Strasbourg, 15 June 2016 **CDL-AD(2016)011**

Opinion No. 805 / 2015 Engl.only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

TURKEY

OPINION

ON LAW No. 5651 ON REGULATION OF PUBLICATIONS ON THE INTERNET AND COMBATING CRIMES COMMITTED BY MEANS OF SUCH PUBLICATION ("THE INTERNET LAW")

Adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)

on the basis of comments by

Mr Richard CLAYTON (Member, United Kingdom)
Ms Herdis KJERULF-THORGEIRSDOTTIR (Vice-President, Iceland)
Mr Pieter van DIJK (Former member, the Netherlands)
Mr Wolfgang BENEDEK (Expert, Austria)
Ms Karmen TURK (Expert, Estonia)

Table of contents

I. Introduction

1. In its Resolution 2035(2015) on the Protection of the safety of journalists and of media freedom in Europe, adopted on 29 January 2015, the Parliamentary Assembly of the Council of Europe requested the Venice Commission to *"analyse the conformity with European human rights standards of the Law no. 5651[1] as well as its application in practice".*

2. The Venice Commission appointed Mr Richard Clayton and Ms Herdis Kjerulf Thorgeirsdottir as well as Mr Pieter van Dijk (former member), Mr Wolfgang Benedek (Expert), and Ms Karmen Turk (Expert) to act as rapporteurs.

3. On 19-20 April 2016, a delegation of the Venice Commission visited Ankara and held meetings with representatives of the Ministry of Justice, of the Ministry of Transport, Maritime Affairs and Communications, of the Constitutional Court, of the Presidency of the Court of Cassation, of the Telecommunication and Communication Presidency, of the Turkish Bar Association and of the Union of Access Providers, as well as representatives of a number of civil society organisations. The Venice Commission is grateful to the Turkish authorities and the other stakeholders for their excellent co-operation during the visit.

4. The authorities submitted written observations on the Draft opinion during the 107th Plenary Session.

5. *This Opinion, which was prepared on the basis of the comments submitted by the rapporteurs, was discussed at the Sub-Commission on Fundamental Rights and Democratic Institutions on 9 June 2016 and was subsequently adopted by the Venice Commission at its 107th Plenary Session, in Venice (10-11 June 2016).*

II. European Standards

6. Turkey is a State party to all major international human rights instruments, including the international Covenant on Civil and Political Rights (hereinafter, "ICCPR") and the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter, "ECHR").

7. Freedom of expression is guaranteed by Article 10 ECHR, by Article 19 ICCPR and by Article 19 of the Universal Declaration of Human Rights.

8. The exercise of the right to freedom of expression may be subject to restrictions. Such restrictions have to meet the requirements foreseen in Article 10(2) ECHR and in subparagraphs (a) and (b) of paragraph 3 of Article 19 ICCPR. These requirements are as follows:

a) Legality: the restriction has to be "prescribed by law" (Article 10(2) ECHR and Article 19(3) ICCPR). This implies that the Law has to be adequately accessible and foreseeable, i.e. "*formulated with sufficient precision to enable the citizen to regulate his conduct*".[2] In addition, there must be "*a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by the Convention*".[3]

b) Legitimacy: the restriction has to pursue a legitimate aim. An exhaustive list of such legitimate aims is provided in Article 10(2) ECHR and Article 19(3) ICCPR.

[1] CDL-REF(2016)026 The Law on Regulation of Publications on the Internet and Combating Crimes Committed by means of such Publications of Turkey and Amendments of 27 March 2015.
[2] ECtHR, *Sunday Times v. United Kingdom*, Application No. 6538/74, 26 April 1979, par. 49.
[3] ECtHR, *Malone v. the United Kingdom,* Application No. 8691/79, 2 August 1984, par. 67.

c) Necessity in a democratic society: the restriction has to respond to "*a clear, pressing and specific social need*"[4] and be "*proportionate to the legitimate aim pursued*".[5]

9. The Committee of Ministers of the Council of Europe has adopted several recommendations relating to Internet freedoms. In its Recommendation CM/Rec(2015)6[6] on the free, transboundary flow of information on the Internet, the Committee of Ministers has put forth the following two general principles in this field:

> *"1.1. States have an obligation to guarantee to everyone within their jurisdiction the right to freedom of expression and the right to freedom of assembly and association, in full compliance with Articles 10 and 11 of the ECHR, which apply equally to the Internet. These rights and freedoms must be guaranteed without discrimination on any ground such as gender, sexual orientation, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.*
>
> *1.2. States should protect and promote the global free flow of information on the Internet. They should ensure that interferences with Internet traffic within their territory pursue the legitimate aims set out in Article 10 of the ECHR and other relevant international agreements and do not have an unnecessary or disproportionate impact on the transboundary flow of information on the Internet.*
>
> *2. Due diligence principles. States should exercise due diligence when assessing, developing and implementing their national policies with a view to identifying and avoiding interferences with Internet traffic which have an adverse impact on the free transboundary flow of information on the Internet."*

10. More recently, on 13 April 2016, the Committee of Ministers adopted Recommendation CM/Rec(2016)5 on Internet freedom which states, *inter alia,* that:

> *"As part of their obligation to secure to everyone within their jurisdiction the rights and freedoms enshrined in the Convention, States should create an enabling environment for Internet freedom. To this end, it is recommended that States carry out regular evaluations of the Internet freedom environment at the national level, with a view to ensuring that the necessary legal, economic and political conditions are in place for Internet freedom to exist and develop. Such evaluations contribute to a better understanding of the application of the Convention to the Internet in member States and to its better implementation by national authorities.*
>
> *2.4.1. Any restriction of the right to freedom of expression on the Internet is in compliance with the requirements of Article 10 of the Convention, namely it (…) is necessary in a democratic society and proportionate to the legitimate aim pursued. There is a pressing social need for the restriction, which is implemented on the basis of a decision by a court or an independent administrative body that is subject to judicial review. The decision should be targeted and specific. Also, it should be based on an assessment of the effectiveness of the restriction and risks of over-blocking. This assessment should determine whether the restriction may lead to disproportionate banning of access to Internet content, or to specific types of content,*

---

[4] ECtHR, *Vajnai v. Hungary,* Application No. 33629/06, 8 July 2008, par. 51.

[5] ECtHR, *Parti Nationaliste Basque – Organisation Régionale d'Iparralde v. France,* Application No. 71251/01, 7 September 2007, par. 45. See also, General Comment 34 on Article 19 ICCPR: Freedoms of opinion and expression, Human Rights Committee (2011), paras. 22 and 34: "*[R]estrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function;"*

[6] Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies).

and whether it is the least restrictive means available to achieve the stated legitimate aim."

11. Previous related recommendations of the Committee of Ministers concerning the Internet freedoms include Recommendation CM/Rec(2014)6 on a Guide to human rights for Internet users, Recommendation CM/Rec(2011)8 on the protection and promotion of the universality, integrity and openness of the Internet, Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2009)5 on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet and Recommendation Rec(99)5 on the protection of privacy on the Internet.

12. During its 1252nd meeting, on 30 March 2016, the Committee of Ministers adopted the Council of Europe Strategy concerning Internet Governance for 2016-2019. The overall aim of the Strategy is "*to ensure that public policy for the Internet is people-centred, meaning that it should respect the core values of democracy, human rights and the rule of law. Its strategic objectives are to build democracy online, to protect Internet users, and to ensure respect and protection for human rights online."*[7]

13. The Parliamentary Assembly of the Council of Europe, in its Resolution 1987(2014) on the Right to Internet Access, adopted on 9 April 2014, considered that: "[t]*he Internet has revolutionised the way people interact and exercise their freedom of expression and information as well as related fundamental rights. Internet access therefore facilitates the enjoyment of cultural, civil and political rights."* Consequently, the Assembly emphasised *"the importance of access to the Internet in a democratic society in accordance with Article 10 of the European Convention on Human Rights".*

14. The Parliamentary Assembly also adopted, on 29 January 2015, Resolution 2035(2015) on Protection of the Safety of Journalists and of Media Freedom in Europe, where it considered "*the generalised blocking by public authorities of websites or web services as a serious violation of media freedom, which deprives a high and indiscriminate number of Internet users of their right to Internet access*".

15. The European Court of Human Rights (hereinafter, "ECtHR") has a relatively rich case-law relevant in the Internet context, concerning in particular restrictions imposed on freedom of expression on the Internet[8], data-protection and retention issues relevant for the Internet under Article 8 ECHR[9], Internet and intellectual property[10], access to information and the Internet under Article 10 ECHR[11], obligation of States to combat violence and other criminal or unlawful

[7] CM(2016)10-final, 30 March 2016, Internet Governance- Council of Europe Strategy 2016-2019, point 5.
[8] ECtHR, *Delfi AS v. Estonia [GC],* Application No. 64569/09, 16 June 2015.
[9] See, among many others, ECtHR, *S. and Marper v. United Kingdom [GC],* Application Nos. 30562/04 and 30566/04, 4 December 2008 where the ECtHR considered that the protection of personal data is of fundamental importance to a person's enjoyment of his right to respect for private and family life; ECtHR, *Copland v. the United Kingdom,* Application No. 62617/00, 3 April 2007, where the ECtHR stated that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8. There are also a number of pending cases before the ECtHR, currently under examination, concerning data protection with specific reference to the Internet (*Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*, Application No. 62322/14, communicated to the Government on 5 January 2015, and *Benedik v. Slovenia,* Application No. 62357/14, communicated to the Government on 8 April 2015, concerning the legal obligation for an Internet access provider to divulge to the police the personal details attached to an IP address, without the consent of the subscriber.
[10] ECtHR, *Neij and Sunde Kolmisoppi v. Sweden* (dec.), Application No. 40397/12, 19 February 2003.
[11] In *Times Newspapers Ltd v. the United Kingdom,* Application Nos. 3002/03 and 23676/03, 10 March 2009, the ECtHR held that in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general.

activities[12], etc. In the case of *Times Newspapers Ltd v. the United Kingdom,* the ECtHR applied the general principles developed in relation to Article 10 ECHR to cases concerning *online* publication: "*In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10.*"[13] It further put an emphasis, in the case of *Editorial Board of Pravoye and Shtekel v. Ukraine*[14]*,* on the States' positive obligation to create a sufficient regulatory framework to ensure effective protection of journalists' freedom of expression on the Internet while it recognised at the same time that "*the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press.*"[15]

16. The European Parliament adopted, on 15 March 2006 Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks[16], and Recommendation 2008/20160(INI) of 26 March 2009 on strengthening security and fundamental freedoms on the Internet[17]. In April 2014, the Grand Chamber of the European Court of Justice declared the Directive 2006/24/EC (the Data Retention Directive) invalid on the ground that European Union legislator had exceeded the limits of proportionality in forging the Directive (see, para. 81 of the present Opinion).

