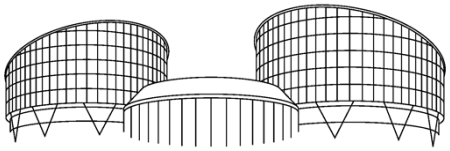

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF ENGELS v. RUSSIA

(Application no. 61919/16)

JUDGMENT

Article 10 • Freedom to receive and impart information • Website owner compelled to remove information on filter-bypassing tools, which was arbitrarily banned by court, in order to avoid blocking of his entire website • Information technologies content-neutral • Sweeping measure solely based on the fact that the impugned material might enable malevolent access to extremist content on other unrelated websites • Interference with access to all content which might be accessed using the technologies in issue • Vague and overly broad legal provision not giving any indication as to nature or categories of content susceptible to be banned • Domestic law lacking foreseeability and 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 • No prior assessment of impact and immediate enforcement of the blocking measure depriving interested parties of the opportunity to appeal • Domestic courts' failure to perform a Convention-compliant review weighing up various interests at stake and to consider legitimate purposes of the impugned technologies
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 Engels 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,
María Elósegui,
Gilberto Felici,
Erik Wennerström, *judges,*
and Milan Blaško, *Section Registrar,*

Having regard to:

the application (no. 61919/16) 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 German national, Mr Grégory Engels ("the applicant"), on 11 October 2016;

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 decision by the German Government not to exercise their right to intervene in the proceedings under Article 36 § 1 of the Convention;

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 a decision by the Russian courts that information about unfiltered-browsing technologies available from the applicant's website constituted prohibited content.

THE FACTS

1. The applicant was born in 1976 and lives in Offenbach, Germany. He was represented by Mr S. Darbinyan, a lawyer practising in Moscow.

2. The Government were represented initially by Mr A. Fedorov, head of the office of the Representative of the Russian Federation to the European Court of Human Rights, and then by Mr M. Galperin, the Representative.

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

4. The applicant is a Russian-born German politician and activist working to support freedom of expression on the Internet. In 2012, he founded, together with local Russian activists, the RosKomSvoboda website (rublacklist.net) dedicated to news, information, analysis and research relating to freedom of expression online,

online privacy issues, copyright and digital communications. Its name is an abbreviation for "Russian Committee for Freedom", an allusion to the name of the Russian telecoms regulator Roskomnadzor ("Russian Committee for Oversight"), which maintains a list of proscribed online content.

5. One page of the RosKomSvoboda website (rublacklist.net/bypass) provided a list and a short description of tools and software for bypassing restrictions on private communications and content filters on the Internet, such as virtual private networks (VPN), the Tor browser, the "invisible Internet" (I2P) technology, the "turbo" mode in web browsers, and the use of online translation engines for accessing content.

6. In 2015, a district prosecutor in the Krasnodar Region lodged a public-interest claim with the Anapa Town Court, seeking a decision that information on the rublacklist.net/bypass page should be prohibited from dissemination in Russia. The prosecutor submitted that the anonymising tools available from that page enabled users to access extremist material on another, unrelated website. On 13 April 2015 the Anapa Town Court, without informing the applicant about the proceedings, granted the prosecutor's application. It noted that the information on the rublacklist.net/bypass page had been made freely available without a password or registration to any user who wished to read or copy it. The Town Court declared illegal the content of the rublacklist.net/bypass page and ordered Roskomnadzor to enforce the decision immediately by blocking access to the applicant's website.

7. Roskomnadzor asked the applicant to take down the webpage rublacklist.net/bypass, otherwise the website would be blocked. The applicant complied with the request and deleted the offending information.

8. Counsel for the applicant lodged an appeal. He pointed out that the applicant's full contact details were listed on the website and that the examination of the prosecutor's claim in his absence had breached the principle of fairness. He also submitted that providing information about tools and software for the protection of the privacy of browsing was not contrary to any Russian law.

9. On 29 September 2015 the Krasnodar Regional Court rejected the appeal in a summary fashion, without addressing the applicant's arguments.

RELEVANT DOMESTIC LEGAL FRAMEWORK

10. Section 3 of the Information Act (Federal Law no. 149-FZ of 27 July 2006) establishes legal principles governing access to information and information technologies. Principle 1 guarantees the freedom to search for, receive, impart, create and disseminate information by all legal means. Principle 2 requires that any restriction on access to information be set out in a federal law. Principle 8 prohibits legal regulations from favouring the use of particular information technologies.

11. Section 15.1 gives the telecoms regulator, Roskomnadzor, the authority to maintain the Integrated Register of domain names, webpage references (URL) and network addresses of websites featuring content which is banned in the Russian Federation. Subsection (5) provides for three grounds on which content may be deemed illegal and added to the Integrated Register: first, where the competent executive body has decided that the material falls under any of seven categories of illegal content, such as child pornography, the manufacture or use of narcotics, or methods of suicide; secondly, where a "judicial decision ... identified particular

Internet content as constituting information the dissemination of which should be prohibited in Russia"; and thirdly, where a bailiff has issued an order restricting access to libellous information. Subsection (7) requires the web hosting service provider – immediately upon being notified by Roskomnadzor that illegal content has been added to the Integrated Register – to inform the website's owner and ask him or her to remove that content.

