

# **Evaluating the Regulation of Access to Online Content in Turkey in the Context of Freedom of Speech**

**Batu Kinikoglu**

VU University Amsterdam  
Senior Counsel – BTS & Partners  
[batu.kinikoglu@bts-legal.com](mailto:batu.kinikoglu@bts-legal.com)

**Abstract:** This paper aims to critically examine internet access regime in Turkey within the framework of freedom of speech set by international human rights agreements. The enactment of the Law No. 5651 in 2007 led to strict regulation over access to online content. The current situation in Turkey is marked by a general blocking mechanism, a non-transparent filtering mechanism and significant role ascribed to administrative bodies in blocking and filtering decisions. By tracing internet access regime in Turkey historically and discussing the general relationship between internet access regulation and international human rights agreements, the paper addresses the ways in which the internet access regime in Turkey violates the right to freedom of speech. In the light of this assessment, the paper concludes with nine-steps that can be taken to meet the requirements of international human rights agreements.

## **1. Introduction**

There are over 20.000 blocked websites in Turkey, over 4.000 of which have been blocked in 2012.<sup>1</sup> These numbers constitute a mirror image of the internet access regime in Turkey, which has caused a series of protests in the Turkish society. On 17<sup>th</sup> of July 2010, thousands marched against the blocking mechanism designated in Law numbered 5651 on the Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications (Law No. 5651), i.e. the first Law regulating internet access in Turkey.<sup>2</sup> Likewise, simultaneous protest marches in 31 cities of Turkey took place on 15<sup>th</sup> of May 2011, just after the Information Technologies and Communications Authority (ITCA) of Turkey announced the new filtering mechanism.<sup>3</sup>

The contemporary situation in Turkey raises concerns that Turkey's internet access regime diverts from the basic principles of the international human rights agreements that Turkey is a party of, especially the Universal Declaration of Human Rights (UDHR), and the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights; ECHR). These concerns are not groundless. The two mechanisms used in Turkey, the blocking and the filtering mechanisms, are intervening in the right to the freedom of speech of individuals. The general blocking regime in Turkey results in a massive amount of over-blocking, while both blocking and filtering mechanisms fail to be transparent and responsive to the public. More than that, the content of the websites that are filtered or blocked and the heightened role of the administrative bodies in decisions regarding what is to be blocked or filtered is equally problematic.

It is at this time of unrest that this paper aims to offer an evaluation of the current regulation of access to online content in Turkey in the context of freedom of speech. This assessment entails a description of

---

<sup>1</sup> According to unofficial statistics of EngelliWeb, a voluntary project in Turkey that lists blocked websites in Turkey. For more information, please see, <http://engelliweb.com/istatistikler/> (in Turkish).

<sup>2</sup> "Sansure Karsi Yuruyus" ("March against Censorship"). For more information, please see, <http://www.sansuresansur.org/> (in Turkish).

<sup>3</sup> <http://www.sansuresansur.org/internetin-icin-yuru/> (in Turkish).

the internet access regulation in Turkey with a historical perspective; a discussion of the general relationship between internet access regulation and the human rights regime; and an analysis of the contemporary regime in Turkey in the light of the freedom of speech regime. In due course, the paper is divided into three main sections. The first section will give a historical account of the internet access regime in Turkey before and after Law No. 5651. The second part will offer a wider discussion on internet access regulation and the freedom of speech regime designated in the international human rights agreements. In the most comprehensive last chapter, the Turkish case will be situated in the international human rights arena through an analysis of whether Turkey respects the international human rights agreements and what should Turkey change in order to respect these agreements.

## **2. Regulation of Access to Online Content in Turkey**

### **2.1 Attempts to Regulate the Internet and Blocking of Websites before Law No. 5651**

Before Law No. 5651 was enacted in 2007, there was no specific law governing internet access in Turkey. Yet, the attempts to regulate the internet in Turkey date back to 2001. At that time, it was thought that the already-existing laws, such as the Turkish Criminal Law and the Press Law, could be used for regulating access to online content and the crimes committed on the internet.<sup>4</sup> The reason behind this approach could be that the internet was not regarded as a distinct aspect of social life in Turkey. Instead, it was considered as a branch and a continuation of the traditional mass media, which could be governed by already-existing regulatory mechanisms.

Using existing laws for internet-related crimes inevitably had unfortunate consequences especially in terms of criminal law. For example, in 1999, Coskun Ak, a forum moderator working for an internet service provider called Superonline, was sued for a forum message posted by an anonymous user. This message allegedly insulted the Turkish Republic, the military, the police, and the courts of law.<sup>5</sup> In the criminal charges against Ak,<sup>6</sup> the public prosecutor admitted that there is no regulation for the crimes committed on the internet. Nevertheless, he stated that Ak's position was similar to an editor of a newspaper, which made him responsible for what the anonymous user had posted on the forum. In the case, the court sentenced Ak to 40 months of prison for the alleged insults.<sup>7</sup> Needless to say, this decision was against one of the basic principles of criminal law in continental Europe, *nullum crimen nulla poena sine lege*, i.e. there can be no crime or punishment without law. Fortunately, after a series of trials in the High Criminal Court, the Supreme Court, and the Plenary of Criminal Chambers of the Supreme Court, Ak was found to be innocent. However, his innocence was not based on the fact that there was no legislation covering his position as an internet forum moderator, but based on the fact that what was written on the forum was found to be within the scope of freedom of speech. Fortunately, the case did not end up with an unfortunate conviction and the decision was given with reference to freedom of speech. Yet, the *Coskun Ak* case signifies two important points. First, the importance of defining the actors on the internet (e.g. content provider and hosting provider) became visible. Second, it indicated how dangerous it might be to apply the existing non-internet related laws to crimes committed on the internet. This case was one of the first, signifying the need to regulate the internet.

At first, there were several attempts to regulate the crimes committed on the internet by simply adding specific provisions to the existing laws. In 2002, a provision has been added to the Press Law, which stated that provisions in this Law about compensations arising from insults are applicable to insults made on the internet.<sup>8</sup> Yet later it became apparent that the internet differs from the traditional press in many ways including diversified positions and new actors which cannot be found in conventional mass media. Since the Press Law did not define the internet and its actors, this provision about the internet could not

---

<sup>4</sup> Y Akdeniz and K Altinparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), p.3.

<sup>5</sup> For more information on the case, please see, B Gunaydin, *Internet Yayinciligi ve Ifade Ozgurlugu* (2010), pp.139-153.

<sup>6</sup> Istanbul Chief Public Prosecutor's Office, Press Bureau, Main No.1999/280, Accusation No.1999/348, dated 28.07.1999.

<sup>7</sup> Istanbul 4<sup>th</sup> High Criminal Court, Main No.1999/225, Decision No.2001/56, dated 27.03.2001.

<sup>8</sup> Press Law numbered 5680, Additional Art. 9.

become functional and later the Law was abolished.<sup>9</sup> The existing laws not only tried to be used for regulating crimes committed on the internet. There was also an attempt to apply them in the regulation of the methods of internet publications. In 2002, Article 31 of the Law about the Radio and Television Supreme Council of Turkey (RTSC) was changed. Accordingly, it was designated that the methods and principles of internet publications were to be determined by the RTSC.<sup>10</sup> Although this provision remained in force until the Law was changed in 2011, the RTSC never tried to regulate internet publications.<sup>11</sup>

Another attempt to use existing laws became visible in decisions regarding blocking access to websites. In the early 2000s, hundreds of websites were blocked in accordance with the existing, but non-internet related laws, mostly because the content on the websites was found to infringe copyright or found to be threatening the unity and integrity of the Turkish Republic. For example, in 2005, Istanbul 3<sup>rd</sup> Criminal Court of Peace blocked access to 14 websites (including [www.downloadarsivi.com](http://www.downloadarsivi.com), [www.turkmaster.com](http://www.turkmaster.com), [www.araindir.com](http://www.araindir.com), [www.muziksitesi.net](http://www.muziksitesi.net)) for copyright infringement.<sup>12</sup> Apart from that, Ankara 11<sup>th</sup> Criminal Court of First Instance decided on 21.05.2003 to block access to [www.ozgurpolitika.org](http://www.ozgurpolitika.org) for an infringement of the (now abrogated) Turkish Criminal Law Article 159 (which regulates insulting Turkishness, the Parliament, the Government, Ministries, Armed Forces, Police Forces and the Judiciary).<sup>13</sup> As these examples suggest, there were “blocking orders issued by courts and enforced by the then dial up ISPs”<sup>14</sup>, before Law No. 5651.

