International Standards and Comparative Approaches on Freedom of Expression and Blocking of Terrorist or Extremist Content Online

the OSCE Representative on Freedom of the Media

on the request of the Russian Federation

OSCE, Vienna, January 2018

Table of Contents

I. INTRODUCTION

1. The Russian Federation has requested the Office of the Representative to provide "information on the OSCE groundwork and best practices in the sphere of countering the spread of extremist and terrorist propaganda through mass-media and on the Internet, including provisions to temporary block the sources, which refuse to react on requests of the competent authorities to delete the relevant content as provided by national legislation."

2. In offering this advice, the Representative emphasises his continued readiness to engage in further dialogue with the Russian Federation and other interested OSCE participating States on these issues.

3. This advice will focus on the legal aspects of the issue.

4. At the same time, the advice also builds upon the larger context of the comprehensive approach of the OSCE to security, in which the protection of human rights, including freedom of expression and freedom of the media, is seen as an integral part of the OSCE's participating States' contribution to peace and security. On several occasions, the OSCE Representative on Freedom of the Media highlighted - as his predecessors did before him - that this approach, acknowledging the intertwined character of peace and security efforts in the three dimensions of the OSCE (political and military, economic and environmental policies, and the human dimension), defines the unique character of the OSCE and has been confirmed many times. In 2015, in the Belgrade Ministerial Declaration on Reinforcing OSCE Efforts to Counter Terrorism in the Wake of Recent Terrorist Attacks, Ministers agreed "(…) that respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures, and are an essential part of a successful counter-terrorism effort."[1] The OSCE Representative on Freedom of the Media insisted on several occasions, including in his Report to the Permanent Council of the OSCE in November 2017, that there must be no opposition between protecting freedom of expression and freedom of the media on the one hand, and the fight against extremism and terrorism, on the other hand.

[1] See: http://www.osce.org/cio/207261?download=true

5. These OSCE principles remain guiding in the context of a high level of terrorist threats and security challenges throughout the OSCE region. However, there are many cases where security concerns may lead to the temptation to subordinate, even temporarily, the respect for human rights to the fight against extremism and terrorism. .

6. The first risk of such a subordination is that, since security threats can last, the exception becomes the rule at the expense of fundamental freedoms. .

7. The second risk is the temptation to misuse the national security argument as a pretext to silence dissenting voices and to restrict freedom of expression at large. .

8. At the OSCE Internet Freedom Conference "The Role and Responsibilities of Internet Intermediaries", on 13 October 2017 in Vienna, the Representative on Freedom of the Media noted that we have been confronted, in the past years, with a backlash against the extraordinary open space of Internet. "We have seen the dissemination of degrading and illegal content, of extremist and hate speech, of terrorist content and propaganda, of attacks and threats such as against female journalists. They can impact directly on democracy, peace and cohesion of societies. The Representative added that in response, there is an increasing pressure of states on intermediaries, to counter the circulation of such offensive material, through the adoption of new laws and policies which can meet legitimate goals, but can also affect the open and free Internet as we have known it so far. As a consequence, we are entering again in unknown territory".[2] .

9. This Advice is structured as follows: *first*, international law and standards on the permissibility of blocking measures against websites on the grounds that they disseminate extremist or terrorist content will be set out; and *second*, examples of comparative approaches on the issue of blocking, particularly amongst OSCE participating States, in that regard will be set out. It is intended to offer guidance on the scope of circumstances, if any, in which authorities may block websites according to international law and standards.

10. At the outset, it is noted that the issue of blocking of websites has attracted growing attention amongst international and regional human rights bodies, as well as the European Court of Human Rights (ECtHR) over a number of years. It is a live legal issue at the ECtHR, which is currently

[2] See: http://www.osce.org/fom/350386?download=true

examining in two cases – namely, *OOO Flavus and others v Russia*[3] and *Kharitonov v Russia*[4] – which are the first opportunity for the court to examine Russian legislation on the blocking of websites and national legal proceedings resulting in websites being blocked by court orders.

