EUROPEAN INFORMATION SOCIETY INSTITUTE, O. Z.
Registration address: Štítová 1243/1 040 01 Košice, Slovakia
Postal address: Martin Husovec / EISi, TILT, P.O.Box 90153, 5000 LE Tilburg, The Netherlands
IČO: 42 227 950, www.eisionline.org, eisi@eisionline.org

12 January 2018

The Registrar
European Court of Human Rights
Council of Europe
F-67075 Strasbourg Cedex
France

Third Party Intervention Submission by
European Information Society Insitute (EISi)

In re *OOO FLAVUS against Russia and 4 other applications*
App. No. 12468/15

INTRODUCTION

- This third-party intervention is submitted on behalf of the European Information Society Institute (EISi), an independent non-profit organization based in Slovakia which focuses on the overlap between technology and law. EISi promotes human rights in a digital society by conducting impact litigation before the courts. It also serves as a research center for high technology law.
- EISi welcomes the opportunity to intervene as a third party in this case granted by the leave of the President of the Court on 29 November 2017 (ECHR-LE14.8bP3) pursuant to Rule 44 (3) of the Court. This submission does not take a position on the merits of the applicant's case.
- In our submission, we address mostly: (i) due process requirements, and (ii) availability of effective safe-guards against collateral over-blocking.

STARTING POINT

(1) As opposed to content removal that deletes information at the source, content blocking typically limits its accessibility for a specified audience. Because the Internet consists of different end-points and layers, website blocking may be attempted on several levels with different effects: (1) national level (where the access to a particular content, e.g. Facebook blocking in the whole country), (2) internet access provider level (e.g. by Orange or Deutsche Telekom for its own customers), (3) local network level (e.g. by schools and libraries for their visitors) and (4) the endpoint level (by using software within a computer for a particular user, e.g. due to parental control reasons).

(2) There are several types of content blocking measures.[1] The most often practiced techniques are IP address (e.g. 193.164.229.51 for www.coe.int website) and URL blocking (e.g. subpage www.echr.coe.int). The usual implementation of a blocking order on the access provider level disables access to an entire IP address. The problem is that such an address can be shared by several websites, which means the blocking affects also non-targeted websites. With URL blocking, on the other hand, a particular web address can be targeted. This means that a particular web address (e.g. www.hudoc.echr.coe.int) will be blocked while the rest of the services (e.g. www.echr.coe.int) remain unaffected. In that sense, URL blocking is more precise with a lower chance of collateral over-blocking.[2]

(3) In cases of content blocking, the states have to balance the fundamental rights when targeting particular content. Among the rights, the right to privacy, freedom to conduct business, and freedom of expression are the most affected. Once the blocking goes beyond its purpose, because it also over-blocks also legitimate content, it should no longer be acceptable in a democratic society.[3] In order to truly respect this distinction in practice, especially given the high risks of over-blocking, a number of due process requirements have to be put in place. After issuing blocking orders, it is more difficult to control implementation by the private parties. *Kharitonov v Russia* (App. No. 10795/14) highlights how particular technological choices implemented by intermediaries substantially matter for enjoyment of freedom of expression. In that

[1] See Internet Society, Internet Society Perspectives on Internet Content Blocking: An Overview, 2017, 2017, available at: <https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/>

[2] European Information Society Institute, Third Party Intervention Submission by European Information Society Institute (EISi) In re Kharitonov v Russia, App. No. 10795/14, 2017, available at: <http://www.eisionline.org/files/Interventions/web-kharitonov-russia.pdf >

[3] M. Husovec, Injunctions Against Intermediaries in the European Union: Accountable But Not Liable? (Cambridge University Press, 2017), p. 133

case, a domestic blocking scheme led to an outcome where 97% of all blocked Internet content in Russia is an unintended "side effect" of efforts to limit access to 3% targeted websites. The cause are all mostly implementing choices of private parties.

(4) Delegated enforcement shifts responsibility from the state to private entities, which are as a result given "new power" to decide as private gatekeepers whose content should be subject to blocking.[4] Given the fact that "the State cannot absolve itself from responsibility by delegating its obligations to private bodies or individuals",[5] the *conditions of delegation* should be used to safe-guard conflicting fundamental rights (in a same way as delegation of powers on international organizations is not without oversight). As a consequence, the states should not be completely at liberty to design their blocking schemes as they wish and should actively design effective safeguards into their laws delegating such enforcement.

