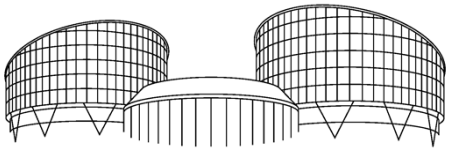

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF VLADIMIR KHARITONOV v. RUSSIA

(*Application no. 10795/14*)

JUDGMENT

Article 10 • Freedom to receive and impart information • Website blocked as automatic consequence of blocking order against another with same IP address • Wholesale blocking of access to an entire website being an extreme measure comparable to banning a newspaper or television station • Manner of implementation of blocking order having practical effect of extending its scope on co-hosted websites and thus far beyond illegal content originally targeted • Domestic law lacking foreseeability and safeguards against excessive and arbitrary effects of blocking measures • Extensive latitude conferred on the Russian telecoms regulator (Roskomnadzor) • No legal requirement to conduct an assessment of impact and potential collateral effects of a blocking measure prior to its implementation • Blocking measures not sanctioned by court or other independent adjudicatory body • No provision for third-party notification of blocking decisions and no access to decision • Domestic courts's failure to perform a Convention-compliant review weighing up various interests at stake
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 Vladimir Kharitonov 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 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 Vladimir Vladimirovich Kharitonov ("the applicant"), on 27 December 2013;

the decision to give notice of the application to the Russian Government ("the Government");

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

the comments submitted by third-party interveners which 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 blocking of access to the applicant's website as a consequence of a blocking order against another website which had the same IP address as the applicant's website.

THE FACTS

1. The applicant was born in 1969 and lives in Moscow. He was represented by Mr D. Gaynutdinov, a lawyer admitted to practice in Russia.

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 the executive director of the Association of Electronic Publishers, a non-commercial partnership, and co-founder of the Association of Internet Users, a non-governmental organisation. He is the

owner and administrator of the website Electronic Publishing News (http://www.digital-books.ru), which features a compilation of news, articles and reviews about electronic publishing.

5. The website was set up 2008 and was hosted by DreamHost, a provider of a shared web-hosting service based in the United States. The service hosts multiple websites which have the same numerical network address ("Internet protocol or IP address") but different domain names. When a user's browser requests a website from the server, it includes the requested domain name as part of the request. The server uses this information to determine which website it would show the user.

6. In late December 2012, users from various Russian regions reported to the applicant that access to his website was blocked by their Internet service providers by reference to "a decision by the competent Russian authority". He checked the register of websites black-listed by the Russian telecoms regulator (Roskomnadzor) and discovered that the IP address of his website had been put on the blocking list pursuant to a decision of the Federal Drug Control Service dated 19 December 2012. The decision was intended to block access to another website, rastaman.tales.ru – a collection of cannabis-themed folk stories "The Rastaman Tales"[1] – which was also hosted by DreamHost and had the same IP address as the applicant's website. According to the Government, on 22 March 2013 the blocking of the IP address ceased; copies of the blocking and unblocking decisions have not been made available to the applicant or the Court.

7. The applicant complained to the Taganskiy District Court in Moscow that the decision to block the entire IP address had had the effect of blocking access to his website which did not contain any illegal information.

8. On 19 June 2013 the District Court rejected the applicant's complaint, holding that Roskomnadzor had acted within its competence, in accordance with the applicable laws and for the purpose of protecting children from harmful information relating to the use of drugs. It did not assess the impact of the contested measure on the applicant's website.

9. The applicant appealed, relying in particular on the Court's findings in the case of *Ahmet Yıldırım v. Turkey* (no. 3111/10, ECHR 2012), which concerned the indiscriminate blocking of a hosting service.

10. On 12 September 2013 the Moscow City Court dismissed the appeal in a summary fashion, finding that the principle of proportionality had been respected because Roskomnadzor had lawfully blocked access to illegal information. It did not address the effect of the blocking decision on the applicant's website.