11. This advice takes many sources into consideration, including treaty law, resolutions, declarations and legal reviews issued by the Office of the OSCE Representative on Freedom of the Media alongside other intergovernmental mandate-holders on freedom of expression, third-party submissions of leading NGOs in the field of freedom of expression and digital rights,[5] and the significant comparative study undertaken by the Council of Europe and published in June 2016, "Study on blocking, filtering and takedown of illegal content on the Internet".[6] .

12. This advice shows that blocking measures can only be compatible with international standards on freedom of expression in very exceptional circumstances, if they are provided by law and a court has determined that a particular measure is both necessary and proportionate to protect a legitimate aim, such as national security or public order.

[3] Application Nos. 12468/15, 20159/15, 23489/15, 19074/16 & 61919/16.
[4] Application no. 10795/14.
[5] See the Third-Party Intervention Submissions by ARTICLE 19, The Electronic Frontier Foundation, Access Now and Reporters Without Borders in *OOO Flavus v Russia*, Application Nos. 12468/15, 20159/15, 23489/15, 19074/16 & 61919/16, 15 January 2018 and the Third Party Intervention Submissions by Access Now in *Kharitonov v* Russia, Application no. 10795/14, 17 October 2017.
[6] See Council of Europe, *Study on blocking, filtering and takedown of illegal content on the Internet*, June 2016 https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

II. INTERNATIONAL LAW AND STANDARDS

A. General Principles

1. Broad scope of freedom of expression

13. Under international law, the right to freedom of expression is protected by Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights ("ICCPR"). Article 19 of the ICCPR, the key international treaty provision on freedom of expression, states:

> **2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.**
> **3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:**
> **(a) For respect of the rights or reputations of others;**
> **(b) For the protection of national security or of public order (ordre public), or of public health or morals.**

14. This provision is similar to provisions of regional human rights law, including notably Article 10 of the European Convention on Human Rights ("ECHR").[7]

15. Article 20(2) of the ICCPR subsequently provides that "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."[8]

---

[7] This provision states: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 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, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

16. At the outset, it is important to note that the right to freedom of expression is broad in its scope encompassing "even expression that may be regarded as deeply offensive",[9] as stated by the Human Rights Committee, or ideas, information and opinions "that offend, shock or disturb the State or any part of the population",[10] as stated by the ECtHR.

2. Protection of online speech as offline speech

17. International human rights bodies, as well as the ECtHR, have acknowledged that human rights, particularly the right to freedom of expression, extends and applies to the online sphere.[11] Human Rights Council resolution 32/13 of July 2016, for instance "[a]ffirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice".[12]

3. Limitations on freedom of expression: three-part test

18. Under international legal standards, limitations of the right to freedom of expression are permissible but "must not put in jeopardy the right itself" and meet certain conditions, namely they must be: (1) "provided by law" which is sufficiently clear and precise; (2) pursue a legitimate aim set out in Article 19 para 3 of the ICCPR (the "rights or reputations of others" or "the protection of national security or of public order (ordre public), or of public health or morals"); and (3) conform to the "strict tests of necessity and proportionality".[13] As stated by the Human Rights Committee, any restrictions "must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their

---

[8] "Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence", Appendix in the Annual Report of the United Nations High Commissioner for Human Rights, A/HRC/22/17/Add.4, 11 January 2013.
[9] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011, para 11.
[10] *Handyside v UK*, Application No 5493/72, judgment of 7 December 1976 at para 49.
[11] Human Rights Council resolutions 26/13 of 26 June 2014 and 32/13 of 18 July 2016; General Assembly resolution 68/167 of 18 December 2013; Report of the Special Rapporteur on freedom of opinion and expression, 11 May 2016, A/HRC/32/38, para 6.
[12] *Ibid*.
[13] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011, para 22.