This brief historical account lends itself to the establishment of Law No. 5651 and shows that the kind of mentality, which governed the conventional press repressively, tried to govern the internet in the same repressive way by simply using or adapting the existing laws.<sup>15</sup> However, it became apparent that the traditional administrative and criminal measures were insufficient to fight crimes committed on the internet, and that a new law was needed for an “effective and right reorganization to fight with the crimes committed via the abuse of the opportunities that the electronic communication means, including the internet, provide”.<sup>16</sup>

## 2.2 Law No. 5651 as a Blocking Mechanism

Blocking of websites was a common practice even before Law No. 5651; however, it did not raise much political concern or public awareness before the enactment of the Law. The parliamentary discussions about the Law were limited to negotiations on the kinds of information on the internet that should be blocked, rather than questioning whether blocking access to websites is an appropriate mechanism to fight crimes committed on the internet. In fact, some MPs from the Republican People’s Party (RPP), the main opposition party during the parliamentary discussion, requested the extension of the scope of the Law. They simply wanted to include the crime of “breach of national unity and territorial integrity” of the Turkish Republic so that websites hosting such criminal content could also be blocked.<sup>17</sup> The narrow scope of the parliamentary discussions led to quick enactment. The Law No. 5651, prepared by the Turkish Ministry of Transportation, was sent to the Parliament by the Ministry in January 2007; the Justice Commission of the Parliament prepared a report about the draft bill in April; and, the Law was discussed and accepted by the Parliament in May 2007.<sup>18</sup> Consequences of the blocking regime became visible only after the Law was passed, which in return created an opposition block consisting of both the

<sup>9</sup> B Gunaydin, *Internet Yayinciligi ve Ifade Ozgurlugu* (2010), pp.98,99.

<sup>10</sup> Law on the Establishment and Broadcasts of Radios and Televisions numbered 3984, Art. 31.

<sup>11</sup> B Gunaydin, *Internet Yayinciligi ve Ifade Ozgurlugu* (2010), p.103.

<sup>12</sup> Istanbul 3<sup>rd</sup> Criminal Court of Peace, Decision No. 2005/1870.

<sup>13</sup> Ankara 11<sup>th</sup> Criminal Court of First Instance, Decision No. 2004/31.

<sup>14</sup> Y Akdeniz and K Altinparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), p.6.

<sup>15</sup> Isil Karakas, European Court of Human Rights Judge has stated that “Turkey is the most convicted country in the European Court of Human Rights for freedom of speech and freedom of press”. See, <http://www.ntvmsnbc.com/id/25300906/> (in Turkish). More than that, in general, Turkey had the “highest number of violations of the European Convention on Human Rights in 2011, the third year in a row”. See, [http://www.todayszaman.com/newsDetail\\_getNewsById.action?newsId=269732](http://www.todayszaman.com/newsDetail_getNewsById.action?newsId=269732).

<sup>16</sup> Official Legislative Intention of Law No. 5651.

<sup>17</sup> Turkish Grand National Assembly, Journal of Minutes, vol.156, session dated 04.05.2007, available at <http://www.tbmm.gov.tr/tutanak/donem22/yil5/bas/b099m.htm> (in Turkish).

<sup>18</sup> Y Akdeniz and K Altinparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), pp.9-12.

public and some of the MPs. Major campaigns and demonstrations for internet freedom started to flourish in major cities of Turkey, while the RPP started to claim that that Law No. 5651 constitutes censorship.<sup>19</sup>

The enactment of the Law was justified upon two articles of the Turkish Constitution, Article 41 and Article 58, in the legislative intention of the Law. Article 41 of the Turkish Constitution, entitled “Protection of the Family”, states that;

*“The family is the foundation of the Turkish society...The state shall take the necessary measures and establish the necessary organisation to ensure the peace and welfare of the family...”*

In addition, Article 58 of the Constitution, entitled “Protection of the Youth”, states that;

*“The state shall take measures to ensure the training and development of the youth...The state shall take necessary measures to protect the youth from addiction to alcohol, drug addiction, crime, gambling, and similar vices, and ignorance.”*

In short, Law No. 5651 was passed to protect the family and the youth from the crimes committed on the internet. In the words of the official legislative intention, the Law “*aims to prevent crimes to be easily committed, by the use of emerging technologies, towards certain social groups, especially the family, children, and the youth, for which the Constitution provides special protection*”<sup>20</sup>. The Minister of Transportation, Binali Yıldırım, also indicated that the Law would “*prevent crimes to be committed to our children, youth and family structure by the use of the Internet. Articles 41 and 58 of the [Turkish] Constitution give us a duty to fight [with these crimes]*”<sup>21</sup>. Here, it is interesting to note that the justification of Law No. 5651 clearly diverts from the earlier attempts to rationalise the regulation of the internet and the blocking of access to websites. Whereas before this Law, the discussions revolved around “threatening the unity and integrity of the Turkish Republic”, with the new Law No. 5651 the debates started to be firmly centred on the protection of the family, youth and children.

Although Law No. 5651 stemmed from an urgency to guard the institution of the family, for the first time it introduced a general framework for blocking access to websites. Law No. 5651 can be distinguished in three aspects: (1) the definition provisions where it defines internet actors like the content providers, hosting providers, and mass-use providers (such as internet cafes); (2) the administrative provisions where the Law designates the roles and obligations of the internet actors and the Telecommunications Communication Presidency (TCP); (3) the well-known Article 8 about blocking access to websites as well as the less-known Article 9 about private law disputes, where the right of content removal and right of reply are designated.

### **2.3 Article 8 and Blocking Access to Websites**

Article 8 of the Law, entitled “Blocking Access Decisions and Executions of Such Decision” designates the blocking regime. The provision starts by stating that “[a]ccess to a broadcast on the Internet may be blocked if there is sufficient suspicion that the content constitutes one of the crimes mentioned below herein”<sup>22</sup> and goes on to designate the crimes for which a website may be blocked. These crimes are: (1) provocation for committing suicide (2) sexual harassment of children (3) easing the usage of drugs (4) supplying drugs which are dangerous for health (5) obscenity (6) prostitution (7) providing place and opportunity for gambling, and (8) crimes mentioned in the Law on Crimes against Atatürk (the founder of the Turkish Republic).<sup>23</sup> After listing these crimes, the provision goes on to delineate how blocking decisions are to be given and executed. Accordingly, blocking decision shall be granted by a judge during

---

<sup>19</sup> For more information, please see, <http://www.chp.org.tr/?p=60839> (in Turkish); <http://www.chp.org.tr/?p=25120> (in Turkish).

<sup>20</sup> Official Legislative Intention of Law No. 5651.

<sup>21</sup> Turkish Grand National Assembly, Journal of Minutes, vol.156, session dated 04.05.2007, available at <http://www.tbmm.gov.tr/tutanak/donem22/yil5/bas/b099m.htm> (in Turkish). It is also interesting to note that years after, in 2011, the Minister gave the same justification about the State’s duty to protect the children and the youth for the enactment of the nation-wide internet filter. For more information on this issue, please see, <http://ekonomi.haberturk.com/teknoloji/haber/631128-internette-yasak-falan-yok> (in Turkish), and <http://www.ntvmsnbc.com/id/25299546/> (in Turkish).

<sup>22</sup> Law No. 5651, Art. 8(1).

