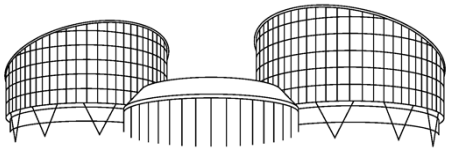

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF BULGAKOV v. RUSSIA

(Application no. 20159/15)

JUDGMENT

Article 10 • Freedom to receive and impart information • Access blocked to entire website because of one piece of prohibited material and continued blocking even after material had been removed • Wholesale blocking of access to an entire website being an extreme measure comparable to banning a newspaper or television station • Blocking access to a website's IP address having practical effect of extending scope of blocking order far beyond illegal content originally targeted • Blocking formula employed by court not featuring in any primary legislation or implementing regulations • Domestic law lacking safeguards against excessive and arbitrary effects of blocking measures • Notification and involvement of website owners in blocking proceedings not required by law • Participation of local Internet service provider not sufficient to endow proceedings with adversarial character • Domestic courts' failure to perform a Convention-compliant review considering less intrusive means or assessing an impact of the blocking measure • Unlawful refusal to lift blocking order after the removal of illegal content
Article 13 in conjunction with Article 10 • Effective remedy • Failure of courts to consider the substance of grievance or to examine lawfulness or proportionality of effects of blocking order

STRASBOURG

23 June 2020

FINAL

16/11/2020

This judgment has become final under Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Bulgakov v. Russia,

The European Court of Human Rights (Third Section), sitting as a Chamber composed of:

Paul Lemmens, *President,*
Georgios A. Serghides,
Helen Keller,
Dmitry Dedov,
Alena Poláčková,
Lorraine Schembri Orland,
Ana Maria Guerra Martins, *judges,*
and Milan Blaško, *Section Registrar,*

Having regard to:

the application (no. 20159/15) against the Russian Federation lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Russian national, Mr Yevgeniy Vladimirovich Bulgakov ("the applicant"), on 13 April 2015;

the decision to give notice to the Russian Government ("the Government") of the complaints relating to the right to impart information and the right to an effective domestic remedy, and to declare the remainder of the application inadmissible;

the observations submitted by the respondent Government and the observations in reply submitted by the applicant;

the comments submitted by third-party interveners who were granted leave to intervene by the President of the Section;

Having deliberated in private on 26 May 2020,

Delivers the following judgment, which was adopted on that date:

INTRODUCTION

The case concerns the method of implementation of a blocking order targeting extremist content which had the effect of blocking access to the applicant's entire website.

THE FACTS

1. The applicant was born in 1978 and lives in Bryansk. He had been granted legal aid and was represented by Mr O. Anishchik, a lawyer practising in St Petersburg.

2. The Government were represented by Mr M. Galperin, Representative of the Russian Federation to the European Court of Human Rights.

3. The facts of the case, as submitted by the parties, may be summarised as follows.

4. The applicant is the owner and administrator of the website "Worldview of the Russian Civilization" (www.razumei.ru). In November 2013, he discovered that the local Internet service provider (ISP) had blocked access to his website on the basis of a judgment by the Kirovskiy District Court in Rostov-on-Don dated 3 April 2012.

5. As it transpired, in late 2011 the Rostov Regional prosecutor had brought a public-interest claim against a regional ISP. The prosecutor claimed that, by using the provider-facilitated connection to the Internet, he had been able to access a particular pamphlet and an electronic book ("the e-book"), both of which had been previously categorised as extremist publications. One copy of the e-book in PDF format was accessible, in particular, in the files section of the applicant's website. The prosecutor asked the Kirovskiy District Court to block access to the publications "by adding filter rules for the websites' IP addresses to the area border router" (*«путем добавления на пограничном маршрутизаторе правил фильтрации IP-адресов указанных сайтов»*), that is to say, by way of blocking access to the websites by their numerical network addresses ("IP address"). Referring to the provisions of the Suppression of Extremism Act and section 10(1) and (6) of the Information Act, the Kirovskiy District Court required the ISP to block access to the applicant's website using the formulation of the blocking measure which the prosecutor had suggested.