protective function".[14] Hence, any broad measures invoking "terrorism" or "extremism" to justify online restrictions on freedom of expression, including through website blocking, must therefore by clearly defined and establish a "direct and immediate connection between the expression and the threat" to national security".[15]

B. International standards on freedom of expression as applied to counter-terrorism and counter-extremism measures

1. General

19. According to international law, there are no universal definitions of either "extremism" or "terrorism", even though these terms are regularly used in the texts produced by international and regional intergovernmental bodies, including UN General Assembly, Security Council and Human Rights Council resolutions and the OSCE's own commitments, as well as states' laws and policies.[16] In General Comment 34, the Human Rights Committee has emphasised that counter-terrorism and counter-extremism measures should be compatible with Article 19 of the ICCPR. It stated:

> **States parties should ensure that counter-terrorism measures are compatible with paragraph 3 [of Article 19 of the ICCPR]. Such offences as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying", or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. Excessive restrictions on access to information must also be avoided. The media plays a crucial role in informing the public about acts of terrorism and its capacity to operate should not be unduly restricted. In this regard, journalists should not be penalized for carrying out their legitimate activities.[17]**

20. In their Joint Declaration on Freedom of Expression and countering violent extremism of 2016, the four inter-governmental mandate-holders on freedom of expression – including the OSCE

[14] Human Rights Committee, General Comment No 27, CCPR/C/21/Rev.1/Add.9, 9 November 1999, para 14.
[15] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011, para 35.
[16] See, for instance, Declaration on Strengthening OSCE Efforts to Prevent and Counter Terrorism, Document of the Twenty-Third Meeting of the Ministerial Council, 8-9 December 2016, Hamburg MC.DOC/1/16.
[17] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011, para 46.

Representative on Freedom of the Media – fleshed out the scope of the right to freedom of expression as it relates to "extremist" content. [18] They reiterated that:

> **1. General Principles**
>
> **(a)** ***Everyone has the right to seek, receive and impart information and ideas of all kinds, especially on matters of public concern, including issues relating to violence and terrorism,*** **as well as to comment on and criticise the manner in which States and politicians respond to these phenomena (…)**
>
> **(c) Any restrictions on freedom of expression should comply with the standards for such restrictions recognised under international human rights law. In compliance with those standards, States must set out clearly in validly enacted law any restrictions on expression and demonstrate that such restrictions are necessary and proportionate to protect a legitimate interest. (…)**

21. They also emphasised that any limitations on freedom of expression, including on the grounds of countering extremism, must be subject to judicial review, stating that:

> **(e) Restrictions on freedom of expression must be subject to independent judicial oversight.**

22. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has further elaborated on what ought *not* to be considered "extremism":

> **38. [S]imply holding or peacefully expressing views that are considered 'extreme' under any definition should never be criminalised, unless they are associated with violence or criminal activity. The peaceful pursuance of a political, or any other, agenda – even where that agenda is different from the objectives of the government and considered to be 'extreme'– must be protected. Governments should counter ideas they disagree with, but should not seek to prevent non-violent ideas and opinions from being discussed.**

[18] Joint Declaration on Freedom of Expression and countering violent extremism adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, adopted on 4 May 2016.

23. Measures on counter-terrorism and counter-extremism are regularly justified on the grounds of protection of national security and/or public order, under Article 19 para 3 of the ICCPR. In this regard, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has warned against vague and overbroad definitions.

2. Restrictions on online content, particularly blocking

24. In 2011, in its General Comment 34 on Article 19 of the ICCPR, the UN Human Rights Committee stated that "generic bans on the operation of certain sites and systems are not compatible" with Article 19 of the ICCPR[19].

