprudence has prevented them from doing so. The case law

---

7 More on this (Szoszkiewicz, 2018).
described in this paper is emphatic: any kind of restrictions to Internet access is drastic, and must be the final, and the most reasoned, measure taken by governments around the world.

References


Ahmet Yıldırım v. Turkey App no. 3111/10 (ECHR, 18 December 2012).

Akdeniz v. Turkey App no. 20877/10 (ECHR, 11 March 2014).


Cengiz and Others v. Turkey App nos 48226/10 and 14027/11 (ECHR, 1 December 2015).


Elvira Dmitrijeva v. Russia App nos. 60921/17 and 7202/18 (ECHR, 30 April 2019).

Engels v. Russia App no. 61919/16 (ECHR, 23 June 2020).


Kablis v. Russia App nos. 48310/16 and 59663/17 (ECHR, 30 April 2019).


Magyar Tartalomszolgáltató Egysülete and Index.hu Zrt. v. Hungary App no. 22947/13 (ECHR, 2 February 2016).


OOO Flavus and Others v. Russia App nos 12468/15, 23489/15, and 19074/16 (ECHR, 23 June 2020).


UNHRC. Disease pandemics and the freedom of opinion and expression. UN Doc A/HRC/44/49 (23 April 2020).

UNHRC. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. UN Doc A/HRC/17/27 (16 May 2011).


Vladimir Khariitonov v. Russia App no. 10795/14 (ECHR, 23 June 2020).


Copyright © 2020 by author(s) and Mykolas Romeris University
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/