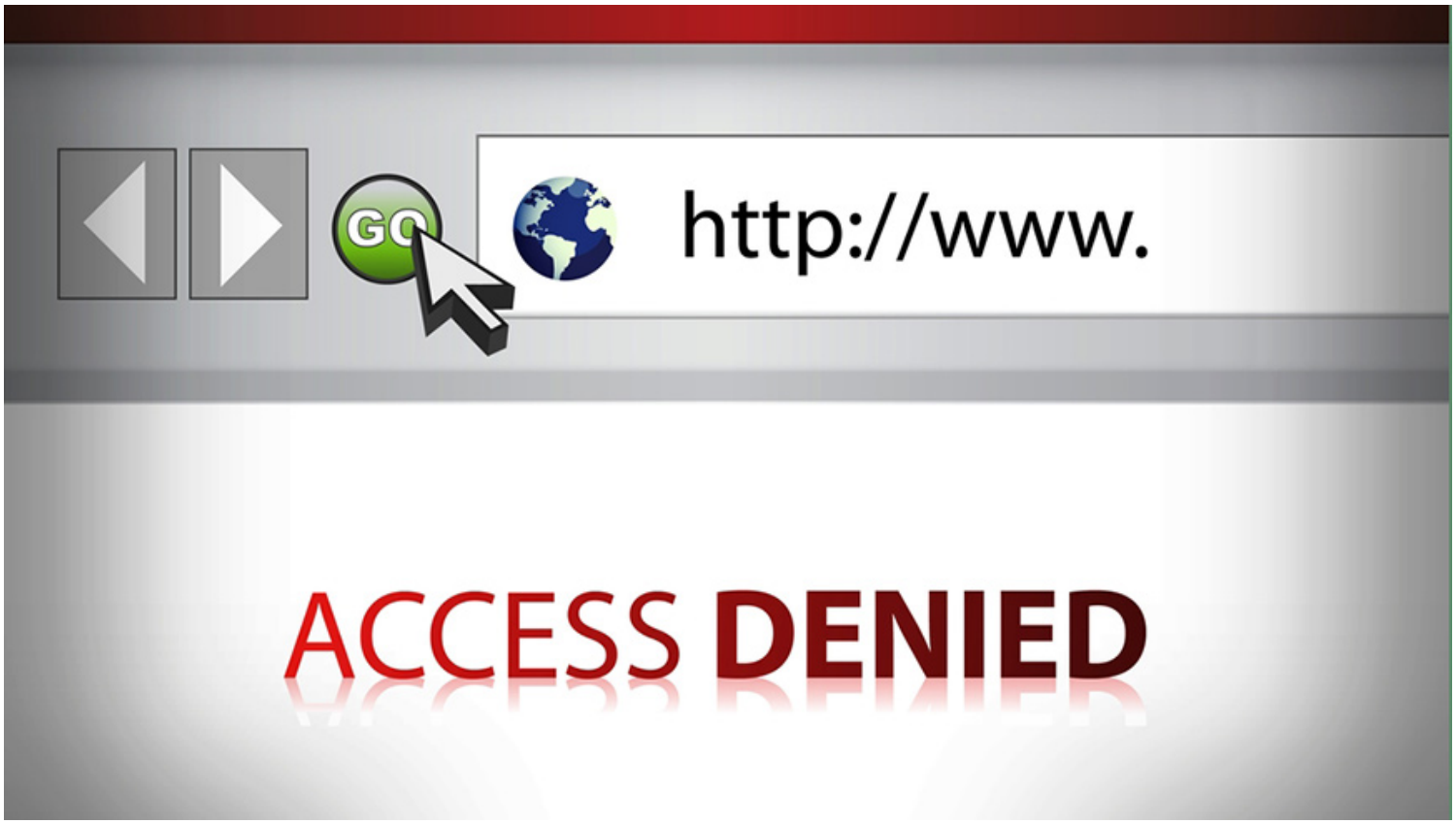
HUMAN RIGHTS COMMENT

Arbitrary Internet blocking jeopardises freedom of expression

Print

STRASBOURG | 26/09/2017



Internet blocking is a widespread phenomenon in Council of Europe member states. Its impact on freedom of expression was highlighted already in 2011, when the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, outlined in his annual report some of the ways in which states were increasingly censoring information online, notably through arbitrary blocking. In this report, blocking was defined as a set of "measures taken to prevent certain content from reaching an end-user", which includes "preventing users from accessing specific websites, Internet Protocol (IP) addresses, domain name extensions."