6. Immediately upon finding out about the Kirovskiy District Court's judgment, the applicant deleted the offending e-book and brought proceedings against the ISP, seeking to have access to his website restored. On 25 March 2014 the Savelovskiy District Court in Moscow granted the claim, noting that the extremist material had been removed. That decision was overturned on appeal: on 14 August 2014 the Moscow City Court held that the Kirovskiy District Court's judgment had required the ISP "to block access to the website's IP address, rather than to a specific page of the website" and that it would be contrary to the terms of that judgment to grant the applicant's claim. On 5 December 2014 and 5 March 2015 the City Court and the Supreme Court, respectively, refused the applicant leave to appeal to the cassation instance.

7. In the meantime, the applicant asked the Kirovskiy District Court to fix a new time-limit for lodging an appeal against the 2012 judgment. On 9 December 2014 the Kirovskiy District Court acceded to his request. Referring to the Constitutional Court's case-law, it noted that the proceedings could not be considered fair if the judgment determined the rights and obligations of, or imposed new restrictions on, persons who had not taken part in the proceedings.

8. In his statement of appeal, the applicant pointed out that as he had been unaware of the original blocking proceedings, he had been unable to defend his rights. In the meantime, the proscribed e-book had been removed. In evidence, he enclosed a copy of the Savelovskiy District Court's judgment and a printout from his website.

9. On 29 January 2015 the Rostov Regional Court dismissed the appeal. It found that the 2012 judgment could not be set aside on the grounds that the applicant had not been able to join the proceedings because the prosecutor had lodged a claim against the ISP, rather than against him. Without examining the applicant's evidence, the Regional Court held that it had not been shown that the offending e-book had been removed. On 15 June and 5 October 2015 the Regional Court and the Supreme Court, respectively, refused the applicant leave to appeal to the cassation instance.

RELEVANT DOMESTIC LEGAL FRAMEWORK

A. Information Act (Federal Law no. 149-FZ of 27 July 2006)

10. Section 2 defines the basic terms as follows:

> "(13) 'Internet site' is an aggregate of computer software and other content ... which can be accessed ... by its domain name or its network address ...
>
> (14) 'page of an Internet site (webpage)' is a part of an Internet site which can be accessed by its reference made up of the domain name and additional characters ...".

11. Section 10 provides that information may be freely disseminated in the Russian Federation subject to the requirements of Russian legislation (subsection (1)). The dissemination of information which may not be disseminated under penalty of criminal or administrative sanction is prohibited (subsection (6)).

B. Case-law of Russian courts

12. By a judgment of 10 May 2011 (case no. 58-Vpr11-2), the Supreme Court of the Russian Federation reversed judgments rendered by the lower courts on a prosecutor's public-interest claim against an ISP. The prosecutor had sought a court order blocking access to a particular website, two pages of which contained documentation of a prohibited political party, by means of "adding filter rules for the website's IP address to the area border router". The lower courts at two instances had dismissed the prosecutor's claim, having found that the ISP had no technical means of blocking access to individual pages of the website and that there were no legal grounds for blocking access to the entire website. The Supreme Court disagreed. It held that the ISP was bound, under section 10(6) of the Information Act, to block the dissemination of extremist content. In so far as it had a technical possibility to enforce the wholesale blocking of the website's IP address by defining filter rules at the area border router, the ISP should have used that method to block access to the website.

13. On 13 March 2012 the Sakhalin Regional Court reversed a judgment by the Town Court dismissing a town prosecutor's claim against an ISP (case no. 33-630/2012). The prosecutor had sought a court order blocking access to a website containing an extremist film. The Town Court had held that, in the absence of evidence that no content other than the prohibited film was housed at that IP address, blocking access to the website's IP address could breach the users' right to freedom of access to legitimate content. The Regional Court reiterated the Supreme Court's arguments and remitted the matter to the Town Court, requiring it to examine whether access to the website could be blocked by filtering its IP address at the area border router.