<sup>23</sup> Law No. 5651, Art. 8(1)(a) and 8(1)(b).

the investigation period and by a court during the prosecution period. Public prosecutors can also grant blocking decisions during the investigation period however, they have to submit the decision to a judge for approval within 24 hours, and the judge should give a decision within the following 24 hours.<sup>24</sup> Yet, it is not only the courts, judges or public prosecutors who can grant blocking decisions. If the content provider or the hosting provider resides outside Turkey, then the TCP can block access to websites, for which there is “sufficient suspicion” that one of the listed crimes are committed on a website, without a need for a court, judge or public prosecutor order.<sup>25</sup> In addition, for the crimes of sexual harassment of children and obscenity, the TCP can block access to websites, even if the content and hosting providers of the website reside in Turkey.<sup>26</sup> The blocking decisions are sent by the TCP to internet service providers (ISPs) for execution. These decisions should be executed by the relevant provider within 24 hours of the receipt of the order.<sup>27</sup> The Law states that if the blocking decisions are not executed by the provider, then the responsible people will be punished with imprisonment from six months up to two years, provided that the crime does not necessitate a heavier penalty.<sup>28</sup>

Despite this detailed account provided in Article 8, there is still one major point of uncertainty. It is stated in Article 8 that the blocking decisions are “protective precautions” and not final decisions. Therefore, interested parties may object to the decision in accordance with the Criminal Procedure Law numbered 5271.<sup>29</sup> However, the Law does not mention clearly who exactly can object to the blocking decisions. It is not apparent whether people, who are trying to “receive” information, and therefore whose freedom of speech is also affected by the decision, can or cannot object to blocking decisions.

### 3. Telecommunications Communication Presidency

Law No. 5651 also assigns the TCP obligations and duties in regulating internet access. The TCP was established in 2005, before Law No. 5651, under the umbrella of the ITCA, a governmental institution. Before the enactment of Law No. 5651, the TCP was responsible for the surveillance and interception of communications in Turkey. With Law No. 5651, it has also become responsible for internet content and blocking decisions.<sup>30</sup> In accordance with the Law, all blocking decisions given by the courts, judges and public prosecutors are sent to the TCP. The TCP, then, sends the decisions to relevant ISPs for execution.<sup>31</sup> Thus, it is plausible to suggest that the TCP has become an intermediary and regulatory institution of the government in regulating all kinds of telecommunications including the internet.

#### 3.1 The Filtering Mechanism

Blocking mechanism is not the only method used in Turkey to “protect” the family, youth and children from the “harms” of the internet. The filtering mechanism called the “safer internet service”, designed by the ITCA, came into force in November 2011. With the safer internet service, two ISP-level, state-controlled, and voluntary filters have been introduced; the “child profile” and the “family profile”. Whereas the first allows access to only certain websites enlisted on a whitelist, the second profile restricts access to websites enlisted on a blacklist. The whitelist and the blacklist, designated by the ITCA, are sent to ISPs so that they can execute an ISP-level filtering.

These profiles have been introduced as voluntary filters; however, there are issues about the process raising concerns. In the first place, the whitelist and the blacklist, which are prepared by the ITCA, are not made available to the public. In contrast with private home filtering software, parents do not know exactly which websites are restricted or accessible in each profile. There is only the option to check each website individually on the “safer internet” website of the ITCA.<sup>32</sup> However, even this chance to check websites

---

<sup>24</sup> Law No. 5651, Art. 8(2).

<sup>25</sup> Law No. 5651, Art. 8(4).

<sup>26</sup> Law No. 5651, Art. 8(4).

<sup>27</sup> Law No. 5651, Art. 8(5).

<sup>28</sup> Law No. 5651, Art. 8(10).

<sup>29</sup> Law No. 5651, Art. 8(10).

<sup>30</sup> For more information, please see the relevant website of the TCP at <http://www.tib.gov.tr/tr-menu-3-baskanligin-gorevleri.html> (in Turkish).

<sup>31</sup> Law No. 5651, Art. 8(3) and 8(4).

<sup>32</sup> [http://www.guvenlinet.org/tr/domain\\_sorgula.html](http://www.guvenlinet.org/tr/domain_sorgula.html) (in Turkish).

individually is restricted. After checking five websites in a row, the “safer internet” website of the ITCA requires the visitor to wait for 15 minutes to be able to check another website. This aggravates the process for individuals to obtain information on the accessibility of websites in the two profiles.

#### **4. Internet Access Regulation and the International Human Rights Agreements**

The internet access regime in Turkey cannot be analysed merely by concentrating on its internal dynamics. It is an imperative to situate the issue in Turkey to a wider context of freedom of speech. In analysing whether Turkey should or should not regulate access to online content and how it should do it, it is important to look at the issue from the human rights perspective and determine whether regulation of access to online content has to respect the human rights regime in the first place.

As the number of internet users and the time spent on the internet have increased,<sup>33</sup> it has become crucial for the states to control the online environment for various reasons which are not necessarily repressive. In fact, the need to control the internet can be seen even in democratic states, where the internet is controlled mostly for preventing access to child sexual abuse content.<sup>34</sup> For certain, different states have different approaches towards illegal and harmful content due to their culturally and historically specific environments and legislations. Therefore, the contents and the ways in which they want to control and combat illegal and harmful content differ from each other. While some states, like the United Kingdom (UK), prefer an industry-led fight towards the unwanted content;<sup>35</sup> some, like Turkey, choose a totally state-centred approach.

There are countries which recognise internet access as a standalone right<sup>36</sup> and there are even strong claims that internet access should be considered as a fundamental human right.<sup>37</sup> However, as yet, access to internet is not an internationally recognised fundamental human right. Still, this does not change the fact that access to internet is “*a powerful tool in the service of various human rights*”<sup>38</sup>; most importantly, freedom of speech. The internet is now “*a key means by which individuals can exercise their right to freedom of opinion and expression*”<sup>39</sup>. Hence, even if internet access itself is not a fundamental human right, states must take the international human rights regime into account while regulating the access to online content.

When regulating the internet access, states interfere with two different aspects of freedom of speech: the freedom of individuals to disseminate their ideas, and the freedom of individuals to receive ideas. It should not be forgotten that “*freedom of speech, by its very nature, is both the freedom of the individual who holds/express her opinion, and the freedom of people towards whom this opinion is targeted*”<sup>40</sup>. The two-sided nature of freedom of speech is also underlined in many international human rights agreements. For the purpose of this study, it is vital to look at the international human rights agreements to which Turkey is a party. Therefore it is important to examine the UDHR and the ECHR. Article 19 of the UDHR states that “[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

The first significant point about the article is the emphasis on the two-sided nature of the freedom of opinion and expression: the freedom “*to hold opinions*” and the freedom “*to seek, receive and impart information and ideas*”. However, the Article also emphasises that this freedom covers the dissemination of ideas “*through any media and regardless of frontiers*”, which includes the internet. Thus, any regulation about access to online content unavoidably has to respect Article 19 of the UDHR. Special

---

<sup>33</sup> International Telecommunication Union, “The World in 2011: ICT Facts and Figures” (2011), p.1.

<sup>34</sup> TJ McIntyre, “Child Abuse images and Cleanfeeds: Assessing Internet Blocking Systems” (2011), p.5.

<sup>35</sup> Id.

<sup>36</sup> For example, Finland and Estonia. For more information, please see, Organization for Security and Co-operation in Europe, The Office of the Representative on Freedom of the Media, “Freedom of Expression on the Internet” (2010), p.10.

<sup>37</sup> M L Best, “Can the Internet be a Human Right?” (2004), *Human Rights and Human Welfare*, Vol.4.

<sup>38</sup> Id., p.24.

<sup>39</sup> F La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” (2011), p.7.

<sup>40</sup> S Gemalmaz, “Insan Haklari Hukuku Acisindan Ifade Ozgurlugu” (1999), *Kitle Iletisim Ozgurlugu Baro Gundemi Dergisi Eki*, p.63.