III. European findings concerning Internet freedom in Turkey

A. Resolutions and reports

17. According to an Information Note provided by the authorities, Law No. 5651, which was enacted on 4 May 2007 and entered into force on 23 May 2007 upon its publication in the Official Gazette[18], aims at fighting against offences committed by misuse of opportunities provided by electronic communication devices and the Internet, and at taking necessary preventive measures against the broadcast promoting the use of drugs and stimulants, inciting to suicide, sexual exploitation and gambling, etc.

18. On 11 January 2010, the Representative of the Organization for Security and Co-operation in Europe (hereinafter, "OSCE") on Freedom of the Media published a Report on the Turkish Internet Law.[19] The report argued, *inter alia,* that the banning of social networks such as YouTube and Google Sites has very strong implications on political expression and that the State's response to Internet content and publications is evidently problematic and the blocking orders issued by the courts and the Presidency of Telecommunication and Communication (hereinafter, "Presidency of Telecommunication" or "Presidency") resulted in blocking access not only to allegedly illegal content but also legal content and information. The report recommended, on the basis of legal and procedural deficiencies identified, that the government should urgently bring Law no. 5651 in line with international standards on freedom of expression, or otherwise should consider abolishing the Law.

19. In his Report published on 12 July 2011 following his visit to Turkey on 27-29 April 2011, the Commissioner for Human Rights of the Council of Europe identified a number of

[12] ECtHR, *K.U. v. Finland,* Application No. 2872/02, 2 December 2008.
[13] ECtHR, *Times Newspapers Ltd v. the United Kingdom,* cited above, para. 27.
[14] ECtHR, *Editorial Board of Pravoye and Shtekel v. Ukraine,* Application No. 33014/05, 5 May 2011.
[15] *Idem*., para. 63.
[16] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
[17] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//EN
[18] Except Articles 3 and 8 which entered into force in November 2007.
[19] http://www.osce.org/fom/41091

problematic issues concerning the implementation of Law No. 5651, including, for instance, that 80% of the blocking orders under Article 8 of the Law (entitled "the decision to deny access and implementation thereof) were issued by an administrative body, Presidency of Telecommunication, in an administrative procedure while the rest have been ordered by courts or a judge, the broad interpretation of the grounds listed in Law No. 5651 for access-blocking to web-sites and the re-imposition of a blanket ban on YouTube on 4 March 2011[20]. These observations led the Commissioner to recommend, *inter alia,* a review of the Internet Law in order to circumscribe the grounds for restriction to those accepted in the case-law of the ECtHR, as he considered that the censorship of the Internet and the blocking of web-sites went beyond what was necessary in a democratic society.

20. A peer review report by the European Union, published in 2011, also concluded that the Internet Law should be either abolished or revised. The report recommended that the higher courts should be made competent to perform the judicial review of blocking orders and that a "strong public interest" clause should be included in the Law in order to better protect journalists, bloggers and other publishers.[21]

B. Case-law of the European Court of Human Rights

21. In December 2012, the ECtHR found a violation of Article 10 ECHR in the case of *Ahmet Yıldırım v. Turkey*[22] which is the first ECtHR ruling addressing access-blocking measures on the Internet taken on the basis of Law No. 5651. The case involved a court decision concerning total access-blocking to the Google Sites Platform from Turkey, in order to prevent further access to one particular website, hosted by the Google Sites, which contained material deemed offensive to the memory of Mustafa Kemal Atatürk (Article 8 (1)b of Law No. 5651). As a result, the applicant was unable to access his academically focused website, also hosted by the Google Sites, which was unrelated to the website with the allegedly offensive content. In its ruling, the ECtHR concluded that the applicant was victim of a "collateral damage" and that the interference into his right to freedom of expression was not "prescribed by law", since the relevant sections of Law No. 5651, which deal with the liability of content providers, hosting providers and access providers, made no provision for a wholesale blocking of access such as that ordered in this case. It further observed that the measure in question produced arbitrary effects and could not be said to have been aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all the sites hosted by Google Sites. Also, the judicial review procedures concerning the blocking of Internet sites were insufficient to meet the criteria for avoiding abuse, as domestic law did not provide for any safeguards to ensure that a blocking order in respect of a specific site is not used as a means of blocking access in general.[23]

22. Similarly, the case of *Cengiz and others v. Turkey*[24] concerned an Ankara court decision rendered in May 2008, which, finding that the content of ten pages on the YouTube website infringed the prohibition on insulting the memory of Atatürk, imposed a blocking order on the entire website which had remained blocked from 5 May 2008 to 30 October 2010. The ECtHR found that the legislation [*i.e.* Law No. 5651] had not authorised the imposition of a blanket blocking order on an entire Internet site on account of the content of one of the web pages hosted by it. The authorities should have taken account of the fact that such a measure, which blocked access to a large quantity of information, would inevitably considerably affect the rights of Internet users and have a substantial collateral effect. Accordingly, the blocking order had not satisfied the condition of lawfulness.

---

[20] CommDH(2011)25 Report by Thomas Hammerberg Commissioner for Human Rights of the Council of Europe, following his visit to Turkey from 27 to 29 April 2011, paras. 60 *et seq.*

[21] European Union, Report on the Peer Review Visit by Lord Mac Donald of River Glover, QC, April 2011. See also, Wolfgang Benedek and Katrin Nyman-Metcalf, *Report on the findings and recommendations of the Peer Review Mission on Freedom of Expression* (Istanbul and Ankara, 12-16 May 2014).

[22] ECtHR, *Ahmet Yıldırım v. Turkey,* Application No. 3111/10, 8 December 2012.

[23] See para. 68.

[24] Application Nos. 48226/10 and 14027/11, 1 December 2015.

IV. Domestic developments concerning freedom of internet

23. In parallel with the European Court of Human Rights, the Turkish Constitutional Court has served as a crucial check on the executive authorities concerning the freedom of expression on the Internet. In a judgment of 2 April 2014 in the framework of an individual application, the Constitutional Court held that a decision of the Presidency of Telecommunication on blocking access to Twitter infringed the applicants' right to freedom of expression. The Constitutional Court observed that the court decisions the Presidency had depended on, namely to block certain URL addresses, did not give rise to a justification for the administrative authority to block the website completely. As a consequence, the Court concluded that banning access to «twitter.com» by the administrative act had no legal basis and hence gave rise to a serious violation of the freedom of expression of all users of the internet website «twitter.com»[25]. The ban on Twitter was lifted accordingly on 3 April 2014.

24. On 29 May 2014, the Constitutional Court decided, also in the framework of an individual application, that a ban blocking access to YouTube imposed by the Presidency in order to prevent the disclosure of state secrets which were disseminated through some 15 URL links on YouTube, was in breach of the applicants' right to freedom of expression. Similar to its reasoning in the Twitter case, the Constitutional Court held that there was no legal provision in the Law allowing the domestic authorities to impose a blanket blocking order on access to the entire website (YouTube), on account of one of its contents.[26]

25. The Internet Law was amended three times in 2014. The amendments introduced in February 2014, by Laws nos. 6518 (6 February 2014) and 6527 (26 February 2014), brought some new procedures concerning access-blocking to websites.[27]

26. The amendments introduced in February 2014 brought some changes to the Law, as, for instance, the amendment to Article 8 which currently provides that the decision to block access to a website under Article 8 may only be given for a limited period of time (before the amendment there was no specific time-limit), and the amendment introduced to Article 9(4) which brought the obligation for the judge to order the blocking of (only) a specific publication (in the form of URL etc.), and not of the whole website, unless this is not possible for technical reasons. In this case, the judge may issue a blocking order on an entire website under a number of conditions.

27. The amendments also increased the powers of the Presidency of Telecommunication and the number of alternative procedures for access-blocking. By the amendments introduced to Articles 4(3) and 5(5) of the Internet Law, the content provider and the hosting provider, respectively, became obliged "*to furnish the Presidency with such information as it may demand within the scope of the performance by the Presidency of functions delegated to it by this Law and other legislation, and shall take such measures as may be directed by the Presidency*". These provisions were later annulled by the Constitutional Court by a judgment of December 2015 (see below). The new Article 9(A), introduced on 6 February 2014, also provides in its paragraph 8 that "*in circumstances where it is considered that delay may present a risk of violation of the confidentiality of private life, the denial of access shall be carried out by the Presidency upon the direct instructions of the President."*

---

[25] Constitutional Court, Application No. 2014/3986, 2 April 2014.
[26] Constitutional Court, Application No. 2014/4705, 29 May 2014.
[27] The legislative process concerning those amendments was criticized by the OSCE Representative on Freedom of the Media, in a report published in January 2014, observing that no consultation process had been conducted during the preparation of the draft amendments, which prevented any meaningful public debate on the issue and that the amendments to the Internet Law were added into an "omnibus amendment law" which included irrelevant amendment proposals on the Family and Social Policy Ministry, the Social Security and the General Health Insurance Law and many others. See OSCE Representative on Freedom of the Media, Briefing on Proposed Amendments to Law No. 5651 The Internet Law of Turkey, January 2014, p. 3 (http://www.osce.org/fom/110823?download=true)

28. The amendment to Article 8, introduced in February 2014, was debated before the Committee of Ministers of the Council of Europe in the context of the supervision of the execution of the ECtHR judgment in the case of *Ahmet Yıldırım v. Turkey* during its 1208th DH meeting (23-25 September 2014). The Committee of Ministers considered that "*it does not appear that legislative amendments made to Article 8 of Law No. 5651 in February 2014 have changed the wording of this provision in a way that would satisfy the foreseeability requirement under the Convention and lifted the concerns raised by the Court in the present judgment as to the arbitrary effects of decisions blocking access to websites. The amendments indicated (…) do not seem relevant to solving the problem identified by the Court in the present judgment."* The issue of the execution of this judgment is still pending before the Committee of Ministers.