14. On 17 November 2014 the Rostov Regional Court upheld a judgment by the District Court dismissing a district prosecutor's claim seeking to have one page of an extremist publication blocked "by way of filtering the website's IP address at the area border router" (case no. 33-15382/2014). The District Court had refused the claim on the grounds that filtering the website's IP address would restrict access to the entire website, rather than to a page of the website.

15. As of April 2020, an online database of judicial decisions (www.sudact.ru) listed over 12,000 judgments in which Russian courts had blocked access to online content "by way of filtering the website's IP address at the area border router". Between 2017 and 2019, one court, the Promyshlennyy District Court in the Stavropol Region, issued as many as 222 blocking decisions in which that formula was used.

RELEVANT INTERNATIONAL MATERIAL

16. The Declaration on freedom of communication on the Internet, adopted by the Council of Europe's Committee of Ministers on 28 May 2003, took note of the Member States' commitment to abide by the following principles in the field of communication on the Internet:

> **Principle 3: Absence of prior state control**
>
> "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. This does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries.
>
> Provided that the safeguards of 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 its illegality."

17. The 2011 Report of the United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/17/27) expressed concerns about the excessive scope of blocking measures:

> "29. Blocking refers to measures taken to prevent certain content from reaching an end user. This includes preventing users from accessing specific websites, Internet Protocol (IP) addresses, domain name extensions, the taking down of websites from the web server where they are hosted, or using filtering technologies to exclude pages containing keywords or other specific content from appearing ...
>
> 31. States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression ... Firstly, the specific conditions that justify blocking are not established in law, or are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively. Secondly, blocking is not justified to pursue aims which are listed under article 19, paragraph 3, of the International Covenant on Civil and Political Rights, and blocking lists are generally kept secret, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose. Thirdly, even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a judicial or independent body ..."

18. The Joint declaration on freedom of expression and the Internet, adopted on 1 June 2011 by the UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression, and the African Commission on

Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, provides in particular:

1. General Principles

"a. Freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognised under international law (the 'three-part' test) ..."

3. Filtering and Blocking

"a. Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse."

19. In General Comment No. 34 on Article 19 of the International Covenant on Civil and Political Rights (CCPR/C/GC/34), adopted at its 102nd session (11-29 July 2011), the United Nations Human Rights Committee stated as follows:

"42. The penalization of a media outlet, publishers or journalist solely for being critical of the government or the political social system espoused by the government can never be considered to be a necessary restriction of freedom of expression.

43. Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information-dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3 [of Article 19]. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."

20. Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom, adopted by the Committee of Ministers of the Council of Europe on 13 April 2016, recommended that member States be guided by, and promote, specific Internet freedom indicators when participating in international dialogue and international policy making on Internet freedom. When adopting this recommendation, the Permanent Representative of the Russian Federation indicated that, in accordance with Article 10.2c of the Rules of Procedure for the meetings of the Ministers' Deputies, he reserved the right of his Government to comply or not with the recommendation, in so far as it referred to the methodology for its implementation at national level. Section 2.2 of the Internet freedom indicators, "Freedom of opinion and the right to receive and impart information", reads:

"2.2.1. Any measure taken by State authorities or private-sector actors to block or otherwise restrict access to an entire Internet platform (social media, social networks, blogs or any other website) or information and communication technologies (ICT) tools (instant messaging or other applications), or any request by State authorities to carry out such actions complies with the conditions of Article 10 of the Convention regarding the legality, legitimacy and proportionality of restrictions.

2.2.2. Any measure taken by State authorities or private-sector actors to block, filter or remove Internet content, or any request by State authorities to carry out such actions complies

with the conditions of Article 10 of the Convention regarding the legality, legitimacy and proportionality of restrictions.

2.2.3. Internet service providers as a general rule treat Internet traffic equally and without discrimination on the basis of sender, receiver, content, application, service or device. Internet traffic management measures are transparent, necessary and proportionate to achieve overriding public interests in compliance with Article 10 of the ECHR.