Rapporteur on the promotion and protection of the right to freedom of opinion and expression of the United Nations (UN) has also underlined this fact and stated that “*the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet.*”<sup>41</sup>

Similar to the UDHR, the ECHR defines freedom of expression, and adds possible restrictions that can be applied to the right to freedom of speech. Article 10(1) of the ECHR states that “[e]veryone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.” Like the UDHR, the ECHR also underlines the two-sided nature of the freedom of speech and the frontier-neutral application of the right. However, in Article 10(2), the ECHR states that freedom of speech may be restricted in certain circumstances and provides a three-step test for the restrictions. Accordingly, any restriction to the freedom of speech should be (1) “prescribed by law” (2) “necessary in a democratic society” and (3) “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 the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

Consequently, since any restriction on access to online content is a restriction on freedom of speech, internet access regulations must pass the three-step test laid out by the ECHR. Here, the case law of the European Court of Human Rights (ECtHR) is crucial in further analysing the three-step test requires the states to do. First of all, according to the ECtHR, “[f]reedom of expression, as enshrined in Article 10, is subject to a number of exceptions which, however, must be narrowly interpreted and the necessity for any restrictions must be convincingly established.”<sup>42</sup> Secondly, the ECtHR believes that in order for a restriction to be necessary in a democratic society, it should be “proportionate to the legitimate aims pursued”. In *The Observer and the Guardian v. The United Kingdom*, the Court has ruled that “account should be taken of Article 10 (art. 10) of the Convention and the judgments of the European Court establishing that a limitation of free expression...should not be regarded as necessary unless...it was “proportionate to the legitimate aims pursued”.”<sup>43</sup> Thirdly, in order for a restriction to be necessary, there should also be a “pressing social need”. In *The Sunday Times v. The United Kingdom*, the Court clearly stated that “[t]he adjective “necessary”, within the meaning of Article 10 para. 2 (art. 10-2) [of the ECHR], implies the existence of a “pressing social need”.”<sup>44</sup> However, there might be different levels of pressing social need for the same content broadcasted on traditional media and hosted on the internet. On the internet, “the ‘odds are slim’ that a user would enter a sexually explicit site by accident. Unlike communications received by radio or television, ‘the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial...’”<sup>45</sup>. Therefore, on the internet, “the risk of encountering undesirable or illegal content is much lower than in traditional media.”<sup>46</sup> Any attempt to restrict internet access has to take into account the three-step test indicated in the ECHR and the “pressing social need” is just one of the requirements of the restriction to be necessary in a democratic society. In this regard, “rules, which are established as the consequence of a pressing social need, have to also respect the principles and requirements of a democratic society”<sup>47</sup>.

---

<sup>41</sup> F La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” (2011), p.7.

<sup>42</sup> *Thorgeirson v. Iceland*, Application No. 13778/88, Judgement of the European Court of Human Rights, 25 June 1992, 14 EHRR 843, para.63.

<sup>43</sup> *The Observer and the Guardian v. The United Kingdom*, Application No. 13585/88, Judgement of the European Court of Human Rights, 26 November 1991, para.40(c).

<sup>44</sup> *The Sunday Times v. The United Kingdom (No.2)*, Application No. 13166/87, Judgement of the European Court of Human Rights, 26 November 1991, para.50(a).

<sup>45</sup> *Janet Reno, Attorney General of the United States, Et Al., Appellants V. American Civil Liberties Union Et Al*, Supreme Court of the United States, [1997] 521 U.S. 844.

<sup>46</sup> Y Akdeniz and K Altinparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), p.53.

<sup>47</sup> The Plenary of Criminal Chambers of the Supreme Court of Turkey, Main No.2004/8-201, Decision No.2005/30, dated 15.03.2005.

## **4.1 The Turkish Case**

The internal dynamics of internet access regulation in Turkey and the wider human rights regime suggest that there is a visible violation of freedom of speech in internet access regulation in Turkey. Here, the important thing is to scrutinise the ways in which this violation is processed and to delineate the possible ways in which these violations can be overcome.

### **4.1.1 Does Turkey Respect the International Human Rights Regime?**

#### *a) State-Controlled Censorship vs. Industry-Led Censorship*

Turkey has chosen a completely state-controlled approach towards the regulation of access to online content in contrast to other democracies, such as the UK, which choose to leave the matter in the hands of the industry. Turkey's state-controlled approach is apparent in its strong resistance towards industry-led action. For example, when the TTNET (Turkey's biggest ISP) blocked access to websites such as [www.fileserve.com](http://www.fileserve.com), [www.rapidshare.com](http://www.rapidshare.com) and [www.vimeo.com](http://www.vimeo.com) without any court or TCP decision; the ITCA fined TTNET with 0.01% of its 2010 yearly net sales.<sup>48</sup> Therefore, it is evident that the State is trying to assert its legal framework, by not allowing any regulation on internet access outside its body.

Although a state-controlled censorship can (and should) be criticised, the state's approach to tackle with the industry censorship complies with the requirements of the UDHR and the ECHR. The state has two duties to ensure freedom of speech; a passive duty (not to interfere with the use of the right to freedom of speech) and an active duty (to provide an environment where the right to freedom of speech can be exercised).<sup>49</sup> Standing against industry-led censorship is one of the active duties of the state to ensure that its citizens exercise their right to freedom of speech on the internet. The industry-led approach, which is used in democratic countries such as the UK, may seem to be democratic at first glance, as it leaves the state out of the picture. However, transferring the authority from the state to industry does not rule out the state's active duty to provide an arena in which the right to freedom of speech can be exercised by its citizens.

In due course, the approach that rests only in the hands of the industry should also be subject to criticism. Although a state-controlled censorship runs the risk whereby the state shapes and restricts its citizens in a certain way, there is no guarantee that industry would provide a better option. The industry might as well impose its own censorship, or restrict the freedom of speech of individuals because of bad judgement and/or a non-transparent process. Thus, choosing self-regulation over a state-controlled system may create an "invisible and unaccountable 'censorship by proxy'".<sup>50</sup> For instance, in the UK, the Internet Watch Foundation (IWF), a non-governmental organisation, prepares a blacklist and sends this list to the ISPs for execution.<sup>51</sup> It is not mandatory for ISPs to block access to websites listed in the IWF's blacklist; however, the biggest ISPs, which represent 90% of the internet connection in the UK, are voluntarily blocking access to websites listed in the IWF's blacklist.<sup>52</sup> In December 2008, when the IWF included a Wikipedia page, which showed an album cover of the rock band Scorpions, to its blacklist, no ISP in the UK challenged this decision. All ISPs, following IWF's blacklist, blocked access to the relevant Wikipedia page. Consequently, 90% of internet users in the UK could not access that page. It should be noted here that the album cover features the picture of a naked child and it may be argued that it is a child sexual abuse content. However, the picture of the album cover had been available on the internet and the album had been sold legally for years in the UK.<sup>53</sup> What is important here is not the categorisation of the content, but rather the fact that the ISPs did not challenge the decision of the IWF.

Industry has never been and can never be the guardian of the freedom of speech regime neither in a country with an industry-led approach nor in a state-controlled one. The role of the industry in the People's Republic of China illustrates this fact clearly. Commercial companies such as Yahoo, Microsoft, Google and Skype, which are Western companies founded in democratic states, are today the main

---

<sup>48</sup> Information Technologies and Communications Authority Decision, No. 2012/DK-59/19, dated 18.01.2012.

<sup>49</sup> The Plenary of Criminal Chambers of the Supreme Court of Turkey, Main No.2004/8-201, Decision No.2005/30, dated 15.03.2005.

<sup>50</sup> TJ McIntyre, "Child Abuse images and Cleanfeeds: Assessing Internet Blocking Systems" (2011), p.1.

<sup>51</sup> <http://www.iwf.org.uk/about-iwf>

<sup>52</sup> L Edwards, "From child porn to China, in one Cleanfeed" (2006), *Script-ed* vol.3, issue 3, p.174.