29. In March 2015, the Internet Law was further amended. The amendment introduced a new Article 8(A), which provided for another access-blocking procedure ("Removal of content and/or blocking of access in circumstances where delay would entail risk") which starts at the initiative of the Office of the Prime Minister and the Ministry concerned with the protection of national security and public order for a number of reasons, including the protection of national security, public order etc., with *ex post* judicial control over the blocking measure.

30. By a judgment of 8 December 2015, the Constitutional Court annulled Articles 4(3)d, 5(5) and 6(1)d concerning, respectively, the obligation imposed on content and hosting providers to furnish to the Presidency information as requested (see para. 27 of this Opinion) and the obligation imposed on access providers to take measures to prevent alternative methods of access to publications concerning which there has been a decision to block access.[28] The judgment of the Constitutional Court will enter into force on 28 January 2017.

31. The Turkish authorities declined the Venice Commission delegation's request for official statistics regarding the actual number of blocked URLs or websites. According to unofficial sources[29], as of May 2015 approximately 80 000 websites had been reportedly blocked in the country.[30] In a press release of 15 April 2016, the OSCE Representative on Media Freedom underlined that more than 110 000 websites and thousands of news and social media related URLs were blocked from Turkey, many without judicial oversight. The Representative on Media Freedom added that the Internet Law remains in urgent need of reform.[31]

V. Analysis

A. Access-blocking procedures in Law No. 5651

1. General considerations concerning the access-blocking procedures in the Law

32. Law No. 5651 provides for four different access-blocking procedures:
   a. Article 8 ("The decision to deny access, and implementation thereof");
   b. Article 8A ("Removal of content and/or blocking of access in circumstances where delay would entail risk");
   c. Article 9 ("Removal of content from publication, and blocking of access"); and
   d. Article 9A ("Blocking access to content on grounds of the confidentiality of private life").

33. It appears, however, that there is a fundamental difference between the procedure of access-blocking under Article 8 of the Law, and the procedures foreseen under Articles 8A, 9 and 9A.

[28] CDL-REF (2016)027 Judgement of the Constitutional Court of Turkey (2014/87E, 12015/112K) of 8 December 2015.
[29] The Turkish authorities contested the accuracy of the information provided by unofficial sources.
[30] http://freedomhouse.org/report/freedom-net/2015/turkey
[31] http://www.osce.org/fom/233926

34. Under Article 8, the measure of access-blocking appears as a "precautionary measure" or "interlocutory measure", taken in the framework of criminal proceedings concerning the crimes listed under Article 8(1) a) and b), by a judge at the investigation stage and by a court at the prosecution stage, or by a public prosecutor at the investigation stage where delay would present a risk. The "destiny" of the "precautionary measure" is linked to and depends on the substantial criminal procedure, since, according to paragraphs 7 and 8 of Article 8, a decision not to prosecute by the public prosecutor at the end of the subsequent investigation into the commission of crimes indicated in the first paragraph of Article 8, and an acquittal decision given by criminal courts at the prosecution stage, result in the lifting of the blocking measure (precautionary measure) ordered at the investigation or prosecution stage. Thus, the aim of the precautionary measure under Article 8(2) is to prevent the risk of irreparable damages and to maintain the status quo pending the criminal trial concerning the catalogue crimes under Article 8(1).

35. Instead, differently from Article 8, Articles 8A, 9 and 9A establish independent access-blocking procedures which are not linked to and do not depend on any other substantive criminal or civil procedure. In other words, the "access-blocking" decisions taken in the context of Articles 8A, 9 and 9A are not "precautionary measures" in order, for instance, to prevent the risk of irreparable damages pending the substantive trial, but constitute fully-fledged, independent procedures through which substantive decisions on "access-blocking" are taken. Consequently, because of this fundamental difference between the nature of "access-blocking" decisions taken under Article 8, on one hand, and Articles 8A, 9 and 9A, on the other, these procedures will be examined separately below.

36. In its Recommendation CM/Rec(2016)5 on Internet Freedom, the Committee of Ministers of the Council of Europe considered that "*before restrictive measures to Internet access are applied, a court or independent administrative authority determines that disconnection from the Internet is the least restrictive measure for achieving the legitimate aim*". As mentioned above, the principle of "least intrusiveness" is an important element of the proportionality requirement when reviewing the conformity of such restrictions with European and international standards.

37. However, the only measure provided for in Law No. 5651 is the measure of access-blocking/removal of content which is the most severe measure possible on the Internet. The Law does not provide for any other measure, less intrusive than blocking/removal, as for instance, requirement of "explanation" from the interested party (content provider, web-site owner, etc.), "response", "correction", "apology", "content renewal", "access renewal" etc. Moreover, the Law does not leave the judge (or the Presidency) any room for imposing a lower sanction in specific circumstances following a proportionality assessment. The authorities explained that the Internet Law, in its original version, contained less intrusive measures, as there was possibility for individuals who claim that their personal rights are infringed through a publication on the Internet, to ask the content provider or hosting provider to publish a "reply" on the same webpage. But this procedure, according to the authorities, did not provide for a fast and efficient remedy to those who claim a violation of their personal rights and was subsequently repealed. The Venice Commission recalls that, as the ECtHR has held in the case of *Wegrzynowski and Smolczewski v. Poland,* rectification or an additional comment on the website may be a sufficient and adequate remedy, in which case the access-blocking/removal of content measure may be considered as disproportionate to the legitimate aims pursued by the restriction and thus constitute a violation of the freedom of expression. Consequently, it is strongly recommended that Law No. 5651 be amended in order to introduce a list of less intrusive measures than access-blocking/removal of content which would allow the judge to make a decent proportionality assessment and apply the least restrictive measures if they are considered as sufficient and adequate to reach the legitimate aim pursued by the restriction.

38. One of the requirements of the principle of proportionality is that the reasons given by the national authorities to justify restrictions to the right to freedom of expression should be relevant and sufficient. Furthermore, this is also a requirement of the principle of fair trial under Article 6 ECHR: judgments of courts and tribunals should give an adequate statement of the reasons on which they are based.[32] A lower court should also give such reasons as to enable the parties to make effective use of any existing right of appeal.[33] Some decisions of the peace judgeships which the Venice Commission has been able to see during the meetings in Ankara, do not provide for any motivation and reasons to justify the interference with the right to freedom of expression. The Venice Commission does not have at its disposal sufficient examples of judgeship decisions. However, it reiterates the crucial importance of the statement of reasons in a court decision in order not only to respect the principle of proportionality under Article 10 ECHR, but also to satisfy the requirements of fair trial under Article 6 ECHR.

39. When assessing the "necessary in a democratic society" condition, the ECtHR always considers the nature and severity of the sanction imposed. Recommendation CM/Rec(2016)5 of the Committee of Ministers states that restrictions to the right to freedom of expression should not inhibit public debate or criticism of State bodies and should not impose excessive fines or disproportionate awards of damages or legal costs.[34] The ECtHR has stressed that, although punitive fines or criminal sanctions could be effective in encouraging compliance with any pre-notification requirement, these run the risk of not being in compliance with Article 10 ECHR and create a chilling effect which would be felt in the spheres of political reporting and investigative journalism which attract a high level of protection under the ECHR. Law No. 5651 sets forth severe sanctions in each of its relevant articles. For instance, under Article 8(10), failing to take the action necessary to implement the decision to block access as a precautionary measure shall, unless the act constitutes an offence which incurs a heavier penalty, be punished by a judicial fine equivalent to from five hundred to three thousand days[35]; under Article 8(11), if the decision to deny access issued as an administrative precaution is not implemented, an administrative fine of from ten thousand (3038.41 euros) to one hundred thousand (30 384.09 euros) New Turkish Lira shall be imposed by the Presidency on the access provider.[36] These judicial and administrative fines appear excessive, in view of the proportionality test of the restriction, in cases where the risk created by the publication on the Internet is minor. It is advisable to limit the judicial fines to the maximum limit indicated in Article 52 of the Penal Code and to reduce the administrative fines foreseen in the Law.

40. Interested parties have the possibility to lodge an individual application before the Constitutional Court alleging a violation of their rights following an access-blocking measure under Law no. 5651. During the meetings in Ankara, the representatives of the Constitutional Court stated that, given the important role played by the Internet in public's access to information and dissemination of information, the cases concerning access-blocking are given priority in the practice and an urgent procedure is applied. The Venice Commission welcomes this approach. During the meetings in Ankara, the Commission has learned from the part of certain applicants that there are an important number of cases pending before the Constitutional Court concerning the blocking orders. The Commission encourages the Constitutional Court to establish a constant practice of applying the urgent procedure to cases

[32] See, among others, *Rummi v. Estonia*, Application No. 63362/09, 15 January 2015, para. 82.
[33] See, *Hirvisaari v. Finland*, Application No. 49684/99, 27 September 2001, para. 30.
[34] CM/Rec(2016)5 Recommendation of the Committee of Ministers to member States on Internet Freedom, point 2.4.2.
[35] According to Article 52 of the Turkish Penal Code, a judicial fine is an amount payable to the State Treasury by the offender, which is calculated, unless otherwise stated in the law, by multiplying the identified number of days, which shall be more than five but not more than seven hundred and thirty, with a daily amount. The daily amount of the judicial fine shall be, at least, twenty Turkish liras (6.23 euros) or, at most, one hundred Turkish Lira (31.17 euros) and shall be determined having regard to the personal and economic conditions of the person. For instance, a judicial fine of 500 days would be between 3115 euros and 15 585 euros and a judicial fine of 3000 days would be between 18 690 euros and 93 510 euros according to the assessment of the judge concerning the economic situation of the person concerned (CDL-REF(2016)011 Penal Code of Turkey).
[36] See also Articles 8A(4) and (5) and 9 (10) of the Internet Law.

involving the freedom of expression in the Internet context and to keep a publicly accessible register of pending Internet cases.

