EHRC EUROPEAN HUMAN RIGHTS CASES UPDATES

ANNOTATIE

Kharitonov t. Rusland & Bulgakov t. Rusland (EHRM, nr. 10795/14 & 20159/15) – Court stands firm on excessive nature of IP-address blocking

T. McGonagle

Annotatie bij Europees Hof voor de Rechten van de Mens, 23-06-2020, ECLI:CE:ECHR:2020:0623JUD001079514 (EHRC-2020-0186)

Annotatie bij Europees Hof voor de Rechten van de Mens, 23-06-2020, ECLI:CE:ECHR:2020:0623JUD002015915 (EHRC-2020-0186)

1. On 23 June 2020, the European Court of Human Rights (Third Section) published two judgments in cases involving the blocking of websites in Russia. In both cases, *Bulgakov* and *Vladimir Kharitonov*, the Court held unanimously that there had been a violation of Article 10 and a violation of Article 13 in conjunction with Article 10. In doing so, the Court has thrown a double punch at internet blocking, which it generally sees as an excessive form of interference with the right to freedom of expression.

2. The outcome of both judgments was predictable. The Court reverted to the tried and trusted reasoning of its *Ahmet Yildirim* judgment[1] - one of the first key judgments in its so-called 'internet' case-law.[2] It reiterated that the internet, by virtue of its accessibility and its capacity to store and communicate vast quantities of information, has become a principal means for everyone to exercise their rights to freedom of expression and information and participation in public life.

3. At issue in *Bulgakov* was the blocking of the applicant's entire website, pursuant to a district court order, because an e-book containing extremist, prohibited material had been available on the website. Access to the website continued to be blocked after the prohibited content had been removed. The District Court's order specified the method of implementation of the blocking measure: it required the internet service provider (ISP) to "apply filtering technology capable of preventing users from connecting to the website located at the specified numerical network address (I[nternet] P[rotocol] address)" (para. 33). The blocking measure did not differentiate between a website and a webpage. As the European Court of Human Rights stated: "Such 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" (para. 34). It also had the practical effect of "extending the scope of the blocking order far beyond the illegal content which had originally been targeted" (*ibid.*). The Court found that there was no legal basis for such an extension in the circumstances of the case.

4. In *Kharitonov*, the applicant's website was blocked as an automatic consequence of the implementation of a decision by the Russian telecoms regulator, *Roskomnadzor*, to put the website's IP-address on a register of black-listed websites for blocking. Crucially, the decision was intended to block access to another "offending" website, due to the alleged illegal content hosted by *that* website. The offending website had nothing to do with the applicant's website, but they had the same IP-address. The ISP DreamHost used the IP-address for a shared web-hosting service. The Court noted that this is "a common and accessible hosting arrangement for small to medium-sized websites" and the owners of individual websites may not be aware of the contents of co-hosted sites (para. 42). *Roskomnadzor*'s decision had, as the Court pointed out, "the immediate effect of blocking access to the entire cluster of websites hosted by DreamHost which shared an IP address with the offending website" (para. 40). The majority opinion of the Court found that the law that conferred such wide discretion on the regulatory body in blocking matters was not sufficiently foreseeable in its effects and did not afford the applicant the opportunity to regulate his conduct.

5. The bottom line in both judgments is that the wholesale blocking of access to an entire website is an extreme measure with far-reaching consequences for freedom of online expression. In both judgments, the Court likened such a blocking measure to the banning a newspaper or a television station (*Bulgakov*, para. 34; *Kharitonov*, para. 38). In *Kharitonov*, the Court stressed that "such a measure, by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect" (*Kharitonov*, para. 45). A Convention-compliant review by the Russian national courts should have included consideration of the effects of the impugned measure (*ibid.*)

6. According to the Court, the blocking of illegal content may (only) be justified in "exceptional circumstances". However, to pass muster under Article 10 of the European Convention on Human Rights, a blocking measure must be necessary, narrowly drawn, specific and targeted in focus, and proportionate to the intended aim. Safeguards must be in place against arbitrary use and due process must be followed. As the Court reiterated in *Kharitonov*, "it is incompatible with the rule of law if the legal framework fails to establish safeguards capable of protecting individuals from excessive and arbitrary effects of blocking measures" (para. 46).