<sup>53</sup> Y Akdeniz, "To Block or Not to Block" (2010), *Computer Law & Security Review* vol.26, p.265.

censors in China. It is known today that Yahoo “provides Chinese citizens with a full suite of censored products”<sup>54</sup>. Microsoft admits that “Windows Live Spaces...in China...would automatically block words like ‘freedom’ and ‘democracy’”<sup>55</sup>, Google has launched “a filtered search engine especially for China”<sup>56</sup> where the “[s]ites China wants to block won’t appear in the Google.CN search engine”<sup>57</sup>, and Skype “has a Chinese-language version developed and marketed in China by the Chinese company TOM Online...[which] censors ‘sensitive’ words in text chats”<sup>58</sup>. These companies, like the ISPs in the UK, are not interested in protecting the rights of individuals; nor should they. They are commercial companies, interested in raising their profits. It is the duty of the state, not the market, to ensure that its citizens can exercise their rights without interference.

Even if an industry-led IPS-level filtering could be highly accountable and transparent, there is still the risk that this system might want to be used for other purposes. Once an ISP-level filtering is established, there is no reason why it cannot be used for other purposes with minor tweaks in the system. This risk can be observed in the *Newzbin* case<sup>59</sup>. Normally the BT uses the Cleanfeed system for blocking access to websites which are enlisted as containing child sexual abuse content by the IWF. Yet, the movie studios in the UK requested to use this system to include the websites to be blocked for copyright infringing content. In other words, the studios wanted “BT [to] implement the same measures with regard to the *Newzbin2* website as it already operates with regard to URLs reported to it by the IWF.”<sup>60</sup> Utilising the means to tackle with child sexual abuse content for copyright infringement signifies a bigger problem. It means that a single system can encompass different demands to block access by the various actors of industry. This might make it easier to block access to content on the part of the industries, while making it harder for the wider public to secure a check-balance system for internet access blocking. As a result, a dramatic increase in the number of the blocked content could be observed. Therefore, however transparent or accountable it is, ISP-level filtering, implemented either by the state or by the industry, poses dangers.

If both state-controlled and industry-led approaches can be considered to be problematic, how will be the access to internet controlled? The answer might be sought in chaos. As a Federal US Court has stated;

*“As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion....Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects.”*<sup>61</sup>

Chaos does not necessarily mean a non-regulated and disordered environment. On the contrary, chaos might exist in a perfectly regulated environment, where the state simply provides the legal framework for internet access by respecting the freedom of speech regime. The chaos is to be found in this legal framework set by the state. Once the boundaries are set, neither the government, nor the industry can interfere in the flow of information and the multiplicity of voices on the internet. At this point, it is the active duty of the state to provide this chaotic yet free environment whereby everyone can receive and impart information in line with the international human rights regime. Therefore, the state-controlled approach, by itself, is not against the freedom of speech regime. It is “what” is regulated and “how” it is regulated in Turkey that leads this approach to become a censorship.

#### 4.1.2 The Situation in Turkey

##### a) Blocking Access to Websites in Turkey

There are various mechanisms which might be implemented to regulate access to online content. These mechanisms might be put into practice by using different techniques. For example, a state might want to block access to websites in regulating access to online content, and might implement different techniques such as IP address blocking, blocking via DNS alteration, URL blocking, or packet inspection for this

---

<sup>54</sup> J Goldsmith and T Wu, *Who Controls the Internet?: Illusions of a Borderless World* (2006), p.10.

<sup>55</sup> J Petley, *Censorship* (2009), p.107.

<sup>56</sup> Id.

<sup>57</sup> L Lessig, *Code: version 2.0* (2006), p.80.

<sup>58</sup> J Petley, *Censorship* (2009), p.108.

<sup>59</sup> *Twentieth Century Fox and others v British Telecommunications plc*, [2011] EWHC 1981 (Ch).

<sup>60</sup> Id., para.70.

<sup>61</sup> *ACLU, et al. v. Janet Reno*, 929 F Supp 824 (1996).

aim.<sup>62</sup> In Turkey, Law No. 5651 does not mandate a specific method for blocking access to websites.<sup>63</sup> Therefore, courts are free to choose any method they would like to block access to websites. Courts in Turkey usually choose URL blocking or IP blocking techniques, or sometimes do not specify any technique at all.<sup>64</sup> In its administrative blocking decisions, the TCP uses URL blocking or IP blocking techniques.<sup>65</sup> However, whatever technique is used, “*none of these techniques is 100% effective [and] each carries...the risk of over-blocking*”<sup>66</sup>.

The ineffectiveness of these techniques, especially of the URL and IP blocking techniques, is visible in the Turkish case. For example, according to Alexa statistics,<sup>67</sup> YouTube was the 5<sup>th</sup> most accessed website in Turkey in June 2008, at a time when it was blocked. Likewise, DailyMotion, which was also blocked at that time, was the 55<sup>th</sup> most accessed website. Furthermore, Ktunnel.com and Vtunnel.com, which are websites offering anonymous web proxy services and helping users to circumvent blocking decisions, were among the top 50 most visited websites in Turkey.<sup>68</sup> Therefore, it is hard to argue that the blocking mechanism used in Turkey works very effectively.

The problem this system creates is not only ineffectiveness but also over-blocking. Since there is no “content filtering system”<sup>69</sup> in Turkey, it is impossible to block access to specific URLs such as [www.youtube.com/abcd.html](http://www.youtube.com/abcd.html). In other words, once a domain address gets blocked, “*no content within the blocked domain remains available*”<sup>70</sup>. This had led to many unfortunate consequences in Turkey, especially for websites such as YouTube, which offer Web 2.0 services. From time to time, the entire content on the websites such as YouTube, DailyMotion, Geocities, and BlogSpot have been blocked because of a single video, text or picture, which is claimed to be against Law No. 5651.<sup>71</sup> For example, YouTube, to which “*48 hours of video are uploaded every minute, resulting in nearly 8 years of content uploaded every day*”<sup>72</sup>, has been blocked in Turkey for years and the entire content of YouTube remained legally inaccessible because of a few illegitimate videos.<sup>73</sup> In fact, since share of IP addresses is a common practice among websites,<sup>74</sup> this block on YouTube also affected other Google services such as Google Maps, Google Docs, Google Analytics and Google Translate because they shared same IP addresses with YouTube.<sup>75</sup> As a result, the operation of these services slowed down, or they became inaccessible. It is very hard to conclude that blocking thousands or even millions of different contents, and even entirely different services, for a single illegal content is “*proportionate to the legitimate aims pursued*”<sup>76</sup>. Since, according to the UDHR, “*the least restrictive means required to achieve the purported aim*”<sup>77</sup> should be followed, and since there are other less restrictive methods available to prevent the illegal content to be accessed; it may be concluded that using blocking measures, especially for Web 2.0 services, is against the UDHR.

One of the less-restrictive techniques (in terms of access to online content) that may be used in this matter is the content filtering system with deep packet inspection. However, this technique has its own

---

<sup>62</sup> OFCOM, “Site Blocking” to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act” (2011) p.3.

<sup>63</sup> M B Kaya, *Teknik ve Hukuki Boyutlariyla Internette Erisimin Engellenmesi* (2010), p.142.

<sup>64</sup> For examples of different blocking decisions, please see, Y Akdeniz and K Altinparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008).

<sup>65</sup> <http://www.ihbarweb.org.tr/sss.html> (in Turkish).

<sup>66</sup> OFCOM, “Site Blocking” to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act” (2011), p.5.

<sup>67</sup> [www.alexa.com](http://www.alexa.com)

<sup>68</sup> Y Akdeniz and K Altinparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), p.51.

<sup>69</sup> R Clayton, “Failures in a Hybrid Content Blocking System” (2005), section 2.1.

<sup>70</sup> Id.

<sup>71</sup> Freedom House, “Freedom on the Net 2011: A Global Assessment of Internet and Digital Media” (2011), p.330.

<sup>72</sup> <http://www.youtube.com/t/faq>

<sup>73</sup> Freedom House, “Freedom on the Net 2011: A Global Assessment of Internet and Digital Media” (2011), p.330; Organization for Security and Co-operation in Europe, “Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship” (2010), p.16.