[1] Currently available, in Russian and English, at www.rastamantales.com Access to the website was not restricted in Russia as on the date of the judgment.

11. On 17 July 2014 the Constitutional Court refused to consider an application lodged by the applicant for a constitutional review of section 15.1 of the Information Act. The court held:

> "As regards the owners of websites that do not contain any prohibited information, who had seen access to their websites blocked as a consequence of having their network address added to the register, what affected their right to impart information was not, in essence, the decision to add the network address to the Integrated Register but the failure on the part of the hosting service provider to act diligently. Accordingly, their right to impart information must be asserted, first and foremost, in their legal relationship with the hosting service provider."

RELEVANT DOMESTIC LEGAL FRAMEWORK

12. On 28 July 2012 a new section 15.1 was added to the Information Act (Federal Law no. 149-FZ of 27 July 2006). It established the Integrated Register of domain names, webpage references (URL) and network addresses of websites featuring content which is banned in the Russian Federation (subsection 1). The telecoms regulator Roskomnadzor is responsible for updating the Integrated Register (subsection 3). Pursuant to a decision by the competent executive body, it lists websites featuring prohibited content, of which there are seven categories, including information relating to the manufacture and use of narcotics (subsection 5(1)(b)). The decision to list the website may be challenged before a court by the website's owner, hosting service provider or Internet service provider (subsection 6). Immediately on receiving notification that a website has been listed, the hosting service provider must inform the website's owner and ask him or her to remove the unlawful content (subsection 7). If the owner fails to react, the hosting service provider must block access to the website (subsection 8). In the absence of any reaction from the hosting service provider and the website's owner, the website's IP address is added to the Integrated Register (subsection 9) and Internet service providers must block access to it (subsection 10).

13. On 26 October 2012 the Government approved regulations on establishing, compiling and maintaining the Integrated Register of domain names, webpage references (URL) and network addresses of websites containing prohibited content (Resolution no. 1101). The regulations set out the procedure for implementing section 15.1 of the Information Act.

RELEVANT INTERNATIONAL MATERIAL

14. 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 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."

15. 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 ..."

16. 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."

17. In General Comment No. 34 on Article 19 of the International Covenant on Civil and Political Rights, 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. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3 ..."

18. *The rule of law on the Internet and in the wider digital world*, an issue paper published by the Council of Europe Commissioner for Human Rights in 2014, identified some of the deficiencies of the blocking system: (i) blocking, notably when performed by software or hardware that reviews communications, is inherently likely to produce (unintentional) false positives (blocking sites with no prohibited material) and false negatives (when sites with prohibited material slip through a filter); (ii) the criteria for blocking certain websites, but not others, and the lists of blocked websites, are very often opaque at best, and secret at worst; (iii) appeal processes may be onerous, little known or non-existent, especially if the decision on what to block or not block is – deliberately – left to private entities.

19. 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

20. The applicant complained that the Russian authorities' decision to block access to the offending website by blacklisting its IP address had had the disproportionate collateral effect of blocking access to his website. That measure had breached his rights under Article 10 of the Convention, which reads:

"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

21. 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 applicant

22. The applicant accepted that the blocking of access to information about the production and use of drugs could have pursued a legitimate aim. However, the scope and manner of the interference had been disproportionate to that aim. "The Rastaman Tales" was a crowd-sourced collection of comic and folk stories about cannabis. It targeted an adult audience and could not be compared to a practical guide on the manufacture or use of drugs. The stories had been published many times in book format and nominated for a prestigious Russian literary award. Indeed, after the website had been blocked, it had been legally sold in paper form for many years and remained available from multiple sources on the Internet. The authorities' decision to block access to one of many copies of the collection had failed to achieve the aim they had set out to achieve and had also caused substantial and unjustified damage to the applicant's right to freedom to impart information.