RELEVANT INTERNATIONAL MATERIAL

12. 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 ..."

13. 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 ..."

14. 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."

15. 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:

"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 ..."

16. 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

17. The applicant complained that the decision requiring him to remove information from his website had been in breach of Article 10 of the Convention, which reads in the relevant parts:

> "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

18. 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

19. The Government submitted that the web tools described on the page rublacklist.net/bypass had enabled users to gain unlimited access to prohibited extremist material, including a collection of material on the Federal List of Extremist Material. The Anapa Town Court had correctly granted the prosecutor's application seeking the blocking of access to that content. The legal framework for updating the Integrated Register had been sufficiently clear and foreseeable in its application, and Roskomnadzor's decision to add the page to the Integrated Register of banned content had been a legal, justified and necessary measure. Since the applicant had taken down the offending page, access to his website had not been blocked. The Government concluded that there had been no violation of Article 10.

(b) The applicant

20. The applicant submitted that there had been interference with his right to impart information, because he had been forced to take down legitimate content in order to avoid having his entire website blocked. The Russian authorities had not cited any legal provision restricting information about tools for filter-free browsing; nor had they shown that the impugned page had contained any extremist

or terrorist material. The requirement to take it down had breached principle 8 in section 3 of the Information Act, which prohibited preferential treatment of particular information technologies. The second part of section 15.1(5), on which the interference had been based, did not meet the foreseeability requirement. It allowed courts to pronounce any content illegal, without specifying the nature or category of such content. Website owners, such as the applicant, could not have known in advance whether a particular publication would lead to a take-down order or blocking of the website. The legal framework governing blocking orders lacked precision and permitted wholesale blocking of access to a website on the grounds that it contained some offending material. The applicant pointed out that Russian legislation provided website owners with no safeguards against abuse.

(c) Third-party interveners

21. 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 as 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.

22. 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, an organisation defending freedom of the press, emphasised that any law providing for blocking powers should specify the categories of content that could be lawfully blocked. The blocking of information about virtual private networks (VPN) and similar technologies could never be justified because such technologies were content-neutral and blocking interfered with access to all content which might be obtained using those technologies. Accordingly, the blocking of such technologies was inherently incapable of being defined by reference to categories of legitimately proscribed content. 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 was 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.

23. 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

24. 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).

25. The applicant is the owner and administrator of a website dedicated to the protection of freedom of expression online and digital privacy. Unbeknownst to him, in April 2015 a Russian court determined that a section of his website constituted banned information and required the telecoms regulator to immediately block access to the entire website. The blocking measure was not actually implemented, since the applicant had removed the offending content upon receiving Roskomnadzor's request to that effect. The Court notes that the applicant was confronted with a choice between removing the allegedly illegal content and having access to his entire website blocked. The court's decision that the content of one of his webpages was illegal caused the applicant to take it down in order to avoid the blocking measure and also prevented visitors to the website from accessing that content. It amounted therefore 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)). Such 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.

26. 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).

27. The statutory basis for the interference was section 15.1 of the Information Act. Subsection (5) of that provision lists three types of decisions by which the Russian authorities may categorise online content as illegal. In the instant case, the decision was made by a court of general jurisdiction in accordance with the second part of subsection (5). Unlike the first part of that subsection, which defined seven particular categories of online content susceptible to blocking, or the third part, which referred expressly to libellous content, the second part allowed websites to be blocked on the basis of a "judicial decision which identified particular Internet content as constituting information the dissemination of which should be prohibited in Russia". The Court finds that the breadth of this provision is exceptional and unparalleled. It does not give the courts or website owners any indication as to the nature or categories of online content that is susceptible to be banned. Nor does it refer to any secondary legislation, by-laws or regulations which could have circumscribed its scope of application. The Court finds that such a vague and overly broad legal provision fails to satisfy the foreseeability requirement. It does not afford website owners, such as the applicant, the opportunity to regulate their conduct, as they cannot know in advance what content is susceptible to be banned and can lead to a blocking measure against their entire website.

28. The present case illustrates the manner in which this legal provision is capable of producing arbitrary effects in practice. Following an application lodged by a town prosecutor, a Russian court held that the information about filter-bypassing tools and software available on the applicant's website constituted "information the dissemination of which should be prohibited in Russia". It did not establish that filter-bypassing technologies were illegal in Russia or that providing information about them was contrary to any Russian law. Nor did it find any extremist speech, calls for violence or unlawful activities, child pornography, or any other prohibited content on the applicant's webpage. The only basis for its decision was the fact that filter-bypassing technologies might enable users to access extremist content on some other website which was not connected or affiliated with the applicant and the content of which he had no control over.