2.2.4. Internet users or other interested parties have access to a court in compliance with Article 6 of the Convention with regard to any action taken to restrict their access to the Internet or their ability to receive and impart content or information.

2.2.5. The State provides information in a timely and appropriate manner to the public about restrictions it applies to the freedom to receive and impart information, such as indicating websites that have been blocked or from which information was removed, including details of the legal basis, necessity and justification for such restrictions, the court order authorising them and the right to appeal."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION

21. The applicant complained that the domestic courts had upheld a measure blocking access to his entire website at the level of the ISP, even after the prohibited content had been taken down. He relied on Article 10 of the Convention, which reads in the relevant part:

"1. Everyone has the right to freedom of expression. This right shall include freedom ... to receive and impart information and ideas without interference by public authority and regardless of frontiers ...

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such 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 ..."

A. Admissibility

22. The Court considers that this complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. Submissions by the parties

(a) The Government

23. The Government submitted that pursuant to the Kirovskiy District Court's judgment, access to the applicant's website had been blocked by an ISP. The judgment had not been submitted to the telecoms regulator, Roskomnadzor, for implementation, and Roskomnadzor had not deployed any blocking measures against the applicant's website. Once the extremist content had been taken down, no measures to restrict access to the applicant's website had been implemented.

(b) The applicant

24. The applicant explained that the formula which had been used in the blocking decision in the present case – blocking access to the website's IP address at the level of the ISP – harked back to the Supreme Court's judgment of 10 May 2011 (see paragraph 12 above). From that time, the Russian courts had used the formula in a large number of cases to block access to the IP addresses of entire websites, even where the prohibited material was located on just one or two pages of the websites (see paragraph 13 above). That formula flouted the distinction between the website as a whole and a particular page of a website, in disregard of the definitions in section 2 of the Information Act. On textual reading, the courts ordered the blocking of access to particular webpages which contained extremist material. As the scope of the order was ostensibly limited to illicit content, they were not bound to consider whether it affected the accessibility of the website's legitimate content. However, the court-mandated technical means of implementing a blocking order – blocking access to the website's IP address – inevitably resulted in blocking access to the entire website, because only websites had IP addresses whereas their individual webpages did not. To the applicant's knowledge, there had been only one instance in which the courts had correctly acknowledged that blocking access to one page by way of the website's IP address would have the collateral effect of blocking the whole website (see paragraph 14 above). Incidentally, that judgment had been upheld by the same Rostov Regional Court which, two months later, had reached the opposite conclusion in the applicant's case. The applicant concluded that the judicial practice, which had developed following the Supreme Court's decision and of which his case was but one example, failed to meet the "quality of law" requirement. It disregarded the distinction between a "website" and a "webpage" and allowed courts to block access to an entire website on the grounds that one of its pages contained problematic content. It also removed the need for considering how that form of blocking affected legitimate content. For the applicant, that manner of proceedings was tantamount to holding that "access to hearing room 5 should be restricted by blocking the main entrance to the courthouse".

(c) Third-party interveners

25. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, an independent expert mandated by the Human Rights Council to report on the extent, nature and severity of restrictions and violations of freedom of expression, submitted that individuals should be allowed to enjoy freedom of expression in online space to the same extent that they enjoyed it offline. States frequently adopted anti-extremism laws that were so broad as to give authorities excessive discretion to restrict online expression, contrary to the lawfulness requirement. Such legislation prioritised restrictions on, rather than protection of, free expression as the primary State responsibility and failed to define precisely limitations on online expression and justifications for those limitations. The wholesale blocking of websites rarely, if ever, satisfied the criteria for permissible limitations on freedom of expression, taking into account that permissible restrictions should be content-specific and should not target websites solely because they were critical of the government or political system.