23. The applicant pointed out that he had used his website to publish news, which was, in the Court's words, "a perishable commodity" losing its value and interest in the event of delayed publication, even for a short period (he referred to Observer *and* Guardian *v. the United Kingdom*, 26 November 1991, § 60, Series A no. 216). By the time the blocking measure had been taken, his website had existed for four years; it had been indexed by search engines and enjoyed a steady readership. Moving to a different platform would have involved a dip in the number of readers and investment of considerable time and resources. It would also have cut off access to the website's four-year archive of publications. Most importantly, structural defects in the Russian Internet law made it entirely possible that any alternative platform would be subject to a similar wholesale blocking order for reasons unconnected to the applicant and outside his control. The Russian authorities had publicly stated many times that they were prepared to block Facebook and Google; as of October 2017, over 3,900,000 websites, which did not have any illegal content but shared an IP address with others that did, were blocked in Russia.

24. The blocking decision had not been produced in the domestic proceedings – the courts had rejected his disclosure request in that respect – and the Government had not submitted it to the Court, either. He had in no way been connected to the offending website or Internet service provider (ISP) and could not have been aware of any steps they might have taken for the protection of their rights. As a good-faith website owner he had been at the mercy of three actors, over which he had had no leverage: the Russian authorities, the owner of the offending website, and the hosting service

provider. Both the website owner and the hosting service provider were non-Russian legal entities and could not have been expected to comply with demands by the Russian authorities. The existing provisions of Russian law offered no protection to owners of law-compliant websites which happened to have the same IP address as those with unlawful content. The law did not require Roskomnadzor to assess the impact of its blocking decision on such websites.

(b) The Government

25. The Government submitted that the blocking of the offending website, rastaman.tales.ru, had pursued an important policy objective, namely to restrict information about the manufacture and use of drugs. The telecoms regulator, Roskomnadzor, had not immediately entered the offending website's IP address in the register of banned websites. First, it had notified the hosting service provider, in Russian and English, that the website contained unlawful information. Only after the provider had failed to remove the offending information, five days later, had Roskomnadzor added the website's IP address to the Integrated Register. The way in which Roskomnadzor had proceeded had been in strict compliance with subsection 9 of section 15.1 of the Information Act and constituted a legal, justified and necessary measure. The law did not require Roskomnadzor to notify owners of all websites which shared an IP address with a blocked website. They could check the existence of restrictions by filling in a form on the Integrated Register's website.

26. In the Government's submission, the fact that the hosting service provider had been given prior notification and that the blocking order had been implemented by private ISPs distinguished the present case from the case of *Ahmet Yıldırım v. Turkey* (no. 3111/10, ECHR 2012). In that case, the Turkish criminal court had not informed Google before blocking its hosting services and the blocking order had been applied directly by the State telecoms directorate. In the present case, the applicant had not brought proceedings against the ISP, requesting the court to assess whether the blocking of the IP address was the only method available for restricting access to the offending website. The Government contended that, unlike Russia, Turkey had banned thousands of websites, including popular services such as YouTube, GeoCities and Dailymotion (they referred to *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, ECHR 2015 (extracts), which concerned the blocking of YouTube).

27. The Government submitted that the applicant was not a victim of the alleged violation, in the same way as a Turkish user of a music-streaming website had been merely indirectly affected by the blocking of that website (they referred to *Akdeniz v. Turkey* (dec.), no. 20877/10, 11 March 2014). The applicant could have carried on publishing information about the electronic book industry on other websites, platforms and online resources,

such as LiveJournal, YouTube or Facebook. Access to his website had been restricted for a short period of time not exceeding three months. He had not shown that the owner of the offending website or the ISP had challenged the blocking decision. The Russian courts had correctly established that the measures taken by Roskomnadzor had sought to forestall circulation of unlawful information and that the relevant provisions of the domestic law had provided the applicant with a sufficient degree of protection against arbitrary interference.

28. Lastly, the Government cited the provisions of the British, French, German, Chinese and United States law relating to the suppression of child pornography and concluded that all States, without exception, provided for some form of filtering of Internet material. The Government also dismissed the submissions by third-party interveners as irrelevant to the subject matter of the present case.