2. Access-blocking procedure in Article 8

41. A decision on access-blocking following the procedure under Article 8, shall be issued if there are sufficient grounds for suspicion that the content constitutes any of the crimes listed in paragraphs a) and b) of para. 1 of this Article: 1) Incitement to commit suicide (article 84 of the Criminal Code), 2) Sexual exploitation of children (article 103, first paragraph), 3) Facilitating the use of narcotic or stimulant substances (article 190), 4) Supply of substances which are dangerous to health (article 194), 5) Obscenity (article 226), 6) Prostitution (article 227), 7) Providing premises or facilities for gambling (article 228), and any of the offences under the Law on Offences against Atatürk, Statute 5816, dated 25/7/1951.

42. Articles 8(2) and 8(4) provide for two different access-blocking measures: under Article 8(2), a "precautionary measure", taken by a judge at the investigation stage and by a court at the prosecution stage or by a public prosecutor at the investigation stage where delay would present a risk, and in Article 8(4), an "administrative measure" taken directly by the Presidency of Telecommunication.

43. According to Article 8(2), in case the decision on access-blocking is taken by the public prosecutor, this decision shall be submitted to the approval of a judge within 24 hours and the judge shall give his/her decision within a maximum of 24 hours. If the judge does not validate it, the blocking measure is lifted immediately. The lifting of a blocking measure results also from a decision not to prosecute of the public prosecutor at the end of the subsequent investigation into the commission of crimes indicated in the first paragraph of Article 8, and from an acquittal decision given by criminal courts at the prosecution stage.

44. Under Article 8(4), the Presidency of Telecommunication has competence to issue an *ex officio* blocking order which is executed by the access provider within a maximum of four hours as from the notification, in two different situations: 1) the content or hosting provider of the publications with content which constitutes offences as specified in the first paragraph of Article 8 is located outside the country, and 2) the content of publications constitutes offences mentioned in subsections (2) and (5) and (6) of section (a) of the first paragraph of Article 8 (i.e. sexual exploitation of children, obscenity and prostitution), even if the content or hosting provider is located within the country.

45. The issuing of an access-blocking decision, under both paragraphs (2) and (4) of Article 8, constitutes an interference into the right to freedom of expression that requires justification under any of the grounds and legitimate aims listed in the second paragraph of Article 10 ECHR.[37] The crimes listed in paragraph 1 of Article 8 as grounds for blocking orders appear to be covered by several legitimate aims for restrictions listed in the second paragraph of Article 10 ECHR, as for instance, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, etc. The restrictions under those legitimate grounds, in order to respect the right to freedom of expression, must also be necessary in a democratic society, i.e. they should be suitable to realise the legitimate aims put forward to justify the interference, there should be a pressing social need for the interference and the restrictions should be proportional to the legitimate aims pursued and least intrusive into the right.

46. The decision on access-blocking following the procedure under Article 8 shall be issued if there are "sufficient grounds for suspicion" that the content constitutes any of the crimes listed in para. 1. The term "sufficient grounds for suspicion" is borrowed from Article 170 of the Code of Criminal Procedure (hereinafter, "CCP"), and is a prerequisite for the submission of an indictment by public prosecutors, thus a condition for the initiation of the prosecution stage

[37] See the relevant ECtHR case-law in paragraph 15 of this Opinion.

under criminal procedural law. As Article 8 uses this term without distinguishing it from that used in Article 170 CCP, it should be assumed that the level of suspicion required for the procedure under Article 8 is similar to the level of suspicion required by Article 170 CCP (submission of an indictment). Consequently, "sufficient grounds for suspicion" should not be interpreted as an autonomous concept by the judge (peace judgeships) or the Presidency of Telecommunication, but should follow the strict conditions set forth in Article 170 CCP. The same holds true for the interpretation of the crimes listed in paragraph 1 of Article 8. As this paragraph refers directly to the provisions of the Criminal Code, the peace judgeship or the Presidency of Telecommunication, when applying the access-blocking procedure under Article 8, should strictly interpret the crimes listed in paragraph 1, since an interpretation broader than their meaning in the Criminal Code may create problems concerning the foreseeability of the interference and constitute a breach of Article 10 ECHR for not fulfilling the requirement that the interference should be "prescribed by law".

47. The Venice Commission has learned that the term "obscenity" indicated in Article 8, para 1/a/5 and the term "prostitution" indicated in Article 8, para. 1/a/6, are given a broad interpretation by the peace judgeships and the Presidency of Telecommunications when blocking access to LGBT related websites, as websites defending LGBT rights or homosexual dating sites. In a decision of 26 August 2013, the 14th Criminal Peace Court of Istanbul decided[38], on the basis of an allegation that the personal information about the complainant was used in order to create a fake account on a homosexual dating site (grindr.com), to block the access to the entire web-site from Turkey, considering that the web-site content was in breach of the prohibition of "obscenity" and "prostitution". Other LGBT related websites, as for instance Lezce or Gaymag, were blocked by the Presidency of Telecommunication for "obscenity", but those measures were subsequently revoked by the Presidency when a media campaign criticised the decisions of access-blocking. It has been claimed that, in practice, any web-site related to LGBT issues can be considered as "obscenity" by the Presidency and the judges/courts. Without being in a position to assess the content of the above-mentioned web-sites and the individual decisions on blocking access, the Venice Commission reiterates that the broad interpretation of the crimes listed in Article 8, para. 1, as for instance "obscenity", will first and foremost create a problem of foreseeability, since, to the knowledge of the Venice Commission, in the established case-law of the criminal courts in Turkey, mere sexual orientation or legitimate expressions of sexual orientation are not considered as "obscenity" under Article 226 of the Criminal Code. Thus, the decision-making bodies on access-blocking (especially the Presidency and the peace judgeships), should follow the guidance of the criminal courts in the interpretation of the crimes listed in Article 8 para. 1. for the sake of foreseeability of the interference into the right to freedom of expression.

48. Although Article 8 limits the procedure to cases where there is "sufficient suspicion" of the commission of any of the crimes listed in paragraph 1 and thus satisfies the requirement that the interference must pursue a legitimate aim, it does not mention, explicitly or implicitly, the requirement that the restriction must be "necessary in a democratic society". In addition, the provision, according to the English translation, is a "shall" provision, meaning that a decision to block access will have to be issued in case the internet publication contains any of the content listed there. However, the resulting interference with the freedom of expression is only justified if it is necessary for the protection of any of the interests listed in the second paragraph of Article 10 ECHR and if it meets the proportionality requirement. As mentioned above, in order to be "necessary in a democratic society", the "interference" with the freedom of expression should correspond to a "pressing social need" and be proportionate to the legitimate aim pursued while the reasons given by the national authorities to justify it should be relevant and sufficient.[39] Especially in view of the far-reaching restrictions as a wholesale blocking of a site regardless of its present and future content, but also in case of blocking orders concerning a precise content (URL address), the test of proportionality is of vital importance when reviewing the conformity of such restrictions with European and international standards.

[38] Istanbul 14. Criminal Peace Court, 2013/406 D.is.
[39] see *The Sunday Times v. the United Kingdom* (no. 1), judgment of 26 April 1979, Series A no. 30, p. 38, § 62.

49. Although the principle of "democratic necessity" is guaranteed in Article 13 of the Constitution[40] and even though the authorities stated that judges are under the obligation to apply the "democratic necessity test" in their case-law, this principle should preferably be included in Article 8 as a reminder and a yardstick in order to strike a fair balance between the right to freedom of expression and the public interest in the protection of legitimate aims pursued by the restriction.

50. According to Article 8(2), an objection to an access-blocking decision taken as a precautionary measure (*i.e*. taken by a judge or public prosecutor, as opposed to administrative measure taken by the Presidency (art. 8(4)) may be made under the Code of Criminal Procedure. According to Article 268 (3)a of the CCP (amended on 18 June 2014) the appeal against a decision given by a peace judgeship can be made, in places where there are several peace judgeships, to the peace judgeship bearing the next number. If there is only one peace judgeship in a given place, the appeal should then be made to the peace judgeship which is within the competence zone of the closest assize criminal court. The decision given by a peace judgeship in appeal procedure is final. Thus, as in other access blocking procedures under Law No. 5651 (*i.e.* procedures under Articles 8A, 9 and 9A – see below), the measure of access blocking taken by a peace judgeship cannot be appealed against before the Court of Cassation, but only before another peace judgeship and the only appeal mechanism is the framework of an individual application to the Constitutional Court.