29. The Court notes that the utility of filter-bypassing technologies cannot be reduced to a tool for malevolently seeking to obtain extremist content. Even though the use of any information technology can be subverted to carry out activities which are incompatible with the principles of a democratic society, filter-bypassing technologies primarily serve a multitude of legitimate purposes, such as enabling secure links to remote servers, channelling data through faster servers to reduce page-loading time on slow connections, and providing a quick and free online translation. None of these legitimate uses were considered by the Russian court before issuing the blocking order.

30. The Court notes that all information technologies, from the printing press to the Internet, have been developed to store, retrieve and process information. As the third-party interveners and the UN Human Rights Committee pointed out, information technologies are content-neutral (see paragraphs 15 and 22 above).

They are a means of storing and accessing content and cannot be equated with content itself, whatever its legal status happens to be. Just as a printing press can be used to print anything from a school textbook to an extremist pamphlet, the Internet preserves and makes available a wealth of information, some portions of which may be proscribed for a variety of reasons particular to specific jurisdictions. Suppressing information about the technologies for accessing information online on the grounds they may incidentally facilitate access to extremist material is no different from seeking to restrict access to printers and photocopiers because they can be used for reproducing such material. The blocking of information about such technologies interferes with access to all content which might be accessed using those technologies. In the absence of a specific legal basis in domestic law, the Court finds that such a sweeping measure was arbitrary.

31. 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 considers that the breadth of the discretion afforded by subsection (5)(2) of section 15.1 of the Information Act is such that it is likely to be difficult, if not impossible, to challenge the court's decision on appeal (see *Kablis v. Russia*, nos. 48310/16 and 59663/17, § 96, 30 April 2019). It also finds that the Russian law did not provide website owners, such as the applicant, with any procedural safeguards capable of protecting them against arbitrary interference. It did not require any form of involvement of the website owners in the blocking proceedings conducted under section 15.1 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. Even though the applicant's contact details had featured prominently on the website, he had not been informed or invited to explain the purpose of the information about unfiltered-browsing technologies. The Town 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 Internet service provider (ISP).

32. The Court finds that the participation of a local ISP as the designated defendant was not sufficient to endow the proceedings with an adversarial character. The ISP provides a connectivity technology enabling users to access millions of websites which 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, 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. Neither the prosecutor nor the Town Court made any assessment of the impact of the blocking measure prior to its implementation; nor did they explain the urgency of enforcing it immediately without giving the interested parties the opportunity to lodge an appeal.

33. Lastly, as regards the proceedings which the applicant instituted to challenge the blocking order, the Court notes that 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). In reaching the decision, the Regional Court did not seek to weigh up the various interests at stake. It confined its scrutiny to establishing formal compliance with the letter of the law. However, in the Court's view, a Convention-compliant review should have taken into consideration, among other elements, the fact that a blocking measure, by rendering large quantities of legitimate information inaccessible, substantially restricted the rights of the website owner and of Internet users, and had a significant collateral effect (see *Ahmet Yıldırım*, cited above, § 66).

34. The Court reiterates that 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 sweeping blocking measures, such as those in issue in the instant case. In the light of its examination of the Russian legislation as applied in the instant case, the Court concludes that the interference resulted from the application of the procedure under subsection (5)(2) of section 15.1 of the Information Act which did not satisfy the foreseeability requirement under the Convention and did not afford the applicant the degree of protection from abuse to which he was entitled by the rule of law in a democratic society. 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.

35. 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

36. The applicant complained that the Russian courts had not involved him in the blocking proceedings or considered the merits of his arguments on appeal. The Court considers that this complaint falls to be examined under Article 13 of the Convention, taken in conjunction with Article 10. Article 13 reads as follows:

> "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

37. 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

38. 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, there had been no violation of his rights.

39. The applicant emphasised that the domestic remedies had not been effective. He had not been involved in any capacity in, or at least informed of, the proceedings in which the content had been banned. The appellate court had not considered the nature or the contents of his website, or the manner in which the first-instance court's decision had affected his rights.

40. 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.

41. 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.

42. 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.

43. Although the applicant was able to lodge an appeal against the blocking order, the appellate court did not consider the substance of his grievance. Nor did it address the specific nature of the information about particular technologies or examine the necessity and proportionality of the blocking measure. 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).

44. 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

45. 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."

46. The applicant claimed 10,000 euros (EUR) in respect of non-pecuniary damage.

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

48. The Court awards the applicant the amount claimed in respect of non-pecuniary damage, plus any tax that may be chargeable.

49. 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, EUR 10,000 (ten thousand euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;
   (b) that from the expiry of the above-mentioned three months until settlement, simple interest shall be payable on the above amount 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 Registrar	Paul Lemmens President