(c) Third-party interveners

29. Access Now, a global civil-society organisation defending the digital rights of users at risk, submitted that an assessment of proportionality of restrictions on freedom of expression, including website blocking, should include both substantive (what is blocked) and procedural (how it is blocked) elements. The level of safeguards must be appropriate to the nature of allegedly illegal content. Website blocking interferes with the core of the right to freedom of expression, and affected individuals must be notified and granted adequate remedies to challenge blocking measures.

30. ARTICLE 19, a global campaign for freedom of expression, and the Electronic Frontier Foundation, a legal and policy organisation safeguarding privacy in the digital world, emphasised that blocking access to entire websites was an extreme and disproportionate measure. It was analogous to banning a newspaper or television station, and was incapable of distinguishing between lawful and unlawful content. Any order to block access to content should be as narrowly targeted as possible and be the least restrictive means to deal with the alleged unlawful activity. It must take into consideration the overall effectiveness of the measure and the risks of "over-blocking" other lawful content, including by reference to the technologies available to comply with the order. The interveners cited judgments from European high courts, which concurred that blocking websites by IP address carried a greater risk of undesirable effects on third parties and of "over-blocking" (they cited the Antwerp Court of Appeals judgment of 26 September 2011 in *VZW Belgian Anti-Piracy Federation v. NV Telenet*, 2010/AR/2541; two United Kingdom High Court judgments, *Dramatico Entertainment Limited & Ors v. British Sky Broadcasting Ltd & Ors (No. 2)* [2012] EWHC 1152 (Ch), and *Cartier International AG & Ors v. British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch); and the Federal Court of Justice judgment of 26 November 2015 in the

3dl.am case, (BGH) I ZR 3/14). Consistent with international standards, the law should provide for the following procedural standards: (i) blocking should be ordered by a court or an independent adjudicatory body; (ii) ISPs and other interested parties should be given the opportunity to intervene in proceedings in which a blocking order is sought; (iii) users and victims of collateral blocking should have the right to challenge, after the fact, the blocking order; (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.

31. The European Information Society Institute, a Slovakia-based non-profit organisation focusing on high-technology law, pointed out that Russia's implementation of website blocking led to collateral website blocking on a massive scale and lacked adequate safeguards against abuse. As of 28 June 2017, 6,522,629 Internet resources had been blocked in Russia, of which 6,335,850 – or 97% – had been blocked collaterally, that is to say, without legal justification. At various times, due to collateral blocking, Russian users were not able to access widely-used Internet services such as Google, Wikipedia, Web Archive, Reddit, Amazon Web Services and Disney. In addition, the Russian blocking system had vulnerabilities that facilitated over-blocking and abuse, such as the possibility to change unilaterally the IP address of a blocked website to the IP address of any other website, rendering it immediately unavailable for Russian users. An approach to website blocking which was based on the principle of proportionality called for an assessment of the positive and negative effects of a blocking order in each particular case and the choice of the method of its implementation. If it was predictable that ISPs would choose the IP address blocking technique because of its lower cost, the State should bear a higher burden in order to create conditions for a human-rights compliant manner of blocking content.

32. RosKomSvoboda, a Russian non-governmental organisation supporting open self-regulatory networks and the rights of digital users, submitted that the legal framework for blocking online content, as it had existed at the material time, had led to unpredictable consequences and the untargeted blocking of websites. It had not provided an effective mechanism for challenging blocking orders because a bona fide website owner would discover the existence of such an order only after it had become effective.

2. The Court's assessment

33. 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*, cited above, §§ 48-54).

34. The applicant has been the owner and administrator of a website featuring content relating to the production and distribution of electronic books, from news to analytical reports to practical guides. The website has existed since 2008 and has been updated several times a week. It has been stored on the servers of a US-based company offering accessible shared web-hosting solutions. The applicant's website has a unique domain name – "www.digital-books.ru" – but shares a numerical network address ("IP address") with many other websites hosted on the same server.