26. ARTICLE 19, a global campaign for freedom of expression, the Electronic Frontier Foundation, a legal and policy organisation safeguarding privacy in the digital world, Access Now, a global civil-society organisation defending the digital rights of users at risk, and Reporters without Borders, a French non-profit organisation defending freedom of the press, emphasised that blocking access to entire websites was an extreme and disproportionate measure which was incapable of distinguishing between lawful and unlawful content and, as such, should never be required by law. Even where blocking was permissible, the law should provide for the following minimum standards: (i) blocking should be ordered by a court or an independent adjudicatory body; (ii) interested parties should be given the opportunity to intervene in proceedings in which a blocking order has been sought; (iii) all victims of blocking orders should have the right to challenge, after the fact, the blocking order; and (iv) anyone attempting to access the blocked website should be able to see the legal basis and reasons for the blocking order and information about avenues of appeal.

27. The European Information Society Institute, a Slovakia-based non-profit organisation focusing on high-technology law, submitted that any blocking measure which went beyond its target and over-blocked legitimate content, was not acceptable in a democratic society. The authorities had a duty to carry out an individualised assessment of whether the same result could be achieved with a less intrusive measure. The targeted website should be informed and given a reasonable amount of time to remove the offending content and to make submissions before a decision was taken.

2. The Court's assessment

28. The Court reiterates that owing to its accessibility and capacity to store and communicate vast amounts of information, the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information. The Internet provides essential tools for participation in activities and discussions concerning political issues and issues of general interest, it enhances the public's access to news and facilitates the dissemination of information in general. Article 10 of the Convention guarantees "everyone" the freedom to receive and impart information and ideas. It applies not only to the content of information but also to the means of its dissemination, for any restriction imposed on the latter necessarily interferes with that freedom (see *Ahmet Yıldırım v. Turkey*, no. 3111/10, §§ 48-54, ECHR 2012).

29. The applicant is the owner and administrator of a website. In November 2013, he discovered that access to his website had been blocked by a local ISP pursuant to a judicial decision. The Court reiterates 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 (see *Ahmet Yıldırım*, cited above, § 53). In so far as the blocking measure was imposed by a Russian court, it does not matter that it was implemented by an ISP rather than the telecoms regulator. The measure which prevented visitors to the applicant's website from accessing its content amounted to "interference by a public authority" with the right to receive and impart information, since Article 10 guarantees not only the right to impart information but also the right of the public to receive it (see

Ahmet Yıldırım, cited above, §§ 51 and 55, and *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, § 56, ECHR 2015 (extracts)).

30. As regards the scope of the interference, the applicant did not dispute that the e-book which had been available on his website constituted prohibited material. He took issue, however, with the domestic courts' decisions to block access to his entire website because of one piece of prohibited material and to continue blocking access even after that material had been removed. The Court will examine the two aspects in turn. It reiterates that 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.

31. The Court reiterates that the expression "prescribed by law" not only refers to a statutory basis in domestic law, but also requires that the law be both adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual to foresee the consequences which a given action may entail. In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must afford a measure of legal protection against arbitrary interferences by public authorities with the rights safeguarded by the Convention, and indicate with sufficient clarity the scope of any discretion conferred on the competent authorities and the manner of its exercise (see *Hasan and Chaush v. Bulgaria* [GC], no. 30985/96, § 84, ECHR 2000-XI; and *Ahmet Yıldırım*, cited above, §§ 57 and 59).

32. The District Court's decision of 3 April 2012 which gave rise to the interference in the present case had a legal basis in section 10(6) of the Information Act. That provision allowed the authorities to block any content, dissemination of which was punishable under administrative or criminal law. The e-book fell within the scope of that provision. It had been previously categorised as extremist material. Such material may not be distributed or transmitted over public communication networks (see *Mariya Alekhina and Others v. Russia*, no. 38004/12, §§ 93-94, 17 July 2018) and its mass dissemination constitutes an offence under Article 20.29 of the Code of Administrative Offences. It follows that, in so far as the District Court's decision targeted the e-book, the interference can be said to have been "prescribed by law".