51. First, the provision does not provide for any notification procedure of the interested party about the procedure under Article 8(2). The authorities explained that the name of the court or authority that implement the order of access blocking, is displayed on the relevant page of the website whose access is blocked due to violent content and the concerned party is consequently informed about the access blocking measure However, the Commission stresses that this is not sufficient and a proper notification procedure should be put in place in order to give the content providers the opportunity to have knowledge of the blocking measure and of the reasons put forth by the authorities to justify the measure. Those are however essential elements in order for the legal remedy provided under Article 8(2) to be effective. The principle of "equality of arms" implies that each party must be afforded a reasonable opportunity to present his/her case – including his/her evidence- under conditions that do not place him/her at a substantial disadvantage vis-à-vis the other party.[41] Furthermore, it is clear under the case-law of the ECtHR that it is inadmissible for one party to make submissions to a court without the knowledge of the other and on which the latter has no opportunity to comment. It is strongly recommended that the provision be amended to impose on the authorities the obligation to notify the interested party about the access-blocking measure and its reasons. This is all the more important in view of the heavy fines imposed on the access/hosting providers for failure to implement the blocking decisions taken as precautionary or administrative measure under para. 10 and 11 of Article 8.

52. Secondly, the lack of cassation appeal against the blocking-access measure under Article 8 may be explained to the extent that the measure of access-blocking under Article 8(2) is only a "precautionary measure" taken in the framework of criminal proceedings concerning the crimes listed under Article 8(1) a) and b). At any rate, the competent criminal court, i.e. the trial court judge in criminal proceedings, should be empowered to review the necessity of maintaining the precautionary measure on access-blocking and to lift this measure immediately, if he/she considers that the measure is not necessary in order, for instance, to prevent any risk of irreparable damages pending substantial trial. The trial court judge is best placed to assess the necessity of the precautionary measure related to the case-file under his/her examination and the interested parties (i.e. content or hosting provider) should have the possibility to ask the trial court judge the lifting of this precautionary measure at any stage of the criminal procedure. Nevertheless, it is deplorable that Article 8 does not draw all the consequences of the

[40] "[the] restrictions shall not be in conflict with the letter and spirit of the Constitution and the requirements of the democratic order of the society and the secular Republic and the principle of proportionality."
[41] See, ECtHR, *Dumbo Beheer B. V. v. the Netherlands,* Application No. 14448/88, para. 33.

consideration of the blocking-measure as a "precautionary measure" pending trial: it is not at all clear in Article 8, whether at the prosecution stage, the trial court judge has or has not the power to lift the blocking measure taken by a peace judgeship at the investigation stage or by the Presidency of Telecommunication, before the criminal court gives a decision on the substance of the accusation (i.e. conviction or acquittal). On the contrary, paragraph 8 of Article 8, which states that the decision to block access shall be invalidated "if the prosecution results in an acquittal" appears to exclude any possibility for the trial court judge to review the necessity of the blocking measure and to lift it before the end and during the criminal trial. It is not acceptable that the decision taken by a peace judgeship as a "precautionary measure" should be binding on the trial court judge in the substantive criminal proceedings. Consequently, Article 8 should clearly mention that the criminal court has the power to review the necessity of maintaining the "precautionary measure" on access-blocking taken by a peace judgeship or the Presidency and to lift this measure at any moment during the criminal trial.

53. Concerning the *ex officio* blocking orders issued by the Presidency of Telecommunication under conditions indicated in Article 8(4), *i.e.* the content or hosting provider is located outside the country or the content of publications constitutes offences of sexual exploitation of children, obscenity and prostitution, the necessity of this provision is not clear to the Venice Commission. The access-blocking measure under Article 8 is a precautionary measure taken in the framework of a criminal case and it should be the role and responsibility of a judge to assess the necessity of this measure during the criminal trial. The reasons set forth under Article 8(4) do not justify the competence of an administrative body to issue *ex officio* blocking orders without prior judicial review. This competence of the Presidency should be repealed.

3. Access-blocking procedures in Articles 8A, 9 and 9A

54. As opposed to Article 8, the procedures on access-blocking under Articles 8A, 9 and 9A do not concern an interlocutory or precautionary measure taken in the framework of a pending criminal or civil procedure before the domestic courts, but constitute fully-fledged, autonomous procedures through which substantive decisions on "access-blocking" are taken for a number of aims indicated in those Articles. It is true that Article 9A for instance, in its first paragraph uses the term "measure" for the access-blocking decisions taken in order to protect the confidentiality of private life. However, the use of this term is of no consequence, since, as in Articles 8A and 9, the existence of a civil or criminal procedure is not a requirement of the "autonomous" access-blocking procedure under this Article. Also, the applicants who request the application of an access-blocking measure under the procedures set forth in Articles 9 and 9A, for instance, claiming that their personal rights or privacy have been violated as a result of a publication on the Internet, are not under an obligation to introduce civil or criminal procedures against those responsible for the violation of their rights to privacy. This nature of the access-blocking decisions under Articles 8A, 9 and 9A, which is fundamentally different from the nature of the precautionary measure of access-blocking under Article 8, should be taken into account when assessing the conformity of those procedures with international standards.

55. The amendment of the Internet Law in March 2015 added a new Article 8A providing for an additional procedure for removal of content and/or blocking of access in order to protect the right to life or security of life and property, national security and public order, public health and for the prevention of commission of crimes (Art. 8A(1)). According to this provision, access to an Internet site may be blocked by a judge (peace judgeship), or where a delay would present a risk, by the Presidency of Telecommunication, subsequent to a request by the Office of the Prime Minister or a ministry concerned with the protection of national security and public order, the prevention of commission of crimes or the protection of public health. The access providers and the content and hosting providers shall be immediately notified by the Presidency of the decision and the blocking or removal measure shall be implemented immediately, within a maximum of four hours as from the notification of the decision. According to para. 2 of Article 8A, any decision for the removal of the content and/or blocking of access issued by the Presidency at the request of the Office of the Prime Minister or the relevant ministries shall be

submitted by the Presidency for approval by a magistrate within 24 hours. The judge shall announce his/her decision within 48 hours; otherwise the decision shall automatically lapse.

56. Article 9 provides for another procedure for access-blocking/removal of content for the violation of "personal rights" as a result of information published on the Internet. According to paragraph 1, real persons, legal entities and institutions and organisations may, if they assert that their "personal rights" have been violated, apply for removal of publication of that content by means of a warning to the content provider or, if the content provider cannot be contacted, to the hosting provider, or they may also apply directly to a judge to request denial of access to the content. The judge shall make a decision within a maximum period of 24 hours without holding a hearing.

57. Under the procedure provided for in Article 9A, persons who assert that the confidentiality of their private life has been violated by a publication on the Internet may, by applying directly to the Presidency, request that access to that content be blocked. The Presidency shall immediately inform the Union of Access Providers in order to ensure that this request is implemented, and access providers shall carry out the request immediately, within a maximum of four hours. Persons who request blocking of access shall submit their demand for prevention of access to a judge within twenty four hours of the demand for blocking of access. The judge shall announce his/her decision within a maximum of forty-eight hours. Further, according to Article 9A, paragraph 8, in circumstances where it is considered that delay may present a risk of violation of the confidentiality of private life, the access-blocking shall be carried out by the Presidency upon the direct instructions of the President.

58. The appeal against access-blocking decisions taken by a peace judgeship under Articles 8A, 9 and 9A, can be made, as in the procedure under Article 8, in places where there are several peace judgeships, to the peace judgeship bearing the next number. If there is only one peace judgeship in a given place, the appeal should then be made to the peace judgeship which is within the competence zone of the closest assize criminal court. The decision given by a peace judgeship in the appeal procedure is final and an appeal before a higher court is not possible, apart from the possibility to introduce an individual application before the Constitutional Court.

59. As mentioned above, the access-blocking decisions under Articles 8A, 9 and 9A are fundamentally different from the access-blocking measures provided for under Article 8. Under Article 8, the trial court judge in criminal procedure in the framework of which the access-blocking measure (as a precautionary or interim measure) is taken, is and should be competent to review the necessity of maintaining the precautionary measure on access-blocking and to lift this measure immediately if he/she considers that the measure is not necessary for the sake of the criminal procedure. This nature of the precautionary measure under Article 8 and the subsequent review by the trial court judge may justify the short terms within which the peace judgeship called to apply the precautionary measure on access-blocking should make his/her decision (24 hours) and also the lack of any separate appeal procedure before a higher court against the decision taken by the peace judgeship.

60. Instead, the procedures under Articles 8A, 9 and 9A, as they currently stand, do not require the institution of any civil or criminal procedures and the applicants who request access-blocking under Articles 9 and 9A, for instance, are not under an obligation to file a case under civil or criminal procedures against the content which is claimed to be harmful to their private life or personal rights. The procedures under Articles 8A, 9 and 9A do not concern an interim or precautionary measure taken in the framework of a pending criminal or civil procedure before domestic courts, but constitute independent procedures on "access-blocking". Therefore, there is no possibility of review of those decisions by a trial court as in Article 8. Under these circumstances, the short time allowed to the peace judgeship to take a decision on access-blocking (24 hours under Articles 8A and 9; 48 hours under Article 9A), without holding a hearing (Article 9) and without any possibility of appeal before a higher court against the

decision on access-blocking, cannot be considered as providing the necessary procedural guarantees in order to protect the right to freedom of expression on the Internet.

61. First, the Venice Commission is of the opinion that, as in Article 8, the procedures under Articles 8A, 9 and 9A should be made dependent on the institution of a criminal or civil procedure and the decision on access blocking under those procedures should only constitute a "precautionary measure" which can be taken in anticipation of the substantive criminal or civil proceedings when there is a reasonable suspicion of a violation of the law and the danger of an irreparable damage. The trial judge, in the subsequent criminal or civil proceedings, should be able to review the necessity of maintaining the precautionary measure on access-blocking and to lift this measure immediately if he/she considers that there are no elements supporting the reasonable suspicion or that the danger has been averted.

62. In case the current character of the procedures under Article 8A, 9 and 9A as autonomous procedures on access-blocking should be maintained, then the procedures should be amended profoundly in order to give the Internet provider sufficient time and facilities to defend itself and the judgeship sufficient time and possibilities to take a well-reasoned decision, and in particular the competence to hold a hearing in order to make an appropriate proportionality assessment on the necessity of the interference with the freedom of expression. A hearing would give the judge the opportunity to examine properly all the concrete circumstances of the case and to examine the points of view of the parties to set a fair balance between the freedom of expression and the rights of others.