35. In December 2012, the applicant discovered that access to his website had been blocked. This was an incidental effect of a State agency's decision to block access to another website which was hosted on the same server and had the same IP address as the applicant's website. 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).

36. The applicant was not aware of the proceedings against the third-party website, the grounds for the blocking measure or its duration. He did not have knowledge of, or control over, when, if ever, the measure would be lifted and access to his website restored. He was unable to share the latest developments and news about electronic publishing, while visitors to his website were prevented from accessing the entire website content. It follows that the blocking measure in question 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*, cited above, § 56). 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.

37. 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).

38. In the instant case, the statutory basis for the interference was section 15.1 of the Information Act. That provision defines the categories of illegal web content susceptible to be blocked and lays down a step-by-step procedure for putting a blocking order in place. The Russian authorities relied on that provision to block access to an online collection of cannabis-themed stories known as "The Rastaman Tales". The Court notes with concern that section 15.1 allows the authorities to target an entire website without distinguishing between the legal and illegal content it may contain. Reiterating 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, the Court considers that a legal provision giving an executive agency so broad a discretion carries a risk of content being blocked arbitrarily and excessively (see paragraphs 15 and 16 above).

39. The fact remains, however, that while the offending website featured at least some arguably illegal content, the applicant's website did not have any content falling within the scope of section 15.1 (compare *Ahmet Yıldırım*, cited above, § 60). The applicant was in no way affiliated with the owners of the offending website or responsible for the allegedly illegal content. The interference in issue could not therefore have been grounded on the provision that was supposed to have formed its legal basis.

40. As it happened, the blocking of the applicant's website was an automatic consequence of Roskomnadzor's decision to add the IP address of the offending website to the register of blocked material. That decision had the immediate effect of blocking access to the entire cluster of websites hosted by DreamHost which shared an IP address with the offending website. It was issued in compliance with subsection 9 of section 15.1, which allowed Roskomnadzor to enter the IP address of the offending website in the Integrated Register of blocked content. However, the Court's scrutiny of the lawfulness requirement is not limited to establishing whether the State agency acted in accordance with the letter of domestic law. The Court must also ascertain whether the quality of the law in question enabled the applicant to regulate his conduct and protected him against arbitrary interference.

41. Section 15.1 of the Information Act conferred extensive powers on Roskomnadzor in the implementation of a blocking order issued in relation to a specific website. Roskomnadzor can place a website on the Integrated Register of blocked content, ask the website owner and its hosting service provider to take down the illegal content, and add the website's IP address

to the Integrated Register if they refuse to do so or fail to respond. However, the law did not require Roskomnadzor to check whether that address was used by more than one website or to establish the need for blocking by IP address. That manner of proceeding could, and did in the circumstances of the present case, have the practical effect of extending the scope of the blocking order far beyond the illegal content which had been originally targeted (see *Ahmet Yıldırım*, cited above, § 63). In fact, as the applicant and third-party interveners pointed out, millions of websites have remained blocked in Russia for the sole reason that they shared an IP address with some other websites featuring illegal content (see paragraphs 23 and 31 above).

42. Shared hosting is a common and accessible hosting arrangement for small to medium-sized websites. However, owners of individual sites, such as the applicant, may not be aware of the contents of co-hosted websites, while the hosting service provider – in this case a company outside the Russian jurisdiction – is not bound by Russian authorities' determination of illegal content. Whichever shared-hosting platform solution the applicant were to choose, he would incur the risk that the Russian authorities would declare illegal some content of co-hosted websites and that the owners of such websites and the hosting service provider would not heed their take-down orders. Russian law does not require the applicant to control the content of co-hosted websites or the hosting service provider's compliance with take-down orders. Yet, because of the great latitude the law afforded to Roskomnadzor in blocking matters, the applicant had to bear the consequences of the authorities' blocking decision merely on account of an incidental connection, at the infrastructure level, between his website and someone else's illegal content. In such circumstances, the Court cannot find that the law is sufficiently foreseeable in its effects and affords the applicant the opportunity to regulate his conduct.