25. In the 2016 Joint Declaration on Freedom of Expression and countering violent extremism, the international intergovernmental mandate-holders on freedom of expression, including the OSCE Representative on Freedom of the Media, recommended that: [20]

> **2. Specific Recommendations: (...)**
>
> **(e)** ***States should not subject Internet intermediaries to mandatory orders to remove or otherwise restrict content except where the content is lawfully restricted in accordance with the standards outlined above. States should refrain from pressuring, punishing or rewarding intermediaries with the aim of restricting lawful content*** **(…)**
>
> **(j)** ***States should not adopt, or should revise, laws and policies which involve the following:***
>
> **(i)** ***Blanket prohibitions on encryption and anonymity, which are inherently unnecessary and disproportionate*****, and hence not legitimate as restrictions on freedom of expression, including as part of States' responses to terrorism and other forms of violence.**
>
> **(ii) Measures that** ***weaken available digital security tools*****, such as backdoors and key escrows, since these disproportionately restrict freedom of expression**

[19] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011.
[20] Joint Declaration on Freedom of Expression and countering violent extremism adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, 4 May 2016.

> **and privacy and render communications networks more vulnerable to attack. [emphasis added]**

26. International human rights mechanisms have long expressed particular concern about blocking measures as such. In their 2011 Joint Declaration on Freedom of Expression on the Internet, the four inter-governmental mandate-holders on freedom of expression stressed:

> ***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.[21] [emphasis added]**

3. Key cases

27. The jurisprudence of the ECtHR on access to the Internet has included important case-law concerning measures blocking access to the Internet. The cases highlight that the imposition of any blocking measure needs to have clear and actual legal basis, and in doing so meet the foreseeability requirement.

28. In the 2012 decision of *Ahmet Yıldırım v Turkey*, the ECtHR held that there had been a violation of Article 10 of the ECHR on freedom of expression in a case concerning a Turkish court decision to block access to the service *Google Sites*, which hosted a site whose owner was facing criminal proceedings for insulting the memory of Atatürk.[22] The ECtHR decided that, even though the decision did not constitute a blanket ban, but rather a restriction on the Internet, the effects of the measure had been arbitrary and the judicial review of the blocking of access had been insufficient to prevent abuses. Specifically, there was no indication that the Turkish court had made any attempt to "weigh up the various interests at stake, in particular by assessing the need to block all access *to Google Sites*", which was a consequence of shortcomings in the domestic law. The domestic judges ought to have "taken into consideration … the fact that the

[21] Joint Declaration on Freedom of Expression on the Internet, 1 June 2011, para 3 (a).
[22] *Ahmet Yıldırım v Turkey*, Application No 3111/10, judgment of the European Court of Human Rights of 18 December 2012.

measure, by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect".[23]

29. In *Cengiz v Turkey*, decided in 2015, the ECtHR held that there also had been a violation of Article 10 of the ECHR in the case of the wholesale blocking of *YouTube* in Turkey.[24] The court found that, given that there was no statutory provision empowering the domestic court to block all access to *YouTube*, the interference with freedom of expression "did not meet the requirement of lawfulness under the Convention and did not afford the applicants the degree of protection to which they were entitled by the rule of law in a democratic society".[25]

30. It is noted that the Turkish Constitutional Court has also on occasion found that blocking access to *YouTube* and *Twitter* is in violation of freedom of expression.[26]

4. OSCE Representative on Freedom of the Media

31. Besides participating in the development and adoption of successive Joint Declarations on freedom of expression, including those addressing the issue of blocking as referenced above, the OSCE Representative on Freedom of the Media has expressed a position about the permissibility of restrictions on content and the blocking of websites in numerous contexts, many times over many years. .

32. An early example of these expressed positions can be found in the Amsterdam Recommendations on Freedom of the Media and the Internet, launched at a conference in Amsterdam on 14 June 2003. These recommendations state that:

> **Any means of censorship that are unacceptable within the 'classic media' must not be used for online media. New forms of censorship must not be developed.**

[23] *Ibid*, para 66.
[24] *Cengiz and others v Turkey*, Application No 48226/10 et 14027/11, judgment of the European Court of Human Rights of 1 December 2015.
[25] *Ibid* para 65.
[26] TC Anayasa Mahkemesi, Başvuru Numarası, 2014/4705, Karar Tarihi, judgement of the Turkish Constitutional Court of 29 May 2014; T C Anayasa Mahkemesi, Başvuru Numarası, 2014/3986, Karar Tarihi, judgment of the Turkish Constitutional Court of 2 April 2014.