63. More specifically, in case the autonomous character of those procedures should be maintained, an appeal before the Court of Cassation against the decision of access-blocking by the peace judgeship should then be available. It is true that, differently from Protocol No. 7 concerning criminal cases, Article 6 ECHR does not oblige States to institute a system of appeal courts and the right of appeal to a higher court is not laid down, and is also not implied, in Article 6.[42] However, as the Venice Commission emphasised in its Opinion on Articles 216, 299, 301 and 314 of the Penal Code of Turkey[43] the highest courts' guidance is very important for the lower courts in the interpretation and implementation of human rights standards in their case-law. It is evident that an appeal procedure before the Court of cassation, as the highest court, would provide for better guarantees to the interested parties compared to an appeal procedure before a same level judgeship. In this context, the Venice Commission recalls that it is of vital importance that the access-blocking measures, as well as any subsequent decision by the trial court not to lift them, should contain appropriate and detailed reasons.

64. Secondly, the removal of content from and the blocking of access to the Internet constitute restrictions of the right to freedom of expression that require a justification on any of the grounds and on the conditions listed in the second paragraph of Article 10 ECHR. According to this provision, any restriction must be prescribed by law and 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.

65. Paragraph 1 of Article 8A meets the first two sets of requirements in so far as it constitutes a legal basis for the removal and blocking measures, and lists more or less the same limitation grounds (i.e. legitimate aims for restrictions) as those enumerated in the relevant international legal provisions.

66. Nevertheless, the requirement that the restriction must be "necessary in a democratic society", *i.e.* the "interference" into the freedom of expression should correspond to a "pressing social need", and be proportionate to the legitimate aim pursued, and that the reasons given by

[42] Pieter van Dijk, *Right to a fair and public hearing (Article 6)* (Sections 1-4), in: P. van Dijk a.o. (eds) *Theory and Practice of the European Convention on Human Rights*, 4th ed., 2006, p. 564.
[43] CDL-AD(2016)002 Opinion on Articles 216, 299, 301 and 314 of the Penal Code of Turkey, para. 31.

the national authorities to justify it should be relevant and sufficient, is not mentioned in paragraph 1 of Article 8A. The Venice Commission takes note of and agrees with the concern of the authorities that the Internet can be used in particular by criminal organisations to pursue and facilitate their criminal activities. However, the fact that the interference pursues one or several of the legitimate aims for restriction stipulated in paragraph 1 of Article 8A is not sufficient (the justification is not automatic). In addition to those legitimate aims, the interference should also fulfil the requirements of "democratic necessity". In this respect, when applying blocking/removal measures, the competent authority (judgeship or the Presidency) should take into account the ECHR case-law concerning in particular the freedom of political speech[44], which requires a high level of protection of the right to freedom of expression and enables everyone to participate in the free political debate which is at the very core of the concept of a democratic society. It is recommended that a specific provision is included in Article 8A providing that the measure of restriction (blocking/removal) on any of the legitimate grounds listed in para. 1 of Article 8A should be "necessary in a democratic society" and proportionate.

67. Similarly, the blocking or removal measures following procedures under Articles 9 and 9A raise the issue of fair balance which should be struck between, on the one hand, the protection of freedom of expression (art. 10 ECHR), and, on the other hand, the protection of private life/personal rights, since, as the ECtHR stressed in *Delfi AS v. Estonia,* the rights under Article 10 and 8 ECHR deserve equal protection. This balancing exercise is at the core of the proportionality assessment which is a requirement of the criterion "democratic necessity" for the restriction of rights under the Convention. The ECtHR has laid down the relevant principles which must guide its assessment in this area. It has thus identified a number of criteria in the context of balancing the competing rights[45]: contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication etc. Consequently, the fact that the interference into the right to freedom of expression (blocking orders/removal of content) pursues the legitimate aim of protection of rights of others is not sufficient while, in addition to this legitimate aim, the interference should also fulfil the requirements of "democratic necessity", *i.e.* a fair balance should be struck between freedom of expression and the protection of private life/personal rights. Nevertheless, the requirement of "democratic necessity" and its components "fair balance" and "proportionality" are not mentioned in Articles 9 and 9A. It is recommended that a specific provision is included in those provisions providing that the measure of restriction (blocking/removal) should be "necessary in a democratic society" and proportionate.

68. This recommendation is *a fortiori* valid in the context of the procedures under Articles 8A and 9, since these provisions provide that a decision may be given for complete denial of access to the internet site under certain conditions. The ECtHR has held that Article 10 ECHR does not prohibit prior restraints on publication as such.[46] It has stressed, however, at the same time, that the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court.[47] The Court emphasised that this is especially so as far as the press is concerned, for news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest, but that this danger also applies to other publications that deal with a topical issue.[48] The foregoing means that the conditions for the justifiability of restrictions of the freedom of expression have to be interpreted and applied even more restrictively in cases where the restrictions have an undifferentiated (complete denial of access to the internet site) and a preventive character in blocking access to future information and communication. It is thus recommended to prescribe in Article 8A and 9, that the decision to block the whole web-site should be "proportionate" and supported with exceptionally strong arguments that the blocking measure does not cross the boundaries of what is strictly necessary in the specific concrete circumstances of each case. The existence in

[44] See, among many others, ECtHR *Incal v. Turkey*, Application No. 22678/93, 9 June 1998.
[45] See, ECtHR, *Axel Springer AG v. Germany* [GC], Application No. 39954/08, 7 February 2012, paras. 90-95.
[46] ECHR, *Ahmet Yıldırım v. Turkey*, para. 47.
[47] *Ibidem*, para. 47.
[48] *Ibidem.*

the law of alternative, less severe measures (see above) is essential to ensure respect of the proportionality requirement.

69. Thirdly, Articles 8A and 9A provide for an administrative measure of access-blocking by an administrative authority –the Presidency of Telecommunication-, without prior judicial review:

70. The first paragraph of Article 8A provides that "in circumstances where delay would entail risk", the decision on blocking/removal can be taken by the Presidency subsequent to the request of the Prime Minister's Office or the specific Ministry authorised. The decision shall be immediately notified to the access providers and relevant content and hosting providers, who shall implement the decision immediately within a maximum of four hours as from the notification of the decision. The decision on blocking/removal shall be submitted by the Presidency for approval by the peace judgeship in 24 hours. The judgeship shall announce his/her decision within 48 hours. The provision is not clear as to the circumstances in which the delay would present a risk and the delegation was not told during the meetings in Ankara on the basis of what criteria the Presidency decides in practice that the "risk" justifies the "emergency procedure" and thus the Presidency's competence to give blocking orders, instead of peace judgeships. In addition, it is not clear in Article 8A whether the peace judgeship that is called to approve or reject the decision taken by the Presidency is also competent to review whether the case presents an emergency or whether the delay would present a risk, and thus, whether the Presidency's competence to take the blocking/removal measure without prior judicial review is justified. Neither is it clear to the Venice Commission why a decision by a judge might cause a delay. In this case, in circumstances where delay would entail a risk, a court or a judge, instead of the Presidency, could take a blocking measure in an urgent procedure, and this decision should be reviewed by the trial court in the subsequent criminal proceedings (see, para. 60 of this Opinion). It is thus strongly recommended that the system of access-blocking by a decision of the Presidency without prior judicial review be reconsidered. If the competence of the Presidency for access-blocking is maintained, then the judge called to approve or reject the decision taken by the Presidency should also be competent to verify whether the case presents an emergency and whether the exercise of the competence of the Presidency in a given case was justified. In case the emergency procedure is deemed not to be justified, the measure of access-blocking taken by the Presidency should be removed immediately.

71. Under Article 9A (1), persons who assert that the confidentiality of their private life has been violated by a publication on the Internet may apply directly to the Presidency and request that access to that content be blocked. In this case, the Presidency shall immediately inform the Union of Access Providers in order to ensure that this request be implemented, and access providers shall carry out the request immediately, within a maximum of four hours (Article 9A(3)). Thus, the request is implemented in anticipation of a decision by a peace judgeship. It is not specified in this provision what grounds may justify an immediate blocking by an administrative body. Although the decision of the Presidency will be subject to judicial review by a judgeship, and even if the judgeship later on decides that there is no ground for blocking access to the internet information concerned, the original measure by the Presidency will have resulted in a serious interference with the right to freedom of expression. The urgency is not a valid argument in order to justify the competence of the Presidency in taking administrative blocking orders, because the emergency procedure is defined under para. 8 of Article 9A: "*in circumstances where it is considered that delay may present a risk of violation of the confidentiality of private life, the denial of access shall be carried out by the Presidency upon the direct instructions of the President*". Consequently, concerning the procedure under paras. 1 and 3 of Article 9A, there seems to be no reason for an administrative measure of access-blocking without prior judicial review. Leaving such a measure up to the discretion of the executive power presents a risk of arbitrariness. It is strongly recommended that the competence of the Presidency in this respect be repealed and the balancing of the right to privacy and the freedom of expression be entrusted to a judge and not to an administrative body.

72. Contrary to paragraph 3, the procedure under paragraph 8 of Article 9A is limited to "emergency cases", since for the competence of the Presidency to decide on a blocking order *ex officio* (i.e. upon the order of the President but without a request by a private individual being necessary) is restricted to cases where delay may present a risk of violation of the confidentiality of private life. However, the provision is not clear as to the circumstances in which the delay would present a risk which would justify the Presidency's competence for blocking orders. In addition, it is not clear why the Presidency should be competent to take *ex officio* decisions on access-blocking, given the fact that those individuals who assert that their right to privacy is violated as a result of a publication on the Internet, have the possibility, even in urgent cases, to file an application before domestic courts for the application of an access-blocking measure. In addition, the reason why the Presidency needs such emergency powers in cases where there is not even a claim by an individual as in paragraph 1, remains also unclear. The Venice Commission is of the opinion that the power of the Presidency to give *ex officio* blocking orders without prior judicial review should be removed and as stressed above, the duty to carry out the balancing between the right to privacy and the freedom of expression should, in the case of a decision with such serious consequences, be incumbent primarily on a judge and not on an administrative body.

