IN THE EUROPEAN COURT OF HUMAN RIGHTS
APP NO. 25479/19
BETWEEN:-

Wikimedia

Applicant

- v -

TURKEY

Respondent Government

Third party intervention submissions by ARTICLE 19, the European Centre for Press and Media Freedom, Human Rights Watch, Index on Censorship, PEN International and Reporters Without Borders

---

INTRODUCTION

1. This third-party intervention is submitted on behalf of ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19), the European Centre for Press and Media Freedom (ECPMF), Human Rights Watch (HRW), Index on Censorship, PEN International and Reporters Without Borders (RSF), hereafter 'the Interveners'.

2. The Interveners welcome the opportunity to intervene as third parties in this case, by the leave of the President of the Court, which was granted on 18 October 2019 pursuant to Rule 44 (3) of the Rules of Court.

3. The present case concerns the compatibility of a sweeping website blocking order made by the Turkish authorities with the requirements of Article 10 of the Convention. Despite the Court's judgments in the *Ahmet Yıldırım* and *Cengiz* cases, Turkish law continues to allow the wholesale blocking of websites by a governmental body in a wide range of circumstances. The Interveners note that under Turkish law a blocking order directed at one particular website could also restrict access to all other – unrelated – websites sharing the same IP address, and not just a single domain name. The Interveners believe that the present case is significant because it presents an opportunity for the Court to examine the compatibility of the Turkish Internet law (Law no. 5651) that was amended following the Court's judgments in the abovementioned cases. It would also allow the Court to address the core question of whether blanket blocking orders of websites are ever proportionate. As such, it represents a test case for the protection of freedom of expression online in Turkey.

4. In these submissions, the Interveners address the following: (i) the state of freedom of expression online in Turkey; (ii) international and comparative law standards on website blocking measures, with a focus on regulatory approaches and remedies for violations of the right to freedom of expression as a result of website blocking; and (iii) the proper approach to cases involving website blocking.

I. FREEDOM OF EXPRESSION ONLINE IN TURKEY

Turkey's track record in undermining freedom of expression online

5. Turkey has a long track record of undermining freedom of expression online, which has only worsened since the failed coup of July 2016. In the absence of official statistics published either by the former Telecommunications Communication Presidency ("TIB") or its successor Information Technologies and Communication Board ("BTK"), the most authoritative source of information on blocked websites is the Turkish Freedom of Expression Association (IFÖD). In its 2018 EngelliWeb report, IFÖD noted that:[1]

> Prior to 2018, access to a total of 190.922 domain names and websites were blocked from Turkey pursuant to the decisions, orders and legal measures detailed below. 177.515 of these websites were blocked by TIB, and later by the Head of Information Technologies and Communication Board 9.227 domain names were blocked by criminal judgeships of peace, public prosecutors' offices and by the courts. Additionally, as far as is known, prior to 2018, access to 150.000 URL addresses were blocked by criminal judgeships of peace in accordance with Article 9 of the Law No. 5651, and around 50.000 new articles as well as social media content was removed by content providers and platform providers subsequent to receiving the relevant blocking orders. As will be detailed below, in the year of 2018, as far as it could be determined by our efforts under the scope of the EngelliWeb project, a further 54.903 domain names were blocked access to from Turkey. Together with these statistics, by the end of 2018, a total of 245.825 domain names are blocked from Turkey (…)

6. More recently, RSF reported that Turkey's courts had blocked nearly 3000 online articles in 2018.[2] In particular, RSF noted that:[3]

> In addition to this shocking figure, an unknown number of content blockings were carried out without references to the courts. A total of 2,047 pages on the newspaper *Hürriyet*'s website alone were blocked in the past five years, according to Faruk Bildirici, who was recently fired as its ombudsman after it was bought by a pro-government press group.

7. In its 2019 Net Freedom report, Freedom House reported on Turkey's website blocking practices as follows:[4]

> The vast majority of blocking orders are issued by the BTK, rather than by the courts. The procedures surrounding blocking decisions are opaque, creating significant challenges for those seeking to appeal. Judges can issue blocking orders during preliminary investigations as well as during trials. The reasoning behind court decisions is not provided in blocking notices, and the relevant rulings are not easily accessible. As a result, it is often difficult for site owners to determine why their site has been blocked and which court has issued the order. The BTK's mandate includes executing judicial blocking orders, but it can also issue administrative orders for foreign websites, content involving sexual abuse of children, and obscenity. Moreover, in some cases it successfully asks content and hosting providers to remove offending items from their servers, in order to avoid issuing a blocking order that would affect an entire website. This occurs despite the fact that intermediaries are not responsible for third-party content on their sites.