43. Turning next to the issue of safeguards against abuse which domestic legislation must provide in respect of incidental blocking measures, the Court reiterates that the exercise of powers to interfere with the right to impart information must be clearly circumscribed to minimise the impact of such measures on the accessibility of the Internet. In the instant case, Roskomnadzor gave effect to a decision by which a drug-control agency had determined the content of the offending website to be illegal. Both the original determination and Roskomnadzor's implementing orders had been made without any advance notification to the parties whose rights and interests were likely to be affected. The blocking measures had not been sanctioned by a court or other independent adjudicatory body providing a forum in which the interested parties could have been heard. Nor did the Russian law call for any impact assessment of the blocking measure prior to its implementation. The Government acknowledged that Roskomnadzor was not legally required to identify the potential collateral effects of

blocking an IP address, even though commonly used Internet tools, such as "reverse IP address lookup", could have promptly supplied a list of websites hosted on the same server.

44. As regards the transparency of blocking measures, the Government submitted that the applicant should have consulted Roskomnadzor's website. Indeed, Roskomnadzor provides a web service (http://blocklist.rkn.gov.ru/) which enables anyone to find out whether a website has been blocked and indicates the legal basis, the date and number of the blocking decision and the issuing body. It does not, however, give access to the text of the blocking decision, any indication of the reasons for the measure or information about avenues of appeal. Nor does Russian legislation make any provision for third-party notification of blocking decisions in circumstances where they have a collateral effect on the rights of other website owners. The applicant had no access to the blocking decision: it had not been produced in the domestic proceedings and the Russian courts had rejected his disclosure request.

45. Lastly, as regards the proceedings which the applicant instituted to challenge the incidental effects of the blocking order, there is no indication that the judges considering his complaint sought to weigh up the various interests at stake, in particular by assessing the need to block access to all websites sharing the same IP address. 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 their decision, the courts confined their scrutiny to establishing that Roskomnadzor had acted in accordance 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 such a measure, by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect (see *Ahmet Yıldırım*, cited above, § 66).

46. 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 blocking measures, such as those in issue in the instant case. When exceptional circumstances justify the blocking of illegal content, a State agency making the blocking order must ensure that the measure strictly targets the illegal content and has no arbitrary or excessive effects, irrespective of the manner of its implementation. Any indiscriminate blocking measure which interferes with lawful content or websites as a collateral effect of a measure aimed at illegal content or websites amounts to arbitrary interference with the rights of owners of such websites. 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 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 (see *Ahmet Yıldırım*, cited above, § 67). 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.

47. 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

48. 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 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

49. 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

50. The Government submitted that the applicant could have brought a claim against the ISP or the hosting service provider whose failure to react to Roskomnadzor's warning had led to a restriction on his rights.

51. The applicant pointed out that Russia had over 3,500 ISPs in eighty-three regions. Lodging a claim against each of them was not an effective remedy. The law also granted ISPs a choice between blocking access to a website by its domain name or by its IP address. Their conduct would not be contrary to any legal provision irrespective of the blocking mode they might choose. In addition, the Russian courts had refused to carry out a proportionality assessment of the blocking order.

52. The third-party interveners, ARTICLE 19 and the Electronic Frontier Foundation, submitted that most European jurisdictions allowed ISPs to challenge blocking orders addressed to them, and few States explicitly provided victims of collateral blocking with a remedy. France and

the United Kingdom had established that users of the blocked website should be redirected to a page informing them of their right to challenge the blocking order.