33. However, the scope of the District Court's order was not limited to identifying the offending content which was to be blocked. The District Court also determined the method of implementation of the blocking measure. To that end, it borrowed the formula from the application lodged by the prosecutor, who had requested that access to the extremist content be blocked by means of "adding filter rules for the website's IP address to the area border router". In layman's terms, that formula requires the ISP to apply filtering technology capable of preventing users from connecting to the website located at the specified numerical network address (IP address). In other words, the District Court ordered the blocking of access to the offending content by means of blocking access to the entire website, because only websites, but not their individual pages or sections, have IP addresses. The applicant speculated that behind the use of that formula had been a lack of technical expertise on the part of the judges, which had prevented them from

distinguishing a particular page of the website from the website as a whole. The unsettled case-law of the Russian courts may lend support to his hypothesis. There have been cases in which lower courts correctly determined that blocking access to a website's IP address would lead to arbitrary blocking of legitimate content on the same website. Some such decisions were overturned on appeal, whereas others were upheld (see paragraphs 12 to 14 above). The fact however remains that this blocking method has been used in thousands of cases (see paragraph 15 above).

34. The Court reiterates 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 (see paragraphs 17 and 19 above). 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. Blocking access to a website's IP address has the practical effect of extending the scope of the blocking order far beyond the illegal content which had originally been targeted (compare *Ahmet Yıldırım*, cited above, § 63). Such an extension did not have a legal basis in the circumstances of the present case. Section 10 of the Information Act allowed the authorities to target content that was proscribed under administrative or criminal law, rather than an entire website. The blocking formula employed by the District Court did not feature in any primary legislation or implementing regulations. The Government, in their observations, did not point to any legal provision on which the method of implementation chosen by the District Court could have been based.

35. Turning next to the issue of the safeguards which domestic legislation must provide to protect individuals from the excessive and arbitrary effects of blocking measures, the Court notes that the Russian law did not require any form of involvement of the website owner, such as the applicant, in blocking proceedings conducted under section 10(6) of the Information Act. The prosecutor's application for a blocking order had been prepared without advance notification to the parties whose rights and interests were likely to be affected. The applicant had not been informed of the prosecutor's application or afforded the opportunity to remove the illegal content before the application was lodged with the court. The District Court had not invited him to intervene in the proceedings or to make submissions, treating the matter as being between the prosecutor and the local ISP.

36. The Court finds that the participation of a local ISP as the designated defendant was not sufficient to bestow an adversarial character on the proceedings. The ISP provides technology enabling users to access millions of websites it knows nothing about. It does not have the same detailed knowledge of their contents as their owners do; nor does it have the legal resources required to mount a vigorous defence of every targeted website. The ISP has no vested interest in the outcome of the proceedings. Blocking orders have no incidence on its connectivity business; they are enforceable not just against the defendant ISP but, once final, they acquire universal effect requiring all Russian ISPs to implement blocking measures. The Court finds that the blocking proceedings which were conducted in the applicant's absence were not adversarial in nature and did not provide a forum in which the interested parties could have been heard.

37. In the proceedings which the applicant instituted to challenge the blocking measure, the domestic courts did not apply the Plenary Supreme Court's Ruling no. 21 of 27 June 2013, which required them to have regard to the criteria established

in the Convention in its interpretation by the Court (see *Lashmankin and Others v. Russia*, nos. 57818/09 and 14 others, § 217, 7 February 2017). Nor did they consider whether the same result could be achieved with less intrusive means or carry out an impact assessment of the blocking measure to ensure that it strictly targets the illegal content and has no arbitrary or excessive effects, including those resulting from the method chosen to implement it. As regards the transparency requirement, the Information Act makes no provision for communicating the decision taken under section 10(6) to the owner of the targeted website. In the present case, the applicant had been unaware of the blocking order until he discovered that access to his website had been blocked (see paragraph 4 above).