8. Turkey's crackdown on freedom of expression is not limited to blocking access to information online. It has been matched by the arrest, detention and prosecution of large numbers of social media users in the wake of Turkey's military operation in the northwest Syrian district of Afrin.[5] According to the Turkish Interior Ministry, authorities detained 648 people between 20 January and 26 February 2018, over social media posts criticizing Turkey's military operations in Afrin. Authorities held another 197 people for expressing criticism in other forms, including street protests or expressing solidarity with protesters on social media.[6] In March 2018, Human Rights Watch noted that the criminalization of peaceful speech on the Internet had had a chilling effect on social media use and had led to increased self-censorship.[7]

International commentary on Turkey's Internet Law

9. Following the Court's judgment in the *Ahmet Yıldırım* case,[8] the Turkish government amended its Internet law on a number of occasions. However, several human rights institutions, including the Venice Commission and the Committee of Ministers of the Council of Europe (COE), consider that these amendments fail to comply with the Court's ruling.

10. In June 2016, the Venice Commission considered that the new 'access- blocking' procedures under Articles 8A, 9 and 9A of the law failed to provide adequate safeguards.[9] The Venice Commission recommended that:
    (i) The procedures under Articles 8A, 9 and 9A should be made dependent on the institution of a criminal or civil procedure, and that blocking decisions should only constitute a "precautionary measure" which can be taken in the framework of substantive criminal or civil proceedings;

    (ii) Should procedures under Articles 8A, 9 and 9A be maintained as autonomous procedures, appropriate procedural guarantees should be provided, including:
        - the judge should be given sufficient time to make a thorough and reasoned proportionality and necessity assessment of the interference with freedom of expression, should hold a hearing; and an appeal against the decisions on access blocking taken by the peace judgeship before a higher court, including the Court of Cassation, should be possible;
        - the requirement that the restriction must be "necessary in a democratic society" should be introduced in the provisions concerning all access-blocking procedures. The necessity of a fair balance between competing rights and interests when restricting the Internet freedoms should be the guiding principle for the administrative authorities and the courts; an appropriate notification procedure should be put in place in all the access-blocking procedures under the Law. The notification should contain information on the blocking measure and the reasons put forth by the authorities to justify the measure as well as existing remedies;
        - a list of less intrusive measures than that of access-blocking/removal of content should be introduced in the Law, in order to allow the authorities and the courts to apply the least intrusive measure whenever it is sufficient to attain the legitimate aim pursued by the restriction (proportionality assessment); access-blocking measures should be measures of last resort;
        - the system of access-blocking by a decision of the Presidency of Telecommunication without prior judicial review (administrative measure) should be reconsidered. The balancing between competing rights and/or between the measure restricting freedom of expression and the legitimate aims pursued by the measure, should be carried out by a court and not by an administrative body

11. These recommendations have been echoed by the COE Commissioner for Human Rights[10] and the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (SR on FoE).[11] In its 2017 Memorandum on freedom of expression and media freedom in Turkey, the COE Commissioner for Human Rights expressed the view that "*the provisions in the amended texts not only fail to address the core concerns of the ECtHR in the Ahmet Yildirim judgment, but aggravate the situation*".[12] He concluded that "*the censorship of the Internet and the blocking of websites in Turkey continues to be exceptionally disproportionate*".[13] The COE Committee of Ministers has placed the implementation of the *Ahmet Yıldırım* judgment under enhanced supervision[14] and considers that the Turkish Internet law still fails to provide adequate procedural safeguards against arbitrary wholesale blocking of information on the Internet.[15]

12. In light of the above, the Interveners respectfully invite the Court to give the most anxious scrutiny to the Turkish legal framework governing website blocking measures in the instant case.