(5) Moreover, the legal framework shall respect the quality of law when a blocking order is issued. Any blocking provision should be clearly prescribed by law.[6] Some elements and conditions should therefore be present in any such schemes, such as (1) categories of targeted content; (2) technical aspects of the blocking orders; (3) territorial scope; (4) entrusted authority for issuance and follow-up supervision, (5) procedure for the issuance of the blocking order, (6) justifying ground for the blocking order (in the sense of Article 10(2)), (7) compliance with proportionality and necessity principles and (8) effective safeguards in case of over-blocking.[7]

DUE PROCESS REQUIREMENTS

(6) Before issuing the blocking order, the assessment of the competent authority should carefully consider several important factors. Firstly, it should assess the nature, scope and duration of the measure, the legal grounds, the competent authorities who issue, carry out and supervise the blocking measure, and the kind of remedy provided by the national law.[8] Secondly, the authority should also note the caveat that being such a restrictive measure, by rendering large quantities of information inaccessible,

[4] Y. Akdeniz, "To block or not to block: European approaches to content regulation, and implications for freedom of expression", Computer Law and Security Review, 2010, p.1; See also A. Kuczerawy "The power of positive thinking: intermediary liability and the effective enjoyment of the right to freedom of expression", 8 (3) JIPITEC 2017

[5] Costello-Roberts v. the UK (App. No 13134/87), para 27

[6] Gaweda v. Poland; 26229/95; para. 38; 14/03/2002

[7] Concurring opinion of Judge Pinto Albuquerque in the case Ahmet Yıldırım v. Turkey, 3111/10, 18/12/2012

[8] Klass and Others v. Germany, (Series A, NO 28) (1979-80) 2 EHRR 214, 6/9/1978, para. 50 or similarly The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria 62540/00,28/6/2007

blocking is bound to substantially restrict the rights of Internet users and to have a significant collateral effect.[9] Thereby, the authority should individually assess whether the same result can be achieved with a less intrusive measure and whether the measure can achieve its goal.[10] The balance between individual rights should be achieved by minimalization of the interference by the authority, concerning the social context of the restriction and the extent of the interference.[11] Last but not least, the Court should assess whether the state party did not fail in its positive obligation to protect the applicants' freedom of expression, by leaving no alternative means for them to exercise their right to freedom of expression.[12]

(7) In terms of the blocking procedure, as any other procedure, it should guarantee all the affected parties a right to a fair trial. The essential components of this right are the (1) right to have access to the court and (2) the equality of arms. While the former entails number of requirements concerning what is communicated to the target of the blocking or its affected users, the latter mostly refers to the availability of legal remedies to challenge the legitimacy/forms of the blocking, or to undo over-blocking.

(8) Once an entrusted authority, which derives its authority from clear and predictable law, after undertaking a balancing exercise, determines the need for blocking, the targeted website should be informed. This could be achieved through sending a notification, which contains all necessary information so that the owner can understand the legal basis, nature of the measures, reason for their implementation, their expected effects and available legal options. Unless justified by urgency, the notification should provide the targeted website with a reasonable amount of time to remove the content on its own.

(9) If the owner does not remove the content voluntarily and unless justified by urgency, then, after being properly informed, he or she should have the opportunity to present the case, in particular to present the evidence and to be heard**,** before any individual measure which would affect him adversely is taken.[13] In all cases, however, the owner should have sufficient information to be able to challenge the blocking decision and its implementation in the ex-post phase, that is to say after blocking is carried out.

[9] Ahmet Yıldırım v. Turkey, 3111/10, 18/12/2012, para. 66
[10] See for example: Delfi v. Estonia (App. No. 64569/09), paras. 39-43 or C. Angelopoulos et al. "Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability", Journal of Media Law (2016), p. 11
[11] Plowden, P. (2002). "Advocacy and Human Rights Act". Routledge, p. 135
[12] Appleby and others v. the United Kingdom, 44306/98, 13/5/2003, para. 49
[13] See M. Husovec and M. Peguera, "Much Ado About Little – Privately Litigated Disconnecting Injunctions" (2015) 46(1) IIC p. 18-19

(10) Since the blocking of websites can easily become obsolete in a short period of time as the internet is fastly moving medium, the time dimension should be explicitly considered. Moreover, over time, many technical aspects as well as legal aspects (applicable legal basis) can change. That is why the blocking orders should be always released for a fixed period of time with the possibility of authorities to renew their application where justified upon re-assessment.[14]

(11) The unlimited duration of blocking was already held by the Court as lacking proportionality due to the reason that news is "a perishable commodity" and the delay of its publication, even for a short period, may deprive its value and interest.[15] This is especially valid for the online environment.