33. In May 2012, welcoming the adoption of a net neutrality law making the Netherlands the first OSCE country to do so, the Representative has highlighted this law in her presentation to the Permanent Council as an important step to protect Internet traffic from undue restrictions and prioritization, as the law requires operators to treat all Internet traffic equally, regardless of author, origin, destination or content. The OSCE Representative highlighted that the law also prohibits network operators from slowing or blocking third-party services that allow for Internet-based communications.[27]

34. The conclusions of a February 2013 conference on the Internet hosted by the OSCE Representative on Freedom of the Media emphasised:[28]

> **In today's democratic societies, citizens shall be allowed to decide for themselves what they want to access on the Internet. As the right to disseminate and receive information is a basic human right, government-enforced mechanisms for filtering, labelling or blocking content shall not be acceptable.**

35. Communiqué No. 6/2016 of the OSCE Representative on Freedom of the Media of 1 September 2016 also indicates that states should only restrict content that is considered a threat to national security if it can be demonstrated that it is intended to incite imminent violence, likely to incite such violence and there is a direct and immediate connection between the expression and the likelihood of occurrence of such violence.[29] The communiqué also states that blanket prohibitions are disproportionate and therefore unacceptable.[30]

36. The publication "Media Freedom on the Internet: An OSCE Guidebook" (2016) makes the following recommendations to policy makers:

> **• Do rely on blocking only within a strict legal framework with regards to content identified as illegal by the courts of law.**

---

[27] "OSCE media freedom representative welcomes Dutch net neutrality law", press release, 14 May 2012; Regular Report to the Permanent Council for the period from 12 June 2012, FOM.GAL/4/12/Rev.1, 21 June 2012.
[28] Recommendations of the OSCE Representative on Freedom of the Media following the conference "Internet 2013: Shaping polices to advance media freedom" held in Vienna on 14-15 February 2013 published in Regular Report to the Permanent Council for the period from 30 November 2012 to 13 June 2013, FOM.GAL/3/13/Rev.1, 13 June 2013.
[29] Communiqué No. 6/2016 of OSCE Representative on Freedom of the Media of 1 September 2016.
[30] *Ibid*, para (viii).

• Do recall that blocking is not an effective method to address problems associated with Internet content and could have serious side effects including over blocking.

• Don't allow Internet access providers to restrict users' right to receive and impart information by means of blocking, slowing down, degrading or discriminating Internet traffic associated with particular content, services, applications or devices.[31]

37. In his address at the Internet Freedom Conference "The Role and Responsibilities of Internet Intermediaries" in Vienna in 2017, the Representative stated that rules and decisions regulating Internet "should avoid negative impact on access to information, and should in particular avoid development of a variety of content and liability regimes that differ among different areas of the world, thus fragmenting the Internet and damaging its universality". He added that "It has become a human right to have access to the Internet and its services, and to be free to use it. The defence of this online right is the extension of the defence of the universal right to freedom of expression and freedom of the media offline."[32]

III. COMPARATIVE APPROACHES

A. Approaches to blocking "extremist" online content

38. Over recent years, many States have adopted "a combination of repressive legislative measures to block, filter and ban specific content or entire websites" as the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has noted.[33]

39. In June 2016, the Council of Europe published a comprehensive, comparative study on "Filtering, blocking and take-down of illegal content on the Internet".[34] This recent report is

---

[31] *Media Freedom on the Internet: An OSCE Guidebook*, March 2016 (Vienna: OSCE, 2016) pp 6 – 7.
[32] http://www.osce.org/fom/350386?download=true
[33] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 22 February 2016, A/HRC/31/65 para 40.
[34] See Council of Europe, *Study on filtering, blocking and takedown of illegal content on the Internet*, June 2016 https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet
See also *Ahmet Yıldırım v Turkey*, Application No 3111/10, judgment of the European Court of Human Rights, 18 December 2012, paras 31 – 37.

instructive for any comparative assessment of the regulatory frameworks with respect to blocking.