II. INTERNATIONAL & COMPARATIVE LAW STANDARDS ON WEBSITE BLOCKING MEASURES

International standards on website blocking

13. International human rights bodies have long expressed their deep concern about blocking and filtering measures, underscoring they should only be a measure of last resort permissible only in strictly limited circumstances. In particular, the UN Human Rights Committee held in its General Comment no. 34 on Article 19 – Freedoms of opinion and expression: [16]

> 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

14. The four special mandates on freedom of expression held in their 2011 Joint Declaration on Freedom of Expression on the Internet:[17]

> 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. [emphasis added]

15. Similarly, the UN Special Rapporteur on freedom of expression, Frank LaRue, found in his report of May 2011:[18]

> 31. States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression, as the criteria mentioned under chapter III are not met. 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 of achieving 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 or possibility of review by a judicial or independent body.

16. The UN Special Rapporteur made it absolutely clear that blocking measures must always comply with the three-part test under Article 19(3) ICCPR.[19] In this respect, he laid down some minimum criteria that must be met in order for website blocking and filtering to be justified under international law, namely:[20]
    (i) Blocking and filtering provisions should be clearly laid out by law;

    (ii) Any determination of what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences;

    (iii) Blocking orders must be strictly limited in scope in line with the requirements of necessity and proportionality under Article 19 (3);

(iv) Lists of blocked websites together with full details regarding the necessity and justification for blocking each individual website should be published.
(v) An explanation should also be provided to the affected websites as to why they have been blocked.

17. The above standards have been reiterated by regional mechanisms for the protection of human rights, including the OAS Special Rapporteur on Freedom of Expression,[21] the Council of Europe[22] and the Court itself.[23]

18. At EU level, the Court of Justice of the European Union (CJEU) held in the landmark *UPC Telekabel* case that the addressee of a copyright injunction had to ensure compliance with the fundamental right of internet users to freedom of information when choosing the appropriate measures to be adopted in order to comply with the injunction.[24] The CJEU went on to note:

> 56. In this respect, the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued [emphasis added].

19. The CJEU concluded that in order to ensure that copyright injunctions complied with fundamental rights, national procedural rules had to provide a possibility for Internet users to assert their rights before the court once the implementing measures taken by the Internet service provider were known.[25] This requirement is reflected in the 2015 EU Regulation on Open Internet Access, which provides that "*national measures regarding end-users' access to or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, including in relation to privacy and due process, as defined in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms*".[26]

Comparative law standards on website blocking

20. In *Ahmet Yıldırım v. Turkey*, the Court examined a number of comparative law materials on website blocking.[27] The Court concluded that the regulatory frameworks governing website blocking was highly fragmented, particularly in light of rapidly changing new technologies. As such, it was difficult to identify common standards based on a comparison of the legal situation in CoE member States.

21. Since then, the CoE has conducted a comprehensive study of filtering, blocking and takedown of illegal content on the Internet, which was published in June 2016.[28] Among other things, the Council of Europe concluded:[29]
    (i) Several countries do not have specific legislation on blocking, filtering and takedown of illegal content, partly because of the difficulty in keeping pace with technological developments and partly due to their respective legal traditions. These countries usually rely on existing legislation to deal with the issues raised by illegal content on the Internet (the UK, Austria, the Netherlands, Ireland, Poland, the Czech Republic and Switzerland). In practice, this also means that the courts determine whether or not content is illegal and should be blocked.

    (ii) A small number of countries, including Russia, France, Turkey, Portugal, Hungary, Spain and Finland have put in place a specific legal framework allowing blocking and takedown of certain categories of illegal content, in particular child abuse materials, national security, including terrorism, health and morals and "hate crimes". However, the COE noted that some countries,

such as Russia, had extended the common grounds under which blocking may be legitimately authorized to include e.g. homosexual propaganda.[30]

(iii) A minority of countries allows public authorities, such as police, prosecutors or other administrative bodies to order blocking of illegal material without prior judicial intervention (Greece, Portugal, Russia, France, Serbia and Turkey).

(iv) In most countries, interested parties are given an opportunity to challenge blocking measures through criminal or civil procedure rules (see especially Portugal).