(12) Unlimited duration of website blocking orders will almost certainly lead to practical problems. After blocking is implemented, owners of blocked websites may stop paying for the domain name and, with time, the domain name would normally become vacant. After that "any person can purchase the domain name of a blocked website and by changing the IP address associated with this website cause blocking of all websites hosted on this IP address."[16]

EFFECTIVE REMEDY

(12) The scope of the obligation under Article 13 varies depending on the nature of the applicant's complaint under the Convention, but the remedy must be *effective* both in practice and in law, meaning that its exercise must not be unjustifiably hindered by the acts or omissions of the authorities of the State.[17] Naturally, the Court is not called upon to review the compatibility of the relevant law and practice with the Convention *in abstracto*. Rather it is asked to determine whether there was a remedy compatible with Article 13 of the Convention available to grant the applicant appropriate relief as regards his substantive complaint.[18] In online content blocking cases, the Court should

[14] P. Savola, Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers, (2014) JIPITEC 116, 2014, p. 128

[15] Affaire RTBF v. Belgium (App. No. 50084/06), para. 89

[16] E. Berg, 'Activists used the security vulnerability of Roskomnadzor's activity and now they block websites. How does it work?', Meduza , Riga, 2017, available at: <https://meduza.io/feature/2017/06/08/aktivisty-vospolzovalis-uyazvimostyu-v-rabote-roskomnadzora-i-teper-blokiruyut-chuzhie-sayty-kak-eto-ustroeno>

[17] See for example: De Tommaso v. Italy (App. No. 43395/09), para. 179; Paul and Audrey Edwards v. the United Kingdom (App. No. 46477/99), paras. 96-97; Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania (App. No. 47848/08), para. 148

[18] A. v. the Netherlands (App. No. 4900/06), paras. 155-158

also take into consideration the fact that the measures at place render large quantities of information inaccessible and thus substantially restrict the rights of Internet users.[19]

(13) To provide the affected parties with an effective remedy, the blocked websites, whether targeted or not, should have at their disposal simply accessible and efficient legal remedies to challenge the measures and their implementation.

(14) *Ex ante remedies* should guarantee that even before the blocking is undertaken, the owner of targeted content should be in a position to challenge a notification of blocking, whereas *ex post remedies* should ensure that once the order is implemented, there are efficient mechanisms to limit it, or challenge it due to new circumstances. So, if the owner of the content was not informed of the blocking order and was not given the opportunity to effectively intervene in the procedure, it raises the question of whether the blocking order guarantees the right to a fair trial.

(15) Ex post remedies (after the implemention) are necessary to facilitate the exercise of freedom of expression. They can can include, inter alia, a) availability of appeal against website blocking measures, b) limiting duration of website blocking orders and c) post-grant supervision of implementation by state authorities.[20] Availability of appeal against an already implemented blocking measure is less effective than an appeal before blocking. However, a post-blocking appeal can still be an essential means of redress. Such appeal or challenge should be available not only to website operators, but also to users, as recently stressed by the Court of Justice of the European Union.[21] Some of the suggested safe-guards are already being implemented by the courts in the United Kingdom.[22]

(16) Last but not least, the principle of transparency contributes to existence of effective remedies. In general, it refers to the condition of "legal certainty, predictability and foreseeability" of the law.[23] But in this case, it can be also applied as procedural transparency to avoid "Kafkaesque" blocking of the online content. Therefore, the owner of the content, whether targeted or not, should be informed of the reasons, and redress mechanisms. For instance, the implementing internet providers might be obliged to put a notice concerning the blocking of a particular website when the user tries to reach it, explaining the legal basis of the blocking, available forms of redress and links to the initial decision. The technical community

[19] Ahmet Yıldırım v. Turkey (App. No. 3111/10), para. 66
[20] As practiced in the United Kingdom – see Cartier International AG and others v British Sky Broadcasting Ltd and others [2014] EWHC 3354 (Ch), [2015] BUS LR 298
[21] UPC Telekabel Wien (2014) C-314/12, paras. 57-58
[22] Cartier International AG and others v British Sky Broadcasting Ltd and others [2014] EWHC 3354 (Ch), [2015] BUS LR 298
[23] See supra note 13, p. 23

already came up with a technical standard how to communicate such information ("HTTP 451 Unavailable For Legal Reasons").[24]

CONCLUSION

The European Information Society Institute (EISi) suggests that the Court:

- ***recognizes* that states are not completely at liberty to design blocking schemes and that each delegation of enforcement has to be accompanied with a number of due process and remedial safe-guards;**
- ***acknowledges* that the state cannot absolve itself of an obligation to provide for an effective remedy against over-blocking by simply delegating the implementation of its measures to private parties;**
- ***acknowledges* that the owner of the blocked content should have right to have access to the court, procedural equality of arms and efficient legal remedies available; both before blocking is decided upon and after it is implemented by private parties;**

[24] See https://en.wikipedia.org/wiki/HTTP_451