1. No legal framework or general legal framework

40. The 2016 Council of Europe report indicates that:

> **[There] are countries which do not have any specific legislation on the issue of blocking, filtering and takedown of illegal internet content: there is no legislative or other regulatory system put in place by the State with a view to defining the conditions and the procedures to be respected by those who engage in the blocking, filtering or takedown of online material. An argument often put forward in this context is the impossibility for the legislator to keep up with the pace of technological developments. The underlying reasons for a lack of legislative activity may also be found in a country's legal traditions.**
>
> **In the absence of a specific or targeted legal framework, several countries rely on an existing "general" legal framework that is not specific to the internet to conduct ´ what is, generally speaking - limited blocking or takedown of unlawful online material. This is witnessed in countries such as Germany, Austria, the Netherlands, the United Kingdom, Ireland, Poland, the Czech Republic and Switzerland. As such countries become increasingly confronted with the reality of internet content-related disputes, the absence of legislative intervention has presented a challenge. In recent years, diverse mechanisms have been relied on to fill the regulatory gap and to address particular issues. Some jurisdictions have even chosen to combine approaches, maintaining a largely unregulated framework, but with legislative or political intervention in specific areas. In some jurisdictions, such as the UK and Albania, self-regulation has been adopted by the private sector to supplement the void left by the legislator's choice not to intervene in the area at stake. Other countries, such as the Netherlands and Germany, rely on the domestic courts to ensure that the necessary balance between freedom of expression on the one hand and safety of the internet and the protection of other fundamental rights is preserved to the greatest extent possible.**[35]

41. Participating States such as the UK, Austria, the Netherlands, Ireland, Poland, the Czech Republic and Switzerland have relied upon existing legislation to address issues raised by illegal content on the Internet. In practice, this means that the courts in such states decide whether or not

[35] Executive Summary, Council of Europe, *Study on blocking, filtering and takedown of illegal content on the Internet*, June 2016 https://rm.coe.int/168068511c at ii. In 2017, Germany adopted a law on social media, the "NetzDG".

content is illegal and should be blocked. .

42. In the UK, and in the absence of a specific legal framework, the High Court of Justice of England and Wales has offered guidance on the principles to be considered in making blocking orders. In *Cartier International AG v British Sky Broadcasting Ltd*, the judge (Mr Justice Arnold) emphasised the principle of proportionality in the following way:

> **189. (…) I conclude that, in considering the proportionality of the orders sought (…), the following considerations are particularly important:**
>
> **(i) The comparative importance of the rights that are engaged and the justifications for interfering with those rights;**
> **(ii) The availability of alternative measures which are less onerous;**
> **(iii) The efficacy of the measures which the orders require to be adopted by the Internet Service Providers (ISPs), and in particular whether they will seriously discourage the ISPs' subscribers from accessing the Target Websites;**
> **(iv) The costs associated with those measures, and in particular the costs of implementing the measures;**
> **(v) The dissuasiveness of those measures;**
> **(vi) The impact of those measures on lawful users of the internet.**
>
> **190. In addition, it is relevant to consider the substitutability of other websites for the Target Websites.**[36]

2. Specific legal framework

Some participating States – including Germany, the Russian Federation, France, Turkey, Portugal, Hungary, Spain and Finland – have put in place, in some cases very recently, a specific legal framework allowing blocking and takedown of certain categories of illegal content, in particular content that endangers national security, including terrorist content, but also child abuse materials, content that threatens public health and morals, as well as content that constitutes a "hate crime".