53. The third-party intervener, the European Information Society Institute, submitted that both *ex ante* and *ex post* remedies for over-blocking needed to be implemented. *Ex ante* remedies should include prior notification to the owners of collaterally blocked websites, who could be identified by performing a "reverse IP address lookup" and creating a possibility to challenge a blocking order before it was implemented. *Ex post* remedies would enable the owner of a collaterally blocked website to lodge an appeal against the blocking order, limit the duration of blocking orders and ensure that instances of over-blocking were subsequently monitored.

54. 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.

55. 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 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.

56. Although the applicant was able to bring proceedings seeking a review of Roskomnadzor's blocking order and its effect on his website, the Russian courts refused to consider the substance of his grievance. They examined neither the lawfulness nor the proportionality of the effects of the blocking order on the applicant's website. 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).

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

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

58. 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."

59. The applicant claimed 20,000 euros (EUR) in respect of non-pecuniary damage and EUR 5,700 for costs and expenses. He submitted a copy of a legal-services contract with his representative before the Court.

60. The Government submitted that the amount claimed was excessive and that the applicant had not produced proof of payment.

61. The Court awards the applicant EUR 10,000 in respect of non-pecuniary damage, plus any tax that may be chargeable. Having regard to the amount of work which appears reasonable in the circumstances of the case, it awards him EUR 2,000 in respect of costs and expenses, plus any tax that may be chargeable on him.

62. 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 2,000 (two thousand 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;

5. *Dismisses* the remainder of the applicant's claim for just satisfaction.

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

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 with our esteemed colleagues in finding violations of Articles 10 and 13 of the Convention.

We would, however, have preferred a different reasoning under Article 10. Like our colleagues, we are of the opinion that the interference with the applicant's right to freedom of expression was not "prescribed by law". But unlike our colleagues, we believe that this is so because the interference had no basis in domestic law, not because the law did not satisfy the foreseeability requirement.

This issue is not a merely theoretical one. As we will try to explain, the approach adopted has a bearing on the kind of measures that will be required for proper execution of the present judgment.

2. The interference in this case was a blocking measure directed against the website "www.rastaman.tales.ru" (the "Rastaman Tales website"). The applicant's website was a different one (www.digital-books.ru), but both websites were hosted on the same server and had the same IP address. When the Federal Drug Control Service asked Roskomnadzor to block access to the Rastaman Tales website, Roskomnadzor put the latter's IP address on the register of blacklisted websites. The result was that access was blocked, not only to the Rastaman Tales website, but also to all other websites using the same IP address, including the applicant's.

This is therefore a case of the unintended blocking of a website due to the method chosen to block another, specifically targeted, website.

3. The impugned measure was based on section 15.1, subsection 5(1), of the Information Act. According to this provision, a website can be blocked by a decision of a federal executive body (in this case the Federal Drug Control Service) if it contains materials listed in that provision (in this case information relating to the manufacture and the use of narcotics). Roskomnadzor is responsible for implementing such decisions.

It is clear that Roskomnadzor used a wholly inadequate method to block access to the Rastaman Tales website. The question is whether this was the result of section 15.1, subsection 5(1), being insufficiently foreseeable in its effects, or whether Roskomnadzor exceeded the limits of what was permissible under the law. In the first case, the law would not be of the required quality; in the second case, the interference would not have a basis in the law.

4. Our esteemed colleagues are of the opinion that the Information Act did not require Roskomnadzor to check whether the IP address was used by more than one website or to establish the need for blocking by IP address (see paragraph 41 of the judgment). They further argue that "because of the great latitude" the Act afforded to Roskomnadzor in blocking matters, making it possible for the latter to block a website merely on account of an incidental connection at the infrastructure level with another website, the

law was not sufficiently foreseeable in its effects and did not afford the applicant the opportunity to regulate his conduct (see paragraph 42 of the judgment).

We respectfully disagree with this way of looking at the existing domestic legal framework.

5. In our opinion, the Information Act, and in particular section 15.1, subsection 5(1), defines in a sufficiently precise way the categories of information that are prohibited and to which therefore access can be blocked. We do not find that this provision gives "unfettered discretion" to the competent federal executive bodies.