22. Of those countries, which have adopted a specific legal framework allowing website blocking, it appears that very few explicitly provide for "wholesale" blocking of websites or wholesale blocking of websites "sharing the same IP address", rather than blocks that restrict access to a specific website, or domain name (DNS). Turkey amended its legislation in order to provide explicitly for wholesale blocking of websites following the *Yildirim* judgment. In France, a special branch of the police can require ISPs to block access to "electronic addresses" whose content is in breach of the relevant laws on terrorism and child pornography.[31] The regulations specify that electronic addresses must contain either a domain name or the name of a host in the form of a domain name and the name of a server.[32] In Spain, the courts can require ISPs to implement the voluntary measures imposed by the Intellectual Property Commission in order to enforce intellectual property rights.[33] This includes the "suspension" of access to information society providers.[34] However, such measures must be objective, proportionate and non-discriminatory.[35]

23. More generally, it appears that primary legislation seldom provides for the various criteria that should be taken into account before a blocking order can be made. For instance, the Spanish criminal code provides that an entire website may be blocked when it "predominantly" contains hate speech content.[36] However, it appears to be an isolated case. More details can sometimes be found in secondary legislation. In Italy, AGCOM, the communications regulatory authority, can order the blocking of an entire site in cases involving "massive" infringement of intellectual property rights.[37] Similarly, with some limited exceptions (Greece,[38] Italy[39], France[40]), the law is generally silent on the type of technology that may be used to comply with a blocking order.

24. By contrast, a great deal of guidance can be found in countries that have left the issuing of blocking orders to the courts, particularly in the area of intellectual property law.[41] For instance, in *Cartier International AG v BSkyB* before the High Court of Justice of England and Wales, Arnold J considered:[42]

> 189. For the reasons discussed above, I conclude that, in considering the proportionality of the orders sought by Richemont, 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 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;
> In addition, it is relevant to consider the substitutability of other websites for the Target Websites.

25. The application of these criteria, however, does not prevent the courts from ordering the blocking of entire websites if they conclude that it is necessary to do so in the circumstances of the case. For instance, in the *Goldesel* case, the German Federal Court of Justice effectively concluded that the blocking of an entire website may be permissible when the content of the site was mainly unlawful.[43] The courts of England and Wales[44] and Denmark[45] have reached similar conclusions. At the same time, the German decision made clear that website blocking should only be used as a measure of last resort.

26. In addition, some courts have examined the kind of technology available to comply with their orders and determined which should apply in specific cases. In particular, some courts have expressly rejected the use of IP-address blocking and ordered the use of DNS blocking instead:
    (i) In a 2011 Pirate Bay judgment, the Antwerp Court of Appeal considered that IP-blocking had undesirable effects on third parties since it carried greater risks of blocking legitimate information. As such, DNS blocking, which carried less risk, was preferable.[46]

    (ii) In its judgment of May 2012 in *Dramatico v Sky (No. 2)*, the High Court of Justice of England and Wales noted: '*IP address blocking is generally only appropriate where the relevant website's IP address is not shared with anyone else. If it is shared, the result is likely to be overblocking*'.[47] Similarly, in *Cartier International v BSkyB*,[48] Arnold J accepted that IP-address blocking would not be appropriate when a target website for the purposes of a blocking order shares an IP-address with a legitimate website.

    (iii) In the decisions of the *Goldesel*[49] and *3dl.am*[50] cases, delivered on the same day, the Federal Court of Justice of Germany noted that IP-address blocking could lead to "overblocking", particularly when several websites shared a unique IP-address.[51]

    (iv) In a recent 2017 decision, the Swedish Patent and Trademark Courts of Appeal rejected the use of IP-blocking particularly in circumstances where the rights-holder had not provided sufficient evidence that the IP-addresses at issue were not shared with hosts of lawful content.[52]

27. By contrast, some courts have allowed IP-address blocking when they were satisfied that it would not affect lawful third party websites and that the rights of users would be protected. For instance, in the 11 November 2014 judgment in the *Cartier International v BskyB case,* Arnold J agreed that IP- blocking could be applied in circumstances where: (i) it was perfectly obvious that the website sharing an IP-address with a target website was engaged in 'unlawful activity'; (ii) the operators of the 'unlawful' websites would be given a seven-day grace period to move their site to another server or object before the IP address was blocked, in which case a determination would have to be made by the court.[53]