<sup>74</sup> B Edelman, “Web Sites Sharing IP Addresses: Prevalence and Significance” (2003).

<sup>75</sup> Freedom House, “Freedom on the Net 2011: A Global Assessment of Internet and Digital Media” (2011), p.333.

<sup>76</sup> *The Observer and the Guardian v. The United Kingdom*, Application No. 13585/88, Judgement of the European Court of Human Rights, 26 November 1991, para.40(c).

<sup>77</sup> F La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” (2011), p.8.

weaknesses. While it would enable single URLs or even single images in an URL to be blocked,<sup>78</sup> it would be very costly for ISPs to implement this system and it would affect the performance of the network.<sup>79</sup> Furthermore, this technique would also have a negative impact on the privacy of individuals.<sup>80</sup> Although the debates on the packet inspection vs. privacy is beyond the scope of this essay, it is nevertheless a very important discussion as it sheds light on to the dilemma regarding the individual privacy vis-à-vis a less-restrictive method to block access to online content.

Notice & take-down mechanism is another technique that may be implemented and used before blocking access to a website. The TCP is already using the notice & take-down method in Turkey,<sup>81</sup> and this mechanism is mentioned in Law No. 5651 under the responsibilities of the hosting providers. According to the Law, the hosting providers (which also covers Web 2.0 service providers such as YouTube) are required to “remove the illegal content from broadcast, provided that [they have] been informed about the illegal content pursuant to Articles 8 and 9 of [the] Law”<sup>82</sup>. However, currently executing the notice & take-down mechanism is not a prerequisite for executing the blocking mechanism in Turkey. Given the fact that the notice & take-down mechanism is a much less restrictive method to achieve the same goal of the blocking mechanism (the removal / inaccessibility of the illegal content), it can be argued that listing the blocking access of websites as the primary and only method in the Law against the illegal content is not “proportionate to the legitimate aims pursued”<sup>83</sup>.

Another problem about the blocking process in Turkey is transparency. The problem of non-transparency is discernible in two areas; blocking statistics in Turkey, and the notices shown on the blocked websites. Since 2010, the TCP has not published any blocking statistics. Because there is no transparency, it is very hard to draw a detailed picture of the website blocking practice in Turkey. First of all, it is difficult to determine how many websites have been blocked by court orders and how many have been blocked by the administrative orders of the TCP. However, the statistics before 2010 are more transparent. The reports of the TCP indicate that 2200 websites were blocked in Turkey during May 2008 – May 2009. While 18% of these websites were blocked by court orders, 82% were blocked by the administrative decisions of the TCP.<sup>84</sup> To make the blocked websites more transparent, Engelliweb (Blocked Web),<sup>85</sup> a voluntary project in Turkey, lists websites that have been blocked in Turkey. According to Engelliweb, there are now over 20.000 blocked websites in Turkey.<sup>86</sup> Engelliweb states that 84.9% of these websites have been blocked by the administrative decisions of the TCP.<sup>87</sup> However, the content of these websites remains unclear because the TCP does not publish any information about them. The latest statistics released by the TCP about the content of the blocked websites were published in March 2010. In accordance, the majority (69.35%) of the websites, which were blocked by the administrative decisions of the TCP, were blocked due to obscene content,<sup>88</sup> which also covers legal adult content. Considering this high proportion, it might be argued that the TCP started a war against obscene content on the internet. However, since it is legal in Turkey for adults to consume legal adult content,<sup>89</sup> it is not clear why a general blocking system exists for obscene content simultaneously with the family and child profiles of the ITCA, which are introduced to protect the children from the harms of the internet.

---

<sup>78</sup> R Clayton, “Failures in a Hybrid Content Blocking System” (2005), section 2.1.

<sup>79</sup> Id.; OFCOM, “Site Blocking” to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act” (2011) p.3-5.

<sup>80</sup> OFCOM, “Site Blocking” to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act” (2011) p.7.

<sup>81</sup> The head of the Internet Department of the TCP has stated that, in their administrative decisions, before blocking access to a website, the TCP executes the notice & takedown mechanism. For more information, please see, <http://televiayon.com/p/2509/tib-internet-daire-baskani-osman-nihat-sen-ile-roportaj/> (in Turkish).

<sup>82</sup> Law No. 5651, Art. 5(2).

<sup>83</sup> *The Observer and the Guardian v. The United Kingdom*, Application No. 13585/88, Judgement of the European Court of Human Rights, 26 November 1991, para.40(c).

<sup>84</sup> Organization for Security and Co-operation in Europe, “Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship” (2010), p.12.

<sup>85</sup> [www.engelliweb.com](http://www.engelliweb.com)

<sup>86</sup> <http://engelliweb.com/istatistikler/> (in Turkish).

<sup>87</sup> Id.

<sup>88</sup> Information Technologies and Communications Authority, Telecommunications Communication Presidency, Blocking Statistics, 01.03.2010.

<sup>89</sup> Turkish Criminal Code, Art. 226.

Similar attempts to struggle with obscene content can also be observed in the IWF. Yet, while the IWF blacklists content that is “criminally obscene”<sup>90</sup>, the TCP blocks access to both legal adult and criminally obscene content on the internet. Regardless of the type of the content, a restriction to the flow of information is a restriction on the freedom of speech. The general blocking regime for obscene content in Turkey restricts the right of the adults to consume legal adult content. Since the filtering system, which is a less intrusive mechanism, is available to prevent children’s access to adult content, and since “*the least restrictive means required to achieve the purported aim*”<sup>91</sup> should be followed to meet the requirements of the UDHR, it is against Article 19 of the UDHR to have a general blocking regime for legal adult content.

There is also non-transparency regarding notices shown on the blocked websites. When a website is blocked, individuals trying to access the website can usually see which court (or whether the TCP) has blocked access to the website, but they usually cannot see why the website has been blocked. For example, a typical notice when trying to access to a blocked website is as follows; “*Access to this website is banned by the Telecommunications Communication Presidency according to the order of: Ankara 1<sup>st</sup> Criminal Court of Peace, 05/05/2008 of 2008/402.*”<sup>92</sup> However, there is no consistency on the notices shown on the blocked websites. Sometimes, individuals encounter simple notices such as “*Access to this website has been suspended with decision of Court*”<sup>93</sup>. Therefore, they cannot even see which court has given the blocking decision. This non-transparency leads to concerns as to whether the relevant website has been blocked in accordance with the Law. For example, on 27.02.2012, the website of the hacktivist group RedHack ([www.kizilhack.org](http://www.kizilhack.org)) was blocked.<sup>94</sup> RedHack is a Turkish hacktivist group, which defines themselves as Marxist and sometimes works together with the hacktivits group Anonymous.<sup>95</sup> So far, they have attacked many governmental websites including Ministry of Interior, Ministry of Foreign Affairs, Turkish National Police, and the ITCA.<sup>96</sup> When trying to access the website of RedHack from Turkey, a notice states that the website has been blocked in accordance with Law No. 5651. However, there are only a limited number of catalogue crimes listed in Law No. 5651 and hacktivism or even terrorism is not listed in the Law.<sup>97</sup> Therefore, non-transparency about the notices of blocked websites raises concerns that websites might be blocked for reasons not even listed in the Law.

### *b) The Filtering Mechanism*

Currently, Turkey is the only Organization for Security and Co-operation in Europe (OSCE) member state, which has a state-controlled nation-wide filtering system.<sup>98</sup> Like the blocking mechanism, the justification of the filtering mechanism is also made with reference to Articles 41 and 58 of the Turkish Constitution i.e. to protect the family and the children from the harms of the internet.<sup>99</sup> However, it is unclear why the general blocking regime, which restricts adult’s access to protect the family and the children, remains in force when the filtering mechanism is brought into life just for the same purpose to

---

<sup>90</sup> <http://www.iwf.org.uk/about-iwf>

<sup>91</sup> F La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” (2011), p.8.

<sup>92</sup> This was one of the notices when trying to access to YouTube.com in Turkey in 2008. The notice does not mention why the websites has been blocked. For more information, please see, Y Akdeniz and K Altinparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), p.34.