It is true that the Act does not specify how Roskomnadzor should proceed when it receives a request to block a website. However, in our opinion it does not follow from the Convention that the manner of implementing a decision of an administrative authority should be regulated in detail by the legislature. This is all the more true when the implementation requires the taking of measures of a technical nature. To hold the contrary would lead to undesired over-regulation.

It was within Roskomnadzor's discretion to choose the method for implementation of the Federal Drug Control Service's request. Under the principle of the rule of law it was for Roskomnadzor to make sure that, whatever method was chosen, the scope of the blocking measure remained within the limits of what had been requested by the competent executive body.

Where the law grants discretion to an administrative authority, it is obvious that it does not allow that authority to exercise the power thus granted in a way that would violate the law. By using a method that had the effect of blocking the applicant's website, although that website did not feature any illegal content and was not the object of the Federal Drug Control Service's request, Roskomnadzor exercised its power in such a way that the blocking measure went beyond what was permissible under section 15.1, subsection 5(1), of the Information Act.

That means that the blocking measure applied by Roskomnadzor did not have a basis in domestic law.

6. We note that the domestic courts found that Roskomnadzor had acted within its competence and had implemented a decision that was compatible with the Information Act. In fact, they did not address the issue of the blocking measure's impact on the applicant's website (see paragraphs 8 and 12 of the judgment). They simply left open the question, which in our opinion is of decisive importance.

7. Our finding that the impugned measure did not have a basis in domestic law is sufficient to conclude that the measure was not "prescribed by law".

8. We thus consider that it is in the first place Roskomnadzor that is responsible for the violation of the applicant's rights, as it did not remain within the limits of the Information Act. We consider that the domestic

courts too are responsible, as they failed to identify the unlawful nature of Roskomnadzor's actions, failed to have regard to the criteria established in the Convention (see paragraph 45 of the judgment) and failed to restore lawfulness.

Our esteemed colleagues put the blame elsewhere. In their opinion it is the Information Act that is the source of the violation of the Convention. More precisely, it is because the Act is not sufficiently foreseeable as to its implementation that the interference in the present case is held not to be "prescribed by law". We respectfully disagree. We consider that the Russian Information Act is not as such incompatible with the Convention. The content of section 15.1, subsection 5(1), is in fact very similar to that of acts regulating the same issue in other States of the Council of Europe (see the 2017 comparative study on blocking, filtering and take-down of illegal internet content, conducted by the Swiss Institute of Comparative Law on behalf of the Council of Europe and available at https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet). In the present case, it is the *application* of the Act that is problematic.

9. This brings us to the issue of execution of the present judgment.

The problem encountered by the applicant is by no means an isolated one. As is noted in the judgment, millions of websites have been blocked merely because they shared an IP address with some websites featuring illegal content (see paragraph 41 of the judgment). The problem, if not systemic, is in any event widespread.

In our opinion, it would have been sufficient to change the administrative practice (of Roskomnadzor) and the judicial practice (of the domestic courts). Reparation within the meaning of the Convention could have been achieved without the legislature having to intervene.

However, given that the judgment concludes that section 15.1, subsection 5(1), of the Information Act does not satisfy the foreseeability requirement under Article 10 of the Convention, the full execution of the judgment will now require an amendment to the Act. We can only hope that this will be done within a reasonable time.

We would like to stress, however, that Roskomnadzor and the courts should not wait until the act has been amended in order to change their own practices. The execution of the judgments of the Court is a matter for *all* the domestic authorities concerned (see, specifically with respect to the duty of the domestic courts "to ensure, in conformity with their constitutional order ..., the full effect of the Convention standards, as interpreted by the Court", *Fabris v. France* [GC], no. 16574/08, § 75, ECHR 2013 (extracts)). Roskomnadzor and the courts can thus pave the way for a later amendment of the Information Act.