73. Fourthly, Articles 9 and 9A do not provide for any notification procedure of the interested party about the procedures of access-blocking and do not give the interested parties the opportunity to have knowledge of the measure and of its reasons.[49] It is positive that, unlike Articles 9 and 9A, Article 8A provides for a notification procedure of the concerned content provider. However, according to Article 6A(7), decisions of access blocking outside the scope of Article 8 of the Law shall be sent to the Union of Access Providers for action and a notification made to the Union shall be deemed to have been made to access providers. The authorities claimed that the notification under Article 8A is not made to the Union, but the access providers are notified separately of the blocking orders. However, if this is the practice, the wording of Article 6A(7) should then be brought into conformity with it. The affected party should be urgently notified not only about the blocking/removal measure and its reasons, but also concerning the subsequent procedure before the peace judgeship to allow him/her to have reasonable opportunity to present evidence and arguments for the sake of the principle of fair trial.

74. According to Article 9(9) in its original wording, "*if the publication subject to a decision by a judge for blocking of access due to violation of personal rights within the scope of this article, or a publication of the same character, is also published in other internet sites, the existing decision shall also be applied to those other internet sites if an application is made by the person concerned to the Union*." By its decision of 8 December 2015, the Constitutional Court annulled the phrase "*or publications of the same character*". The Constitutional Court considered in this respect that "*[t]he competence to block access to publications of a similar character (…) does not meet the basic condition of the principle of legality that it should be comprehensible, clear and unambiguous, and moreover, its scope and boundaries are undefined. In its term "publications of the same character" the provision is not clear or foreseeable."* The Venice Commission welcomes this decision.

75. Finally, Articles 9(7) and 9A(7) provide that, if the blocked content is removed from publication, the judge's decision becomes automatically invalid. The meaning and the purpose of those provisions remain unclear to the Venice Commission. Under Article 9, for instance, a decision by a peace judgeship to block access is sent by the Union of Access Providers to the access provider concerned who shall implement the decision immediately, within a maximum of four hours (para. 8). The failure to implement this decision is punished by a criminal fine (para. 10). However, it results from paragraph 7 that the implementation of the decision of the peace

[49] It is true that, under Article 9, the complainant has the possibility to request from the content provider or hosting provider the removal of the relevant content before applying to a peace judgeship, in which case the content or hosting provider will be aware that in case of a refusal of the request, the procedure before the peace judgeship may be initiated. However, this is not an obligation for the complainant who can directly apply to the peace judgeship without requesting from the providers the removal of the content.

judgeship results in the invalidation of the latter. It is thus highly unclear whether the judge's decision can even be appealed against after it has become, according to para. 7, null and void, *i.e.* legally inexistent. If what is meant under those provisions is that the voluntary removal of the content *before a decision is taken by the judge,* results in the invalidation of the procedure, this should be more clearly phrased under those provisions.

B. Other issues

1. Obligations of content providers, hosting providers and access providers to provide the authorities with any information they request (Articles 4(3), 5(5) and 6(1)d)

76. These provisions put the content provider, hosting provider and access provider respectively, under an obligation to furnish to the Presidency of Telecommunications such information as it may demand. The content provider, the hosting provider and the access provider, according to those provisions, should also implement the measures as may be directed by the Presidency. Although the scope is somewhat delimitated by the words in Article 4(3) "*within the scope of performance by the Presidency of functions delegated to it"*, it is obvious that this obligation implies that the providers may have to submit all kinds of personal data of Internet users without the persons or organisations concerned being aware of that flow of information. Besides, Articles 5(5) and 6(1)d concerning respectively the obligations of hosting providers and access providers do not delimitate the scope of information as in Article 4(3). The Presidency of Telecommunication is able to request information without a court decision or any other justification.

77. The 2013 Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression emphasises that States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon the one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists and human rights defenders, in particular, cannot be assured that their communications will not be subject to States' scrutiny.[50]

78. The obligation imposed on access, content and hosting providers in the above mentioned provisions is a very far-going intrusion upon the right to protection of privacy of the Internet users under Article 8 ECHR which would require a clear delimitation as to the grounds for such a request by the Presidency, its "necessity in a democratic society" and its proportionality.

79. The Constitutional Court held in its judgment of 8 December 2015 that the above provisions must be annulled as they were in violation of Articles 2 (Rule of Law), 13 (Restriction of fundamental rights) and 20 (Right to Privacy) of the Constitution. The Court underlined in its judgment that the Rule of Law enshrined in Article 2 of the Constitution entails the principle of "clarity" which requires that legal arrangements must be clear, unambiguous, comprehensible and applicable so as to give neither individuals nor the administration any cause for doubt or hesitation, and they must also include safeguards against arbitrary behaviour by public authorities.[51] The Constitutional Court held that any restriction of confidentiality and protection of private life must meet the test of proportionality laid down in Article 13 of the Turkish Constitution. It held that the challenged provisions permitted all kinds of personal data, information and documents belonging to individuals to be transferred to the Presidency unconditionally, without adequate limits in terms of subject, purpose and scope and thereby

[50] United Nations General Assembly, A/HR/C/23/40 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, para. 79. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[51] Judgment of 8 December 2015, No. 2014/84E, 2015/112K, para. 88.

render such individuals undefended against the administration. Consequently, the Constitutional Court held that the challenged provisions, because they were not clear and foreseeable, unreasonably limited individuals' rights to protection of personal data and constituted a violation of Article 20 of the Constitution.[52]

80. The Venice Commission welcomes this decision of the Constitutional Court. In addition, it also recommends that access to retained data should be granted only on the basis of a warrant issued by a court and, except in the context of the investigation of serious crimes, the targeted persons should be informed of the flow of information and be given the possibility to challenge the measure before a court. Furthermore, Article 6(1)c *in fine,* which provides that "the access providers shall furnish to the administration the traffic information of the users at least three months prior to termination of their activities" should be amended in the light of the above observations. Such a blanket revealing obligation cannot fulfil the ECtHR's three steps test. The provision should either be redrafted or repealed.

2. Obligations by hosting providers and access providers to retain traffic information (Articles 5(3) and 6(1)b)

81. According to those provisions, hosting providers are required to retain traffic data (communications data) in relation to their hosting activities from one to two years (Article 5(3)) and access providers for a period of not less than six months and not more than two years.

82. In April 2014, the Grand Chamber of the European Court of Justice declared the Directive 2006/24/EC (the Data Retention Directive) invalid on the ground that European Union legislators concerned had exceeded the limits of proportionality in forging the Directive.[53] The Directive provided for similar obligations to keep traffic data available, specifically for the purposes of fighting against serious crimes, for a period of at least six but not more than 24 months.[54] In particular, the Court held that the Directive entailed a serious interference with the rights to privacy and personal data protection of individuals guaranteed by the Charter of Fundamental Rights, and also failed to establish limits on access by competent national authorities, such as prior review by a judicial or an independent administrative authority. Although that judgment is not binding on Turkey, not even as a candidate State to the European Union, it may give guidance in the assessment of the provisions in question.

83. The United Nations High Commissioner for Human Rights, in a report of 30 June 2014 on the right to privacy in the digital age, underscored that, in addition to the right to privacy, the rights to freedom of opinion and expression and to seek, receive and impart information and the right to freedom of peaceful assembly and association may also be affected by mass surveillance, the interception of digital communications and the collection of personal data. In addition, the UN Human Rights Committee has issued some specific recommendations regarding the standards for data surveillance, retention and use under the right to freedom of expression and to privacy.[55]

84. The Turkish Constitutional Court, when finding that Article 5(3) was not in breach of the Constitution, rightly considered that to retain traffic information may be necessary "*to prevent loss of information that is important and necessary in order to combat offences committed over the Internet and in order to identify perpetrators*".[56] The use of electronic communications is a valuable tool in the prevention of offences and the fight against crime, in particular organised crime. Consequently, retention of data may evidently pursue an objective of general interest.

[52] Judgment of 8 December 2015, No. 2014/84E, 2015/112K, para. 170.
[53] ECJ, Grand Chamber, Case no C-293/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources.
[54] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105 (*invalidated*).
[55] See, for instance, Human Rights Committee, *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland* (CCPR/C/GBR/7), para. 24.
[56] Judgment of 8 December 2015, No. 2014/84E, 2015/112K, para. 177.

However, derogations to the protection of personal data must be "necessary" and the domestic legislation must provide for clear rules concerning the limited scope and application of the measure and impose safeguards in order to protect personal data against the risk of abuse and against any unlawful access and use of that data.[57]

85. Although the legitimate aim of the provisions is the fight against crime, they are applied to all internet users without any differentiation being made in the light of this objective, *i.e.* they are not limited to a circle of persons about whom there are suspicions concerning their involvement in the commission of serious crimes and any other persons whose data retention may contribute to the investigation of serious crimes. Also, the data retention measure under those Articles covers a whole period between a lower and an upper limit indicated in the provisions and is not limited to a particular time period between the lower and upper limits, where there are suspicions concerning the commission of serious crimes. There must be some objective criteria to determine the period of retention in order to ensure that it is limited to what is strictly necessary. Further, the provisions do not limit the measure in its material scope: the measure is not limited to a list of serious crimes, as organised crime, terrorism or paedophilia and do not provide for a threshold for the seriousness of crimes concerning the use of data as elaborated above.