28. Notwithstanding the above, most judgments only tend to make reference to the particular outcome that ISPs are required to achieve without specifying the type of technology they should use to comply. This aspect is usually left to the discretion of the ISP. Thus, in the 2014 decision that put an end to the *Telekabel* case[54], the Austrian Highest Court did not specify the technical means that the ISP should use in order to prevent access to an infringing website, with the caveat that the ISP might be liable if such measures resulted in restricting access to lawful content. So, while cost implications may dictate an ISP's choice of blocking technology, the ISP is still bound by the obligation not to restrict access to lawful content.[55]

29. Finally, whereas in most countries *ISPs* typically have a remedy available to them to challenge blocking orders addressed to them, few countries explicitly provide *third-party websites* with a remedy when they are victim of collateral blocking. In Spain, a website owner was allowed to challenge the wrongful blocking of his site on the basis of tort liability.[56] In the UK, the English High Court agreed to an IP-blocking order drafted by the parties as third-party websites were allowed to object to IP-blocking when they shared an IP-address with a targeted website. [57]

30. In other countries, statute or case-law makes express reference more broadly to the right of *internet users* to challenge wrongful website blocking: the United Kingdom[58], Austria[59] and France.[60] In Austria, the Supreme Court has established that although affected users cannot challenge a blocking order, they can sue both the ISPs under contract law and/or the rights-holder under tort law if the blocking is overly broad. Although most countries do not appear to require that minimum information be provided about remedies for wrongful blocking, France[61] and the United Kingdom[62] explicitly require as a matter of law that users of the blocked website are redirected to a page where they will be informed of their right to challenge the decision. Although both Austrian and French law only make reference to Internet "users", it seems reasonable to assume that this right extends to third-party websites affected by a blocking order. In this sense, the laws of some countries (Belgium[63] and Spain[64]) make reference to the rights of "affected" or "interested" parties to challenge a blocking order.

III. THE PROPER APPROACH TO WEBSITE BLOCKING

Any requirement to block unlawful content must be provided by law

31. Blocking access to websites is an extreme measure of last resort, which is analogous to banning a newspaper or television station. By its very nature, it is a blanket measure that is incapable of distinguishing between the different kinds of content that a website may contain (i.e. lawful and unlawful). For this reason, the Interveners consider that blocking an entire website is almost certain to amount to a disproportionate interference with the right to freedom of expression given the risks involved and the extent of the adverse impact. As such, it should never be required by law.

32. However, to the extent that governments seek to impose blocking measures, any such measure must comply with the requirements of Article 10 (2) ECHR and be provided for in law. In particular, this means that the law should be drafted sufficiently precisely for individuals to be able to regulate their conduct.[65]

33. The Interveners further submit that blocking measures should only be permitted in respect of content, which is unlawful or can otherwise be legitimately restricted under international standards on freedom of expression.[66] Accordingly, any law providing for blocking powers should specify the categories of content that can be lawfully blocked consistent with international standards on freedom of expression.

34. Moreover, consistent with the international and comparative law standards set out in Part II, the Interveners submit that the law should provide for the following procedural safeguards:

    (i) Blocking should only be ordered by a court or other independent and impartial adjudicatory body. The Interveners note that regulatory models whereby government agencies issue blocking orders are problematic, as government agencies are – due to their executive nature - more likely to call for measures that protect the interests they are tasked to protect, such as national security or child safety, rather than freedom of expression;

(ii) When a public authority or third party applies for a blocking order, ISPs or other relevant internet intermediaries should be given the opportunity to be heard in order to contest the application;

(iii) Similarly, there should be procedures in place allowing other interested parties, such as free expression advocates or digital rights organisations, to intervene in proceedings in which a blocking order is sought;

(iv) Users should be given a right to challenge, after the fact, the decision of a court or public body to block access to content.[67] A fortiori, this must include a right for victims of collateral blocking to challenge the wrongful blocking of their website or webpage;

(v) Whenever an order has been made to block content, anyone attempting to access it must be able to see that it has been blocked and a summary of the reasons why it was blocked, in order that they may have the opportunity to challenge the decision.[68] In particular, blocked pages should contain the following minimum information:
   a) the party requesting the block;
   b) the legal basis for the decision to block; the reasons for the decision in plain language;
   c) the case number, if any, together with a link to the relevant court order;
   d) the period during which the order is valid;
   e) contact details in case of an error;
   f) and information about avenues of appeal or other redress mechanisms.