38. The second aspect of the interference which the applicant complained of was the refusal to lift the blocking order after the unlawful content had been removed. The fact that the content had been removed was established in the decision of the Savelovskiy District Court, which also held that the removal of objectionable content was sufficient grounds for restoring access to the applicant's website (see paragraph 6 above). The higher courts, however, disagreed with the District Court's assessment and maintained that the original decision blocking access to the website's IP address should stand. The Court has found above that there was no legal basis for blocking access to the applicant's entire website when it contained one page of extremist material (see paragraph 34 above). This finding of unlawfulness applies *a fortiori* to the continued blocking of the website after that material had been removed.

39. Having regard to the above analysis, the Court concludes that the interference resulting from the application of the procedure under section 10(6) of the Information Act had excessive and arbitrary effects and that the Russian legislation 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. Accordingly, the interference was not "prescribed by law" and it is not necessary to examine whether the other requirements of paragraph 2 of Article 10 have been met.

40. There has accordingly been a violation of Article 10 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION TAKEN IN CONJUNCTION WITH ARTICLE 10

41. The applicant complained under Article 13 of the Convention, taken in conjunction with Article 10, that the Russian courts had not considered the substance of his grievance relating to the blocking of access to his website. Article 13 reads:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

A. Admissibility

42. The Court considers that this complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

43. The Government submitted that the applicant had had effective domestic remedies at his disposal and had used them to the full extent. His case had been heard and decided on the basis of the applicable legislation. Since access to his website had not actually been blocked by Roskomnadzor, there had been no violation of his rights.

44. The applicant did not dispute that he had been able to lodge an appeal and take part in the appeal hearing. He also accepted that the Russian law provided, in theory, a remedy for the alleged violation. The courts could have drawn a distinction between a webpage and a website and pronounce unlawful a blocking order which affected the entire website, rather than a particular webpage. However, in practice, the courts had not considered the merits of his arguments or examined his evidence. They had not addressed them in any way or made any findings of fact or law. He had therefore been denied an effective domestic remedy for his grievances.

45. The third-party intervener, the European Information Society Institute, submitted that both *ex ante* and *ex post* remedies needed to be made available to the affected parties. *Ex ante* remedies should include prior notification to the owners of targeted websites. *Ex post* remedies should ensure that, once a blocking order has been implemented, there are efficient mechanisms for restricting its scope or challenging it on account of new circumstances.

46. The Court notes that the complaint under Article 13 arises from the same facts as those it has examined when dealing with the complaint under Article 10 above. However, there is a difference in the nature of the interests protected by Article 13 of the Convention and those protected under Article 10: the former affords a procedural safeguard, namely the "right to an effective remedy", whereas the procedural requirement inherent in the latter is ancillary to the wider purpose of ensuring respect for the substantive right to freedom of expression (see *Iatridis v. Greece* [GC], no. 31107/96, § 65, ECHR 1999-II). Having regard to the difference in purpose of the safeguards afforded by the two Articles, the Court considers it appropriate in the instant case to examine the same set of facts under both provisions.

47. The Court notes that the applicant had an arguable claim of a violation of his right to freedom of expression. Accordingly, Article 13 required that he should have had a domestic remedy which was "effective" in practice as well as in law, in the sense of preventing the alleged violation or its continuation, or of providing adequate redress for any violation that had already occurred.

48. Although the applicant was able to bring an appeal against the blocking order and to take part in the appeal proceedings, the appellate court did not consider the substance of his grievance. It did not address the legal distinction between a webpage and a website or examine the necessity and proportionality of the blocking measure and the excessive effects of the chosen method of its implementation. Nor did it evaluate the applicant's evidence and make any findings as to whether it should be accepted or rejected. Accordingly, the Court finds that the remedy which the national law provided for was not effective in the circumstances of the applicant's case (see *Elvira Dmitriyeva v. Russia*, nos. 60921/17 and 7202/18, § 64, 30 April 2019).

49. There has therefore been a violation of Article 13 of the Convention, taken in conjunction with Article 10.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

50. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

51. The applicant asked the Court to determine the amount of compensation in respect of non-pecuniary damage. He claimed 941 euros (EUR) in respect of legal costs and postal expenses.