86. As the Constitutional Court annulled, by its decision of 8 December 2015, the above mentioned Articles 4(3), 5(5) and 6(1)d concerning the obligation of hosting and access providers to furnish to the Presidency any information it requests (concerning thus the issue of access to retained data), the authorities will have to prepare new provisions to replace those annulled by the Court. It is recommended that the issue of data retention and that of access to retained data be dealt with under one and the same provision providing guarantees for both procedures.

3. Union of Access Providers (Article 6A)

87. Under Article 6A(10), Internet service providers which are not members of the Union of Access providers, may not operate. The Union of Access Providers was established for the only purpose of implementing decisions to block access outside the scope of Article 8 (para 1). It is a legal entity under civil law (para. 2), but according to paragraph 3, its Charter shall be approved by the Telecommunications Authority and amendments of the Charter shall be subject to its approval. The Union has the right to object to decisions sent to it which it considers not in conformity with legislation (para. 8).

88. In its judgment of 8 December 2015, the Constitutional Court considered that the Union was established to eliminate lack of clarity concerning the identity of the respondent parties (access providers) in the framework of the implementation of decisions to block access, and to ensure that the decisions be implemented promptly. The Court further considered that compulsory membership of the Union for the access providers to ensure that court decisions be implemented promptly is a consequence of the positive obligations of the State, and in no way offers any harm to individuals' right to free enterprise.[58]

89. The Union is not an association in the sense of an organised, independent, not-for-profit body based on the voluntary grouping of persons with the common interest, activity or purpose.[59] As mentioned above, its only purpose is to implement decisions to block access. The compulsory membership is not justified by its being a professional organisation with the character of public institution in the sense of Article 135 of the Constitution, as was also observed by the Constitutional Court in its judgment of 8 December 2015. But the Union has a public function *i.e.* the implementation of decisions by a public authority, and the effective

[57] See, *mutatis mutandis, S. and Marper v. the United Kingdom*, para. 99.
[58] Judgment of 8 December 2015, No. 2014/84E, 2015/112K, para. 92.
[59] OSCE/Venice Commission, Guidelines on Freedom of Association, 2015, p. 5.

exercise of that function is considered as requiring full obligatory membership of the access providers.

90. On the other hand, the compulsory membership of the Union for the access providers may also be seen as a "license" in order for the access providers to operate. In the case of *Informationsverein Lentia and others v. Austria*, the ECtHR considered that "*this Article* [Article 10] *shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. The Court has stated that the purpose of the third sentence is to permit the States to regulate by a licensing system the way in which broadcasting is organized in their territories, particularly in its technical aspects."*[60]

91. In the case of *Groppera Radio AG and others v. Switzerland,* the Court held that the power of the domestic authorities to regulate the licensing system may not be exercised for other than technical purposes and not in a way which interferes with freedom of expression contrary to the requirements of the second paragraph of Article 10.

92. As mentioned above, the only function of the Union is the dissemination of access-blocking orders to its members (currently 66 access providers). The delegation was informed during the meetings in Ankara that all the access-blocking orders and notifications are also communicated to the members of the Union, either by e-mail or via the *National Informatics Network*. The question is whether the mere provision of information to access providers about an access-blocking decision may be considered to have sufficient "technical aspects" justifying a compulsory membership to the Union, having regard to the aforementioned requirements of Article 10, para. 2, ECHR. The Constitutional Court explained in its judgment of 8 December 2015 that the number of access providers increases every day and that it is difficult to keep track of them (para. 103). However, it seems that as of today, there are only 66 of them. Keeping track of the access providers may be possible through a simple registration system. The Commission believes that in order to be in conformity with the democratic necessity and proportionality requirements of Article 10, para. 2, the compulsory membership under Article 6A(10) should be justified with further technical reasons, having also in mind that clauses which allow interference with Convention rights must be interpreted restrictively.[61]

93. Furthermore, Article 6A(8) foresees a right of appeal for the Union, but is silent on the right of appeal of individual members. This seems to indicate that the Union is the only legal entity that may appeal decisions forwarded to it. According to the explanations given by the representatives of the authorities in Turkey, the members have the right to challenge decisions for blocking of access. However, this should be clearly set forth in the Law.

94. Article 6(1)ç imposes the obligation on the access providers to take measures to prevent "alternative methods of access" to publications in whose respect an access-blocking decision has been given. The Venice Commission is of the opinion that this obligation of the access providers should be further clarified and circumscribed. The obligation appears disproportionate in the absence of further explanation as to which alternative methods should be prevented, by which means and in what circumstances.

4. Public use providers (Article 7)

95. The public use providers are those who provide individuals with the possibility of using the internet in a certain location and for a certain period of time (Article 2(1)i).

96. Article 7(2) provides that public use providers, irrespective of whether or not they are operating commercially, must implement the measures specified in regulations concerning blocking access to unlawful content and maintaining access data. Thus, it appears that public

[60] ECtHR, *Informationsverein Lentia and Others v. Austria*, Application Nos 13914/88; 15041/89; 15717/89; 15779/89; 17207/90.
[61] ECtHR, *Stoll v. Switzerland*, Application No.69698/01, para. 61.

use providers are obliged to investigate and monitor on their own initiative, information accessed, and to maintain access data related to the use. Furthermore, commercial internet public use providers must, on their own initiative, take measures, procedures and principles of which are set out in the regulations, with a view to protecting the family, children, preventing offences and detecting offenders.

97. The Venice Commission does not have at its disposal the regulations mentioned in these provisions. However, it reminds that according to the Declaration of the Committee of Ministers of the Council of Europe on Freedom of Communication on the Internet, *"[m]ember states should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity"*. [62] In case the regulations mentioned in these provisions impose such a general monitoring obligation, this would not be a proportionate burden on the public use providers in the light of the standards set forth in the above-mentioned Declaration of the Committee of Ministers.

VI. Conclusion

98. The Internet has become one of the principle means of exercising the right to receive and impart information and ideas "regardless of frontiers". Its specific nature as a "modern means of imparting information" is taken into account by the European Court of Human Rights, which interprets the Convention "in the light of present day conditions". The Committee of Ministers of the Council of Europe, in its recent Recommendation Rec(2016)5 also reiterated that all the Member States have both negative and positive obligations to respect, protect and promote human rights and fundamental freedoms on the Internet and, moreover, to create an enabling environment for Internet freedom. The Venice Commission underlines also the responsibility of global/international Internet actors or companies (hosting and content providers) to cooperate with the States in particular in the context of the fight against terrorism and child abuse and to implement domestic court decisions restricting the Internet freedoms where those restrictions pursue a legitimate aim and are necessary and proportionate.

99. Law No. 5651 on the Internet aims at fighting offences committed by misuse of opportunities provided by the Internet and at taking necessary preventive measures against the broadcast promoting harmful content, as the use of drugs, sexual exploitation of children etc. The amendments introduced in 2014 brought certain positive changes to the Law as the obligation imposed on judges and the Presidency of Telecommunication to consider primarily the issue of blocking decisions in respect of a specific publication (in the form of URL etc.) before issuing a blocking order on an entire website under a number of conditions. However, in an overall assessment those amendments and the amendment introduced in March 2015 have resulted in the increase of the powers of the Presidency of Telecommunication to issue blocking orders without prior judicial review and of the number of alternative procedures for access-blocking/removal of content on different grounds.

100. Under one of the four access-blocking procedures in Law No. 5651 (the procedure under Article 8), the measure of access-blocking appears as a "precautionary measure" or an "interlocutory measure", taken in the framework of criminal proceedings concerning the crimes listed in this provision. As opposed to Article 8, the "access-blocking" decisions taken in the context of Articles 8A, 9 and 9A are not "precautionary measures" in order for instance to prevent the risk of irreparable damages pending the substantive trial, but constitute fully-fledged, autonomous procedures through which substantive decisions on "access-blocking" are taken. In the formulation of the following recommendations, this fundamental difference between the procedure under Article 8 and the procedures under Articles 8A, 9 and 9A is taken into account.

---

[62] See principle 6 in the Council of Europe Committee of Ministers Decl-28.05.2003E, *Declaration on freedom of Communication on the Internet*, adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies.

101. The objectives of access-blocking measures indicated in the Law, such as the prevention of crime and the protection of personal rights or privacy, are covered by several legitimate aims for restrictions listed in the second paragraph of Article 10 ECHR. However, the provisions do not mention, explicitly or implicitly, the obligation of the judge to make also a proportionality assessment in order to set a fair balance between competing rights. The Law lacks a list of less intrusive measures than access-blocking and does not leave the judge any room for a lower sanction in specific circumstances following a proportionality assessment.

102. The possibility for the Presidency of Telecommunications to take access-blocking measures without prior judicial review is also problematic.

103. In order for Law No. 5651 to meet the applicable European standards, the Venice Commission formulates the following main recommendations (in addition to other recommendations contained in the text of the opinion):

- the procedures on access-blocking under Articles 8A, 9 and 9A should, as in the procedure under Article 8, be made dependent on the institution of a criminal or civil procedure, and the decision on access blocking under those procedures should only constitute a "precautionary measure" which can be taken in the framework of substantive criminal or civil proceedings;

- Concerning all the four procedures on access blocking, the trial judge, in the subsequent criminal or civil proceedings, should be able to review the necessity and proportionality of maintaining the precautionary measure on access-blocking and to remove this measure immediately if he/she considers that the measure is not proportionate and necessary in the light of the criminal/civil procedure. Decisions to maintain the access-blocking measure should be duly motivated;

- In case the procedures under Articles 8A, 9 and 9A should be maintained as fully-fledged, autonomous procedures through which substantive decisions on "access-blocking" are taken, then appropriate procedural guarantees should be provided under these procedures: the judge should be given sufficient time to make a thorough and reasoned proportionality and necessity assessment of the interference with the 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 the four 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 the

freedom of expression and the legitimate aims pursued by the measure, should be carried out by a court and not by an administrative body.

104. The Venice Commission remains at the disposal of the Turkish authorities for any further assistance they may need.