35. Finally, in countries where blocking decisions are made by public authorities, the law should guarantee that these authorities are independent of government and that their decisions can be challenged before a court or tribunal.[69] Moreover, the law should lay down the criteria to be applied by these authorities before issuing any blocking order.

Blocking orders should be strictly proportionate to the aim pursued

36. As noted above, the Interveners consider that the wholesale blocking of a website should not be required by law. Even if it is so required, it should almost certainly be considered a disproportionate restriction on freedom of expression. At the same time, the Interveners submit that any order to block access to content, as a severe restriction on freedom of expression, should be limited in scope and strictly proportionate to the legitimate aim pursued. It follows from the comparative material outlined in Part II above that in determining the scope of any blocking order, the courts should address themselves to the following:[70]

(i) Any blocking order should be as narrowly targeted as possible;

(ii) Whether the blocking order is the least restrictive means available to deal with the alleged unlawful activity including an assessment of any adverse impact on the right to freedom of expression;

(iii) Whether access to other lawful material will be impeded and if so to what extent, bearing in mind that in principle, lawful content should never be blocked;

(iv) The overall effectiveness of the measure and the risks of over-blocking, including by reference to an examination of the technologies available in order to comply with the order;

(v) Whether the blocking order should be of limited duration: in this regard, the Interveners consider that blocking orders to prevent future unlawful activity are a

form of prior censorship and as such are a disproportionate restriction on freedom of expression;

37. The same criteria should be applied by administrative bodies tasked with issuing blocking orders. Moreover, as Judge Lemmens pointed out in the *Cengiz* case, even where the law does not provide explicitly for wholesale blocking or any of the safeguards outlined above, the Court should examine whether such orders pursue a legitimate aim and are necessary and proportionate.[71]

CONCLUSION

38. Thanks to digital technologies, millions of users are now able to publish content online on a daily basis. Some of this content inevitably falls short of various countries' laws aimed at protecting the rights of others, national security, public order or public health and morals. In the last few years, States have increasingly resorted to website blocking as a silver bullet preventing access to unlawful and sometimes merely 'harmful' or 'undesirable' content.

39. The Interveners submit that website blocking is a very serious interference with the right to freedom of expression, akin to the banning of a newspaper or a television station. For this reason, it should only be permitted by this Court in the most exceptional circumstances and be subject to the strictest safeguards. As a matter of basic procedural fairness, this means that even if mandatory blocking measures are permissible in the first instance, they should have a basis in law, should be ordered by a court or other independent body and should be strictly necessary and proportionate to the aim pursued. The latter requirement necessarily entails that in considering whether to grant a website blocking order, the court or other independent body tasked with making the order should consider the impact of the order on lawful content and what technology may be used to prevent over blocking. Equally, basic procedural fairness demands that the victims of overbroad blocking orders should be given an opportunity to challenge such orders and therefore be notified of their existence.

40. This case presents the Court with an opportunity to expand on the basic procedural safeguards necessary to justify website blocking orders. Anything less than the above would seriously undermine freedom of expression online.

Gabrielle Guillemin
ARTICLE 19

On behalf of the Interveners

11 November 2019

[1] See IFÖD, EngelliWeb report, 2018, at page 2; by the end of 2018, as far as known, 1680 domain names and hundreds of URL-based news addresses and social media content were blocked by 311 separate orders made on the basis of section 8 A of the Internet law: see *Ibid,* pp. 12-15.
[2] See RSF, *Turkey's courts blocked nearly 3,000 online articles last year,* 12 Marche 2019; see also EngelliWeb report, *op. cit.* pages 16 ff.
[3] RSF, *Op. Cit.*
[4] Freedom House, *Freedom on the Net*, 2019: Turkey country report