43. The 2016 Council of Europe report indicates that:

[36] *Cartier International AG v British Sky Broadcasting Ltd* [2014] EWHC 3354 (Ch), judgment of 17 October 2014, para 189.

> **[I]n many jurisdictions, the legislator has intervened in order to set up a legal framework specifically aimed at regulation of the internet and other digital media, including the blocking, filtering and removal of internet content. Finland, France, Hungary, Portugal, the Russian Federation, Spain and Turkey are examples of jurisdictions that have opted for this regulatory approach. Such legislation typically provides for the legal grounds on which blocking or removal may be warranted, the administrative or judicial authority which has competence to take appropriate action and the procedures to be followed.**
>
> **Whereas the more common grounds for the adoption of blocking, filtering and takedown measures are exhaustive and expressly defined in the legislation of most countries which subscribe to such a regulatory model, certain jurisdictions have, in effect, extended the grounds on which blocking or removal may legitimately be taken - often by amendments to legislation or through creative judicial interpretation.**[37]

3. Procedure

44. According to the Council of Europe report, in relation to material concerning terrorism and national security and also child abuse and criminality, especially hate crimes:

> **many of the States with legal rules targeted at the removal of internet content provide for the urgent blocking of such material without the need for a court order in at least some of the areas mentioned. Greece, France, Portugal, the Russian Federation, Serbia and Turkey are examples.**

45. The report continues as such on aspects of procedure:

> **Administrative authorities, police authorities or public prosecutors are given specific powers to order internet access providers to block access without advance judicial authority. It is common to see such orders requiring action on the part of the internet access provider within 24 hours, and without any notice being given to the content provider or host themselves. In other countries, such as Finland, where a court order is otherwise needed, hosting providers who have knowledge of such material may be expected to remove it voluntarily without judicial authority and to provide the content provider with due notice, which permits them to challenge the action through the courts.**

---

[37] *Ibid.*

A number of national systems (such as Turkey, in some cases) require the relevant administrative authority to obtain subsequent judicial approval of their order, while others place a splash page at the location of the blocked material explaining why the material is blocked and how it may be challenged. In most countries, interested parties are given the opportunity to challenge blocking actions through usual criminal (or, where appropriate, civil) procedure laws. The Portuguese regulation explicitly states so.

Particularly in relation to material concerning child abuse and other serious crimes or in relation to online gambling, many countries, such as France, Greece, Italy, Romania, the Russian Federation, Turkey and the UK, adopt a "list" system, whereby a central list of blocked URLs or domain names are maintained and updated by the relevant administrative authority. This is notified to the relevant internet access providers, who are required to ensure that blocking is enforced.

In many States, the takedown and blocking of material which infringes intellectual property and privacy or defamation rights is effected or authorised pursuant to court order only. Some countries have introduced alternative notice and takedown procedures designed to avoid the need for court action. In Finland, for example, there is evidence of a procedure for rights holders to obtain removal of allegedly unlawful material, subject to content providers being afforded a due process to challenge removal. Particularly in relation to defamatory material or content which otherwise infringes privacy rights enforcement will usually depend on the initiative being taken by the person or organisation harmed, and so many countries offer some form of 'notice and take-down' procedure. These may require the person or organisation affected to notify the relevant website operator directly before procedures for taking down the material can be initiated. Where the website operator refuses to remove material determined to be unlawful, the relevant domestic authority may provide a deadline to the host to remove the material, and/or may leave itself exposed to third party liability for the content. Internet access providers can even be ordered to block access to the URL, or even the entire website.

46. Several of these examples show that a number of participating States through different approaches have introduced laws and policies with the objective to respect international obligations regarding freedom of expression while countering illegal content. Additionally, they have put in place mechanisms of appeal and judicial oversight to ensure the right balance between the two objectives. This legislation will have to be regularly evaluated and if necessary amended. Independent judicial oversight is an essential element in the implementation of such legislation.