<sup>93</sup> Y Akdeniz and K Altinparmak, *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), p.42.

<sup>94</sup> Ankara 6<sup>th</sup> Criminal Court of Peace, Decision No. 2012/253, dated 27.02.2012.

<sup>95</sup> For more information, please see, <http://www.ibtimes.co.uk/articles/332422/20120424/anonymous-join-marxist-redhack-group-against-turkey.htm>; <http://www.hurriyet.com.tr/gundem/21094255.asp> (in Turkish).

<sup>96</sup> For more information, please see, <http://www.hurriyet.com.tr/planet/20904391.asp> (in Turkish); <http://www.hurriyet.com.tr/gundem/20390478.asp> (in Turkish); <http://hurarsiv.hurriyet.com.tr/goster/printnews.aspx?DocID=21026552> (in Turkish); <http://www.hurriyet.com.tr/gundem/21094255.asp> (in Turkish).

<sup>97</sup> Article 8 of Law No. 5651 lists the following crimes; (1) provocation for committing suicide, (2) sexual harassment of children, (3) easing the usage of drugs, (4) supplying drugs which are dangerous for health, (5) obscenity, (6) prostitution, (7) providing place and opportunity for gambling, and (8) crimes mentioned in the Law on Crimes against Atatürk (the founder of the Turkish Republic).

<sup>98</sup> Organization for Security and Co-operation in Europe, The Office of the Representative on Freedom of the Media, “Freedom of Expression on the Internet” (2010), p.26.

<sup>99</sup> <http://www.tib.gov.tr/tr/tr-menu-76-guvenli-internet-hizmet-hakkindaki-sorular.html> (in Turkish).

protect family and children. The justification for the co-existence of these two mechanisms remains unanswered.

The filtering mechanism is advocated on the fact that it is voluntary and it is very easy to shift between different filters. According to the TCP, it takes 10 to 20 seconds to change a profile (for example, from child profile to family profile; or from family profile to non-profile).<sup>100</sup> Yet, these do not dismiss problematic and potentially dangerous aspects of the filtering mechanism in Turkey. The problem of transparency, evident in blocking mechanism, can also be observed in filtering mechanism. In the first place, the blacklist and the whitelist, prepared by the ITCA, are not publicised. Therefore, it is not possible for parents to check which websites are restricted or allowed in each profile. This method of not publicising the blacklists also exists in other illegal content reporting / filtering services outside Turkey. The biggest example is the IWF, which does not publicise its blacklist either. However, the IWF filters content in the categories of “child sexual abuse images hosted anywhere in the world”, “criminally obscene adult content hosted in the UK”, and “non-photographic child sexual abuse images hosted in the UK”.<sup>101</sup> That is to say, the content filtered by the IWF is “illegal” content, and the reason why it should not be publicised is obvious. Yet, the content filtered by the ITCA is not “illegal” content, since access to “illegal” content is already blocked by the courts and the TCP regardless of the filtering mechanism. Filtering is an additional mechanism to blocking, which filters content that may be “harmful” for children,<sup>102</sup> but not “illegal”. Therefore, publicising these lists does not run the same risks as publicising the illegal content list of the IWF does. Knowing which websites are restricted or allowed, adults could make better decisions for their children, and the filtering process could be more transparent.

Another problem about the filtering mechanism in Turkey relates to the content of the websites which are restricted or allowed in each profile. In other words, what kinds of content are allowed or restricted in what purpose is an important question to tackle with. For example, the website [www.aboutdarwin.com](http://www.aboutdarwin.com), which is a website about the life of Charles Darwin, can be accessed via the family profile; however, it cannot be accessed via the child profile.<sup>103</sup> On the other hand, [www.evrimaldatmacasi.com](http://www.evrimaldatmacasi.com), which states that Darwinism and materialism constitute roots for terrorism and that Islam is the solution to terrorism; and [www.darwinizmdini.com](http://www.darwinizmdini.com), which argues that Darwin’s evolutionary theory has been the scientific base of bloody ideologies and ruthless wars, can be accessed both via the family and the child profile.<sup>104</sup> This same conservative approach is visible in the case of [www.gabile.com](http://www.gabile.com), which is a gay/bisexual/lesbian chatting website that cannot be accessed via the child profile.<sup>105</sup> Moreover, while informational and forum websites about atheism such as [www.ateizm.org](http://www.ateizm.org) and [www.ateistforum.org](http://www.ateistforum.org) cannot be accessed via the child profile,<sup>106</sup> websites about Islam religion such as [www.dinimizislam.com](http://www.dinimizislam.com), [www.islamkent.com](http://www.islamkent.com) and [www.islammerkezi.com](http://www.islammerkezi.com) can be accessed via both of the profiles.<sup>107</sup> Also, apparently, the ITCA wants to ensure that the blocking mechanism is not circumvented via websites offering web proxy services. Websites such as [www.ktunnel.com](http://www.ktunnel.com), [www.vtunnel.com](http://www.vtunnel.com), [www.hidemypass.com](http://www.hidemypass.com), [www.anonymouse.org](http://www.anonymouse.org), [www.ninjacloak.com](http://www.ninjacloak.com), [www.hideipvpn.com](http://www.hideipvpn.com), [www.torproject.org](http://www.torproject.org), which allow the visitors to surf the web anonymously, cannot be accessed neither via the family profile nor the child profile.<sup>108</sup>

There is no objective reason stated why a website about the life of Charles Darwin, a gay/bisexual/lesbian chatting website, informational websites about atheism, or services which offer anonymity on the internet might be “harmful” for children or for the family. The non-transparent process about the filtering mechanism and the content of the filtered websites raise concerns, since these filters might become (or already became) one of the means through which the state shapes its citizens. It is important to underline that “*there could be a breach of Article 10 of ECHR if...filtering tools are used at a state level to silence politically motivated speech on the Internet, or the criteria for...filtering is secret,*

---

<sup>100</sup> Id.

<sup>101</sup> <http://www.iwf.org.uk/about-iwf>

<sup>102</sup> <http://guvenlinet.org.tr/tr/sss.html> (in Turkish).

<sup>103</sup> As of 06.08.2012. Checked with the “safer internet” website of the ITCA at [http://guvenlinet.org.tr/tr/domain\\_sorgula.html](http://guvenlinet.org.tr/tr/domain_sorgula.html)

<sup>104</sup> Id.

<sup>105</sup> Id.

<sup>106</sup> Id.

<sup>107</sup> Id.

<sup>108</sup> Id.

*or the decisions of the administrative bodies are not publically made available for legal challenge*<sup>109</sup>. Taking into account the contents of the websites which are filtered, question marks raise on minds on whether the ITCA designates the filters in accordance with the views of the current “neo-Islamist”<sup>110</sup> Government.

## **5. What Should Change?**

Previous chapters have underlined that Turkey’s internet access regulation falls short of meeting the requirements of the UDHR and ECHR in the context of freedom of speech. The main objective of the paper is not only to discuss the ways in which the right to freedom of speech is violated in Turkey, but also to try to outline the possible ways to tackle with these problems. Although the scope of this paper does not allow for all-encompassing policy suggestions, number of reforms can be pinpointed in order for the regulation to respect the freedom of speech regime.