[5] See Human Rights Watch, *Turkey: Crackdown on Social Media Posts,* 27 March 2018
[6] *Ibid.*
[7] *Ibid*.
[8] See also the 2014 decisions of the Turkish Constitutional Court in the Twitter and Youtube cases, which go in the same direction: see summary in Venice Commission, Opinion 805/2015 on Turkey Law 5651 on Regulation of Publications on the Internet and Combatting Crimes committed by means of such Publications ('the Internet law'), 16 June 2016, CDL-AD (2016)011, page 8.
[9] See Venice Commission, *Op. cit.*
[10] See Memorandum on freedom of expression and media freedom in Turkey, CommDH (2017)5, 15 February 2017, paras 100 ff
[11] See A/HRC/35/22/Add.3, 21 June 2017, at paras. 20-23 and 80.
[12] *Op. cit.* para. 103
[13] *Op. cit.* para. 111
[14] See COE Department of the Execution of Judgments, Country Factsheet: Turkey: accessed 30 October 2019
[15] See status of execution of the Yldirim case as of 2017 in HUDOC
[16] Human Rights Committee, General Comment No. 34, para 43; also *Ahmet Yildirim v Turkey*, no. 3111/10, 12 December 2012, para. 68
[17] See 2011 Joint Declaration on Freedom of Expression and the Internet: this was confirmed in the 2017 Joint Declaration on freedom of expression and 'fake news', disinformation and propaganda
[18] See A/HRC/17/27, 16 May 2011, at para. 31
[19] See A/66/290, 10 August 2011, para. 82
[20] *Ibid*. para. 82, see also A/HRC/17/27. at paras. 70 and 71.
[21] Inter-American Commission on Human Rights, Freedom of Expression and the Internet, December 2013, paras. 84-90.
[22] See Council of Europe, Recommendation CM/Rec (2016)5 of the Committee of Ministers to Members States on Internet Freedom and Recommendation CM/Rec (2018)2 on the roles and responsibilities of Internet intermediaries at 1.3.1
[23] European Court of Human Rights (ECtHR), *Ahmet Yildirim v Turkey*, no. 3111/10, 18 December 2012
[24] CJEU, C-314/12, judgment of 27 March 2014, para. 55
[25] *Ibid*. para. 57.
[26] See Article 8 amending Directive 2002/22/EC in Regulation EU 2015/2120 laying down measures on open internet access
[27] See *Ahmet Yildirim v Turkey*, *op. cit.* at paras. 31-37
[28] See Council of Europe, *Study on filtering, blocking and takedown of illegal content on the Internet*, June 2016:
[29] *Ibid*. Executive Summary.
[30] *Ibid*, Comparative analysis.
[31] See Article 8 and 12 of the French Law No. 2014-1353 of 13 November 2014, reinforcing the provisions in the fight against terrorism.
[32] See Article 2 of Decree No. 2015-125 implementing Law No. 2014-1353 cited above. The Conseil d'Etat has ruled that this blocking method (DNS) was proportionate as the risks of overblocking were limited: see France, *Conseil d'État* [State Council], judgement of 15 February 2016, No. 389140, para. 15.The Decree further establishes the administrative authority tasked with the blocking of online terrorist content and child abuse images (*Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication*' (OCLCTIC). In practice, this is a special section of the police.
[33] Compare Article 16 of the Spanish Law 34/2002, concerning Information Society Services and Electronic Commerce.
[34] See Law 21/2014 of 4 November 2013 and Royal Decree 2011/1889/2011 on the enforcement of intellectual property rights.
[35] *Ibid*.
[36] Article 510.6 of the Spanish Penal Code.
[37] See Article 8.3 of Italian Regulation No. 680/13/CONS (2013), concerning the administrative body *Autorità per le Garanzie nelle Comunicazioni* ('AGCOM'), which grants AGCOM the power to block websites. See here for a translation of the text.
[38] See CoE Report *op. cit*, at page 291 (Greece Country Report)
[39] See Article 1 (gg) of Italian Regulation No. 680/13/CONS (2013), which grants to the AGCOM the power to order the blocking of websites both through IP-address and through DNS-blocking. Since the beginning of 2017, AGCOM has only ordered the use of DNS blocking in all its resolutions. Article 4 of the Decree of 29 January 2007 on the prevention of child pornography contemplates both DNS and IP-address blocking.
[40] *Op.cit.* .
[41] These blocking powers derive from the general powers of courts to issue injunctions. In the EU, this is also as a result of Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society (Info Soc Directive) and Directive 2004/48/EC on the enforcement of intellectual property rights.