Since the beginning of my mandate in April 2012, I have encountered several problematic policies and practices in this field. A comparative study commissioned by the Council of Europe has identified two general models for the regulation of blocking by states. The first model concerns countries which do not have any specific legal or regulatory framework on the issue of blocking, and thus rely on an existing

general legal framework that is not specific to the Internet. The second model brings together countries which have adopted a legal framework specifically aimed at the regulation of the Internet and other digital media. In such countries, specific grounds (such as child abuse material, terrorism, criminality – in particular hate crimes – and national security) and conditions for blocking are usually defined. This study on the 47 member states of the Council of Europe gives a useful overview of the situation I have been confronted with in my country work.

Increasing online censorship on the ground

A few years ago, I published a report on Azerbaijan, expressing concern at the occasional blocking of certain websites. In a more recent development, on 12 May 2017, a district court in Baku ordered the blocking of a number of websites, including those of the Azerbaijani service of Radio Free Europe/ Radio Liberty, of the opposition newspaper Azadliq and of the online channel Meydan TV, following a request made by the Ministry of Transport, Communications and High Technologies, which reportedly claimed that these sites posed a threat to public order. This blocking, which leaves virtually no space for independent news online in the country, is now being challenged before the European Court of Human Rights.

In a Memorandum on freedom of expression and media freedom in Turkey published this year, I referred to the pervasiveness of Internet censorship in this country, where over the past two years access to the websites and Twitter accounts of pro-Kurdish media outlets has been banned by the (now abolished) Telecommunications Authority (TİB) numerous times. In February 2015, a Turkish criminal court of peace decided to ban access to a total of 49 websites, including Charlie Hebdo's official site, which were deemed to be anti-Muslim or atheist, holding that they "denigrated religious values". In April and May 2015 the TİB also blocked access to five commonly used LGBTI websites. More generally, access to various social media platforms has also been banned numerous times for not complying with broadcasting bans. I therefore concluded that the censorship of the Internet and the blocking of websites in Turkey continues to be exceptionally disproportionate.

In Ukraine, a decree signed by the President in May 2017 gave rise to concerns. As part of a new package of sanctions against the Russian Federation, the decree blocks access to a number of Russian-owned Internet companies and social media websites, such as the social networks VKontakte and Odnoklassniki and the search engine Yandex, which are very popular in Ukraine. The decree led to an alert submitted to the Council of Europe Platform to promote the protection of journalism and safety of journalists. While the Ukrainian authorities have put forward national security reasons to justify the measure on account notably of the country being the target of disinformation, propaganda campaigns and cyber-attacks, a number of non-governmental organisations have stressed the disproportionality of the measure, which affects legitimate content at the same time as content that may be legitimately prohibited, and is therefore bound to result in unjustifiable restrictions on freedom of expression for many persons in Ukraine.

Blocking is also an issue in the Russian Federation, as shown by a recent report which indicates that no less than 87,000 URLs (web addresses) were banned in 2016 under the so-called Lugovoi Law, a figure which might even be higher as a number of cases of overblocking (blocking of websites originally not targeted) have been reported. This law authorises the prosecutor general or his deputies to request the Russian regulatory authority, Roskomnadzor, to immediately block access to websites that disseminate calls for mass riots, contain "extremist" content, or call for participation in unsanctioned public gatherings. The report also notes that, since 2012, the legal grounds for blocking in the country were significantly broadened and the practice of blocking websites has become more widespread, echoing similar observations made during a round-table I held with digital rights experts from the Russian Federation in November 2015.

Website blocking as part of measures to counter terrorism

The problems do not end here: in a number of Council of Europe member states, we have witnessed an upsurge of legislation on blocking in the context of counter-terrorism. In Poland for instance, a new anti-terrorism law that entered into force on 2 July 2016 was criticised for giving Poland's intelligence agency the right to block websites for up to five days without obtaining prior court permission.