52. The Government submitted that no compensation should be awarded because the applicant's rights had not been violated.

53. The Court awards the applicant EUR 10,000 in respect of non-pecuniary damage and the amount claimed in respect of costs and expenses, minus the EUR 850 granted by way of legal aid, plus any tax that may be chargeable to the applicant.

54. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 10 of the Convention;

3. *Holds* that there has been a violation of Article 13 of the Convention, taken in conjunction with Article 10;

4. *Holds*
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
      (i) EUR 10,000 (ten thousand euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;
      (ii) EUR 91 (ninety-one euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement, simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period, plus three percentage points.

Done in English, and notified in writing on 23 June 2020, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Milan Blaško	Paul Lemmens
Registrar	President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judges Lemmens, Dedov and Poláčková, is annexed to this judgment.

P.L.
M.B.

JOINT CONCURRING OPINION OF JUDGES LEMMENS, DEDOV AND POLÁČKOVÁ

1. We fully concur in the conclusion that Articles 10 and 13 of the Convention have been violated.

We would like to add a few thoughts to the reasoning under Article 10.

2. The interference in this case was a court decision ordering a local Internet provider to block access to the applicant's website "www.razumei.ru". The court order was delivered at the request of a regional prosecutor who had brought proceedings against the Internet provider (but without involving the applicant in them). The prosecutor's request and the ensuing court order were based on the fact that the applicant's website contained a specific item (a specific e-book) that had been previously categorised as "extremist". The prosecutor had asked the court to block access to the applicant's website by adding filter rules for the website's IP address. The court granted the request, including the method to be used for the blocking measure. Following the implementation of the court's decision by the Internet provider, access was blocked to the entire website, not only to the page containing the e-book.

The entire website was thus blocked due to the method chosen to block a specifically targeted webpage on that site.

3. The impugned measure was based on section 10(6) of the Information Act. According to this provision, it is prohibited to disseminate information that is aimed at propaganda for war, or incitement of national, racial or religious hatred or hostility, as well as information the dissemination of which is prohibited on pain of a criminal or administrative sanction. As the Court notes, the applicant did not dispute that the e-book constituted prohibited material. His complaint only concerned the continued blocking of access to the entire website, even after the prohibited material had been removed from it (see paragraph 30 of the judgment).

It is clear that the court ordered the Internet provider to use a wholly inadequate method to block access to the e-book on the applicant's website. We concur in the judgment where it states that "extending the scope of the blocking order far beyond the illegal content which had originally been targeted ... did not have a legal basis in the circumstances of the present case" (see paragraph 34 of the judgment). We also agree, *a fortiori*, that "there was no legal basis for ... the continued blocking of the website after [the unlawful content (the e-book)] had been removed" (see paragraph 38 of the judgment).

In our opinion, the lack of a basis in domestic law in itself suffices to conclude that the interference was not "prescribed by law".

4. We agree, however, with our esteemed colleagues that there has been additionally a deficiency in the way in which the present case was handled at the domestic level.

The judgment indeed criticises Russian law for "[not requiring] any form of involvement of the website owner, such as the applicant, in blocking proceedings conducted under section 10(6) of the Information Act" (see paragraph 35 of the judgment).

5. In sum, the interference violated the Convention for two reasons: firstly, the blocking order was adopted in proceedings which did not allow the applicant to defend his rights; secondly, the order exceeded the limits of what was a permissible interference under domestic law.

In order to properly execute the present judgment, it will be for the legislature to amend the law so that website owners have an opportunity to properly defend their rights and to avoid the blocking of their websites (or a page thereof) by removing any illegal content. It will also be for the prosecutors and the courts to pay due attention to the formula to be used for the blocking of a webpage. If, as the applicant contends, there is a lack of technical expertise on the part of the judges (see paragraph 33 of the judgment), then there is a need for proper training of judges dealing with this kind of case.