[42] See United Kingdom, High Court of Justice of England and Wales, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors*, [2014] EWHC 3354 (Ch), judgment of 17 October 2014. These criteria were confirmed by the Court of Appeal [2016] EWCA Civ 658, judgment of 6 July 2016.
[43] See Germany, *Bundesgerichthof* [Federal Court of Justice], I ZR 174/2014, judgment of 26 November 2015, para 80.
[44] See *mutatis mutandis* High Court of Justice of England and Wales, Chancery Division, *Twentieth Century Fox Film Corp & Ors v. British Telecommunications Plc* [2011] EWHC 1981 (Ch), judgment of 28 July 2011, para. 186.
[45] See Denmark, *Copenhagen Handelsretten* [Maritime and Commercial Court in Copenhagen], No. A-38-14, judgement of 11 December 2014.
[46] See Belgium, *Hof van Beroep Antwerpen* [Antwerp Court of Appeal], 2010/AR/2541, judgment of 26 November 2011.
[47] See United Kingdom, High Court of Justice of England and Wales, *Dramatico Entertainment Limited & Ors v British Sky Broadcasting Ltd & Ors* [2012] EWHC 1152 (Ch), judgment of 2 May 2012, para. 13.
[48] See High Court of Justice of England and Wales, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch), judgment of 17 October 2014, para. 256.
[49] *Op.cit.*
[50] See Germany, *Bundesgerichthof* [Federal Court of Justice], I ZR 3/2014, judgment of 26 November 2015.
[51] *Op.cit.*, para. 88.
[52] See Sweden, *Patent- och marknadsdomstolen* [Patent and Market Court of Appeal], PMT 11706-15, judgement of 13 February 2017
[53] See United Kingdom, High Court of Justice of England and Wales, Chancery Division, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors*, [2014] EWHC 3765 (Ch), judgment of 13 November 2014, paras. 8.
[54] See Austria, *Oberster Gerichtshof* [Highest Court], 4 Ob 71/14s, judgement of 26 June 2014. These proceedings gave rise to the well-known *UPC Telekabel Wien* decision of the Court of Justice of the European Union, Judgment of 27 March 2014, UPC Telekabel Wien, C-314/12, ECLI:EU:C:2014:192
[55] See e.g. in France, Cour Cass, Civ 1, 6 July 2017, *SFR and others v Association of cinema producers and others*, No 16-17.217, 16-18.298, 16-18.348, 16-18.595, ECLI:FR:CCASS:2017:C100909.. In the same sense, burden-sharing is the object of the ongoing appeal against the 2016 Court of Appeal decision in the *Cartier & Ors. v BskyB & Ors.* case (Court of Appeal of England and Wales, [2016] EWCA Civ 658): http://ipkitten.blogspot.co.uk/2017/02/the-next-round-of-cartier-uk-supreme.html.
[56] See Spain, *Audiencia Provincial de Madrid* [Provincial Court of Madrid], Decision No. 3012/2012, judgement of 29 November 2012.
[57] See *supra* note 52.
[58] See *Cartier & Ors. v BskyB & Ors*., *supra* note 49, at paragraph 262-263.
[59] See *supra* note 53.
[60] See French Decree 2015-125, of 5 February 2015, on blocking websites promoting terrorism, and of websites circulating pornographic images and representations of children, Article 3.
[61] *Ibid.*
[62] See *Cartier & Ors. v BskyB & Ors*. *supra* note 46, at paragraph 264.
[63] See Belgium, Criminal Instruction Code. Article 28sexies(1).
[64] See Spain, Law 29/1998, concerning the Contentious-Administrative Jurisdiction. Article 122bis.
[65] See, among many other authorities, *RTBF v. Belgium*, no. 50084/06, § 103, ECHR 2011
[66] See A/66/290, *op.cit,* para. 81.
[67] See e.g. ECtHR, *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, ECHR 2015
[68] See Recommendation CM/Rec(2008)6, *op.cit*. Section I. and Recommendation on the protection of human rights with regard to search engines, o*p.cit.* para 16.
[69] *Ibid.,* Recommendation CM/Rec(2008)6, Section III (ii) and *Ahmet Yildirim v Turkey*, *op.cit*, para. 64
[70] *Ahmet Yildirim v Turkey*, *op.cit*, para. 66.
[71] *Op cit*. Concurring opinion.