7. In both judgments, the Court dwelt on how IP-addresses work and the practical implications of blocking at the level of IP-addresses. The Court thereby demonstrated its growing understanding of the technical features of the internet and their relevance for the effective exercise of the right to freedom of expression online (see also *Magyar Jeti Zrt. v. Hungary*, concerning hyperlinking[3]). Thus, it is disproportionate to block an entire website in order to render content on a specific webpage inaccessible (*Bulgakov*). Similarly, it is disproportionate to block an IP address shared by several websites in order to prevent access to illegal content hosted by a particular website (*Kharitonov*).

8. In both cases, the Court also considered the interplay between Articles 10 and 13 (right to an effective remedy) and in both instances, it held that the remedy provided for by national law was not effective. In *Bulgakov*, although the applicant could lodge an appeal against the blocking order and participate in the proceedings, the appellate court did not consider the substance of his grievance. Nor did it consider issues such as the legal distinction between a webpage and a website, the necessity, proportionality and excessive effects of the blocking measure/the method of its implementation (para. 48). Similarly, in *Kharitonov*, although the applicant could initiate appeal proceedings, the courts refused to consider the substance of his grievance, or the lawfulness or the proportionality of the effects of the blocking order on his website (para. 56).

9. As in other judgments in which the Court has nudged its internet case-law forward, the Court drew on a number of international sources and materials that are extraneous to the European Convention on Human Rights. In doing so, the Court looked beyond its own case-law for experience and inspiration on fast-developing topics. Such an approach is consistent with the 'living instrument' doctrine, under which the Court interprets the Convention in light of present-day conditions. The external international sources and materials referenced in the judgment are: the Council of Europe's Committee of Ministers' Declaration on freedom of communication on the Internet (2003) and Recommendation to member States on Internet freedom (2016); the United Nations Human Rights Committee's General Comment No. 34 on freedom of opinion and expression (2011) and a report by the Special Rapporteur on freedom

of expression (2011). The 2011 Joint declaration on freedom of expression and the Internet, adopted by the specialized international mandates on freedom of expression and/or the media was also referenced. In *Kharitonov*, the Court additionally referred to an issue paper written for the Council of Europe Commissioner for Human Rights: *The rule of law on the Internet and in the wider digital world* (2014). The Court could also draw on the specific expertise of a range of third-party interveners in both cases.[4] The expertise provided via *amicus curiae* briefs has been recognised as a valuable resource for the Court.[5]

10. In *Bulgakov* and *Kharitonov*, the Court did not recognise any new principles as such. It rather re-affirmed several existing principles. In both cases, the impugned blocking measures were clearly disproportionate and excessive, and they caused significant collateral censorship. These are textbook examples of cases in which, as the saying goes, the village has been burned to roast the pig.[6]

Prof. dr. Tarlach McGonagle

Leiden Law School

[1] *Ahmet Yıldırım v. Turkey*, 18 December 2012, no. 3111/10, ECLI:CE:ECHR:2012:1218JUD000311110, «EHRC» 2013/93 case note M.M. Groothuis.

[2] European Court of Human Rights (Research Division), 'Internet: case-law of the European Court of Human Rights', June 2015, available at: https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf; European Court of Human Rights (Press Unit), Factsheet – New technologies, July 2020, available at: https://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf.

[3] *Magyar Jeti Zrt. v. Hungary*, 4 December 2018, no. 11257/16, ECLI:CE:ECHR:2018:1204JUD001125716, «EHRC» 2019/52 case note T. McGonagle.

[4] In *Bulgakov*, the following parties intervened: the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ARTICLE 19, the Electronic Frontier Foundation, Access Now, Reporters without Borders and the European Information Society Institute. In *Kharitonov*, the intervening parties were: Access Now, ARTICLE 19, the European Information Society Institute and RosKomSvoboda (a Russian NGO).

, Conference e-book (Leipzig, European Centre for Press and Media Freedom (ECPMF), 2017), pp. 70-95, at 93, available at: https://www.ecpmf.eu/archive/events/ecpmfecthr2017.html.

[6] This phrase achieved a certain level of popularity in early analyses of freedom of expression and censorship on the internet. See, for example, Felipe Rodriquez, 'Burning the Village to Roast the Pig: Censorship of Online Media', in *From Quill to Cursor: Freedom of the Media in the Digital Era* (Vienna, OSCE Representative on Freedom of the Media, 2003), pp. 85-109, available at: https://www.osce.org/files/f/documents/0/4/13834.pdf; Dalzell, D.J., *ACLU v. Reno*, 929 F.Supp. 824, at p. 882.