IV. COMPATIBILITY OF BLOCKING MEASURES WITH INTERNATIONAL STANDARDS ON FREEDOM OF EXPRESSION

47. On the basis of the international law and standards indicated above (in Part II), website blocking measures can only be compatible with international standards on freedom of expression where they are provided by law and a court has determined that a particular measure is necessary and proportionate to protect legitimate aims as specified by international law.

48. Leading NGOs in the field – namely ARTICLE 19, the Electronic Frontier Foundation, Access Now and Reporters Without Borders – have argued this position in their third-party intervention submissions in the case of *OOO Flavus and others v Russia* of 15 January 2018. The framework presented in the submissions supports the conditions indicated in the international standards upon which the Office of the OSCE Representative on Freedom of the Media relies, indicated above, in fleshing out the very exceptional circumstances in which blocking orders may be permissible. A number of the arguments made in the submissions are particularly relevant for the purpose of this advice.

49. The third-party intervention of the above-mentioned NGOs states that in order to meet the requirement that any blocking measure, as a restriction on freedom of expression, is provided by law, there should be a number of "procedural safeguards" in place. The intervention sets out the following conditions for blocking orders:

> • **Blocking should only be ordered by a court or other independent and impartial adjudicatory body. Regulatory models whereby government agencies directly issue blocking orders are inherently problematic as executive agencies are, by nature, more likely to call for measures that protect the particular state interests they are tasked to protect, such as national security or child safety, rather than freedom of expression;**
>
> • **When a public authority or third party applies for a blocking order, the operators of the website, authors of the offending content, ISPs and/or other relevant internet intermediaries should be given the opportunity to be heard in order to contest the application;**

> • **Similarly, procedures should be in place allowing other interested parties, such as free expression advocates or digital rights organizations, to intervene in proceedings in which a blocking order is sought;**
> • **Users should be given a right to challenge, after the fact, the decision of a court or other independent and impartial adjudicatory body to block access to content. A fortiori, this must include a right for victims of collateral blocking to challenge the wrongful blocking of their website or webpage; (...)** .

The third-party intervention adds that : .

> **In countries where blocking decisions are made by public authorities, the law should guarantee that those authorities are independent of government and that their decisions can be readily challenged before a court or tribunal. Moreover, the law should lay down the criteria to be applied by these authorities to determine whether any blocking order can be issued.** .

It also recommends, with respect to the blocking of certain sites containing information about technologies, that : .

> **The blocking of websites which contain information about VPNs or other similar technologies can never be justified. Such technologies are content-neutral and blocking such websites thus amounts to a restriction on access to all content which might be obtained using those technologies. Accordingly, the blocking of such technologies (or information about them) is inherently incapable of being adequately specified with reference to categories of legitimately proscribed content.**

V. CONCLUSION

50. In conclusion, the Representative on Freedom of the Media emphasizes that in accordance with international law, website blocking, as a very serious interference with freedom of expression, would only be permissible in a very limited and well-defined range of circumstances.

51. According to the law and standards highlighted in this advice, the blocking of websites must be subject to the strictest safeguards.

52. As indicated above, if mandatory blocking measures are permissible at all, they should: (i) have a basis in law, (ii) be ordered by a court or other independent body and (iii) be strictly necessary and proportionate to the legitimate aim pursued. In considering whether to grant a website blocking order, the court or other independent body tasked with making the order must take into account the impact of the order on lawful content and what technology may be used to prevent over-blocking. All those affected by blocking orders, including journalists and other authors, as well as publishers of content, and those who seek to access the content, should be given an opportunity to challenge such orders and must therefore be notified of their existence.

53. Given the permanent evolution of the Internet, existing regulatory practices should be reviewed regularly regarding their respect of the above-mentioned principles, with evaluation mechanisms of implementation established by law, in order to ensure that the authorities, the legislator and civil society will be able to verify regularly that the legislation in place doesn’t go beyond defined legitimate aims such as the fight against extremism and terrorist propaganda, and that human rights, particularly freedom of expression and freedom of the media, are properly protected.