In France, a decree adopted in February 2015 to implement the law on reinforcing the fight against terrorism passed on 13 November 2014 foresees the administrative blocking of websites that incite or condone acts of terrorism or distribute child pornography, without prior judicial oversight. Under the supervision of the National Commission on Informatics and Liberty ("CNIL"), the French Central Office for combating crime related to information and communication technologies ("OCLCTIC") can ask Internet service providers to block a website if the website's host does not remove specific Internet content within 24 hours. According to the annual report of the "qualified person", designated by the CNIL to verify requests for website blocks, 874 requests to block websites were made by the OCLCTIC between March 2016 and February 2017, which represents a 180% increase compared to the previous year. At the same time, the report highlights that the verification proceedings were being jeopardised by a lack of resources and by insufficient access to the relevant information, which in practice makes it difficult to assess whether the requests are well-founded.

A system with flaws

As the country-specific examples above show, the systems in place for blocking suffer from a number of deficiencies. Some of these deficiencies were reflected in an Issue Paper on The rule of law on the Internet and in the wider digital world that I published in 2014:

- Blocking, notably when performed by software or hardware that reviews communications, is inherently likely to produce (unintentional) false positives (blocking sites with no prohibited material) and false negatives (when sites with prohibited material slip through a filter);
- the criteria for blocking certain websites, but not others, and the lists of blocked websites, are very often opaque at best, and secret at worst;

- appeal processes may be onerous, little known or non-existent, especially if the decision on what to block or not block is – deliberately – left to private entities;
- blocking measures are easy to bypass, even for not very technically skilled people;
- crucially, in particular in relation to child pornography, blocking totally fails to address the actual issue: the abuse of the children in question.

The above problems are compounded by the fact that once states have introduced blocking against the most serious issues and legitimate targets such as child pornography and hate speech, they tend to extend it to all sorts of other material that they disapprove of.

Blocking of Internet content: a clear interference with freedom of expression

The blocking of Internet content is a clear interference with the right to freedom of expression, guaranteed by Article 10 of the European Convention on Human Rights.

The case-law of the European Court of Human Rights on Internet blocking, which has developed over the past few years, rests on a three-step approach:

- the need for a clear legal basis for any blocking measure;
- the measure must pursue a legitimate aim, as enumerated by Article 10, paragraph 2 (for example, national security, prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others);
- the measure must be proportionate to the legitimate aim pursued.

On this basis, member states should ensure that any restrictions on access to Internet content affecting users under their jurisdiction are based on a strict and predictable legal framework regulating the scope of any such restrictions and afford the guarantee of judicial oversight to prevent possible abuses. In addition, domestic courts must examine whether any blocking measure is necessary and proportionate, and in particular whether it is targeted enough to impact only on the specific content that requires blocking.

A number of challenges ahead

However, arbitrary blocking by the authorities is only one side of the coin. One of the most pressing problems for freedom of expression online consists in Internet throttling (slowing down) and shutdowns. In Turkey, it has for instance been widely reported that the Turkish authorities have been increasingly resorting to bandwidth throttling during times of domestic crisis, making certain social media and communication platforms inaccessible in practice.

Another problematic aspect relates to content restrictions that are carried out by Internet service providers either entirely at their own initiative or with the encouragement of the authorities. In his latest report, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, addressed the roles played by private actors engaged in the provision of

Internet and telecommunications access. He expressed particular concern regarding reports of threats and intimidation by state authorities against companies, their employees and their equipment and infrastructure.

There is certainly an increasing tendency to leave blocking and the removal of content to the private sector. In Germany for example, the new law on the Improvement of Enforcement of Rights in Social Networks requires private companies to remove contents on the basis of specific provisions of the German Criminal Code. Concerns have been raised that the law might lead to excessive censorship. While state obligations to protect freedom of expression are clear, the various roles and duties of private actors in this sector remain vague. The current work of an expert body of the Council of Europe on the roles and responsibilities of Internet intermediaries is therefore a step in the right direction. It is high time that member states stop relying on or encouraging private companies to regulate the online communication space without ensuring themselves that human rights are protected and that due process guarantees are upheld in line with the European Convention on Human Rights.

Nils Muižnieks

List of resources:

- Commissioner's webpage on media freedom
- Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, adopted on 7 December 2011
- Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users
- Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet
- Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom
- European Court of Human Rights, Factsheet – New technologies, September 2017
- European Court of Human Rights, Research report, Internet: case-law of the European Court of Human Rights, June 2015
- Office of the OSCE Representative on Freedom of the Media: Freedom of Expression on the Internet (2012)
- Joint Declaration on Freedom of Expression and the Internet: Declaration signed by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 1 June 2011