### **5.1 The TCP should not be able to block access to websites for any reason other than child sexual abuse content.**

In terms of blocking decisions, the role of the TCP cannot be ignored in an environment where more than 80% of the websites are blocked by the administrative decisions of the TCP.<sup>111</sup> This number is evidently very high and this situation keeps the owners of the blocked websites excluded from the possible guarantees of court decisions. However, this does not mean that the TCP should not give administrative blocking decision for any content on the web. For instance, child sexual abuse content is a legitimate type of information which may be restricted,<sup>112</sup> and quick action needs to be taken in order for the content not to be disseminated through the internet.<sup>113</sup> Since court decisions may take longer time than the immediate action of the TCP, the TCP should have the power to block access to child sexual abuse content on the internet. Yet, the current regime, in which the TCP can block access to obscene content (including legal adult content), as well as any content listed in Article 8 of Law No. 5651 (for which the content provider or the hosting provider resides outside of Turkey) restricts the freedom of speech of individuals greatly. There should be a clear division of labour between the TCP and the courts. The TCP is an administrative body, and the judgement of legality / illegality of content should only be given by the courts. The UN has warned the states about this issue as follows;

*“Co- and self-regulatory initiatives (codes of conduct and hotlines) by ISPs and other Internet stakeholders should include improved mechanisms and sanctions. Consideration should be given to the fact that ISPs are technical in nature and lack the capacities to determine whether material on the Internet is illegal or harmful. While encouraging these initiatives, States should ensure that the due process of law is respected and effective remedies remain available in relation to measures enforced.”*<sup>114</sup>

The risk that has been set forth for self-regulation of ISPs is also valid for the TCP, which is an administrative body.

---

<sup>109</sup> Organization for Security and Co-operation in Europe, “Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship” (2010), p.3.

<sup>110</sup> C Keyder, “The Turkish Bell Jar” (2004) *New Left Review*, vol.28.

<sup>111</sup> Organization for Security and Co-operation in Europe, “Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship” (2010), p.12; <http://engelliweb.com/istatistikler/> (in Turkish).

<sup>112</sup> F La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” (2011), p.8.

<sup>113</sup> J Kortlander, “Is filtering the new silver bullet in the fight against child pornography on the internet? A legal study into the experiences of Australia and Germany” (2011), *Computer and Telecommunications Law Review*, p.1.

<sup>114</sup> United Nations, “Report of the Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action on its fourth session” (2006), p.12.

## **5.2 Statistics about blocked websites should be published.**

The TCP has not published the total number of blocked websites since 2009, and the rate of blocked websites in each category (of Article 8 of Law No. 5651) since 2010. The TCP is also unwilling to provide these statistics to international organizations. OSCE has requested the relevant statistics from the TCP for the report “Turkey and Internet Censorship”; however, the TCP did not provide the relevant statistics to OSCE.<sup>115</sup> The public has a right to know about the decisions and activities of public administrative bodies. The statistics about the blocked websites would increase the transparency about the activities of the TCP as well as blocking regime in Turkey in general.

## **5.3 A clear indication of why the website has been blocked should be stated and publicised when trying to access the relevant blocked website.**

There is no uniformity and transparency in the blocking decisions of the courts and the TCP. A clear indication on why a website has been blocked is not provided to the individuals, who are trying to access to the relevant page. People, trying to access to a webpage, may be presented with a simple notice as; “*Access to this website has been suspended with decision of Court*”. This non-transparency also makes it hard to judge whether the webpage has been blocked in accordance with the Law.<sup>116</sup> In an environment where even the content providers are not informed clearly about the blocking decisions about their websites,<sup>117</sup> a clear notice on the blocked webpage could serve as the basis of effective legal challenges to the blocking decisions.

## **5.4 Everyone should be able to object to blocking decisions.**

When a webpage is blocked, the right of the content provider and the right of the public (to seek and receive information) are being restricted. According to Article 8 of Law No. 5651, blocking decisions are “protective precautions”; and therefore, interested parties can object to the blocking decisions.<sup>118</sup> However, the Law does not make it clear whether the individuals, who are trying to access to the blocked page are “interested parties”. Since the individuals’ right are also being restricted by the blocking decisions, it should be clearly stated in the Law that they are also among the interested parties; and thus, can object to the blocking decisions.

## **5.5 A differentiation should be made between illegal content and harmful content. Blocking decisions should be given only for illegal content.**

Law No. 5651 enables blocking decisions to be given for both illegal and harmful content. According to the Law, websites with obscene content (including legal adult content) can be blocked both by the courts and the TCP. However, adult content is not illegal in Turkish Law; it is considered as “harmful” for children. Therefore, a general blocking regime on this matter restricts adults’ right to consume legal adult content. As the European Commission (EC) stated:

*“[I]t is crucial to differentiate between content which is illegal and other harmful content. These different categories of content pose radically different issues of principle, and call for very different legal and technological responses. It would be dangerous to amalgamate separate issues such as children accessing pornographic content for adults, and adults accessing pornography about children.”<sup>119</sup>*

---

<sup>115</sup> Organization for Security and Co-operation in Europe, “Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship” (2010), p.10.

<sup>116</sup> For example, in the case of RedHack.

<sup>117</sup> Freedom House, “Freedom on the Net 2011: A Global Assessment of Internet and Digital Media” (2011), p.332.

<sup>118</sup> Law No. 5651, Art. 8(10).

<sup>119</sup> Commission of the European Communities, Communication from the Commission, “Illegal and harmful content on the Internet” (1996), p.10.

Dealing with the harmful content should be the duty of the individual, rather than the state.<sup>120</sup> Therefore, different strategies should be formulated to deal with harmful and illegal contents.

### **5.6 Blocking access to websites should not be the first and the only method to prevent the crimes committed on the internet.**

Blocking access to websites is the only method designated in Law No. 5651 to prevent the crimes committed on the internet.<sup>121</sup> However, this approach creates many problems especially for Web 2.0 services, where blocking the website may result in blocking access to millions of other unrelated legal content. Blocking access to websites, especially for Web 2.0 services, is not “*proportionate to the legitimate aims pursued*”<sup>122</sup> and is certainly not “*the least restrictive means required to achieve the purported aim*”<sup>123</sup>. Therefore, before blocking access to a website, the less restrictive notice & take-down mechanism should be used. Since blocking mechanism intervenes with the freedom of speech of individuals greatly, blocking should be the last method used to combat illegal content on the internet.

### **5.7 URL and IP blocking are not the only techniques to block access to websites. Research on different blocking techniques should be conducted.**

Turkey uses URL and IP blocking techniques to block access to websites.<sup>124</sup> However, there are other techniques available that may be implemented for this issue.<sup>125</sup> Some of these techniques, such as deep packet inspection, have less impact on legitimate services. Yet, they may have more impact on the privacy of the individuals, which might lead to another version of violation of the right to freedom of speech regime. The privacy issue could not be discussed within the scope of this study. However, further research should be conducted on different blocking techniques by considering both the impact on legitimate services and individual privacy.

### **5.8 Blocking access to websites cannot be justified upon the protection of the family and the youth. Private home filtering should be the primary internet access control mechanism.**

A general blocking mechanism, which restricts both adults’ and children’s access to online content, cannot be justified upon the protection of children and the family, i.e. upon protecting certain social groups in the society. Thus, private home filtering should be preferred to a general blocking mechanism for the protection of the family and the youth, since it is both customisable and more effective than a general blocking mechanism. Blocking decisions are given for specific URLs and IPs and this leaves out peer-to-peer (P2P) traffic completely. Still, the importance and rate of P2P traffic cannot be underestimated. Studies show that only BitTorrent, a P2P file sharing protocol, accounts for 20.32% of all peak hour Internet traffic in Europe, while eDonkey, another P2P network, accounts for 9.39%.<sup>126</sup> While a general blocking system cannot protect the children from the “harms” of the P2P networks, private home filtering can. Most of the private home filtering software offer options for monitoring or blocking P2P traffic.<sup>127</sup>

---

<sup>120</sup> Department of Justice, Equality and Law Reform (of the Republic of Ireland), First Report of the Working Group, “Illegal and Harmful Use of the Internet” (1998), p.2.

<sup>121</sup> Article 9 of the Law designates the right of content removal and the right of reply. However, this article can only be applied in private law issues.

<sup>122</sup> *The Observer and the Guardian v. The United Kingdom*, Application No. 13585/88, Judgement of the European Court of Human Rights, 26 November 1991, para.40(c).

<sup>123</sup> F La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” (2011), p.8.

<sup>124</sup> <http://www.ihbarweb.org.tr/ss.html> (in Turkish).

<sup>125</sup> See, generally, OFCOM, “Site Blocking” to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act” (2011); R Clayton, “Failures in a Hybrid Content Blocking System” (2005).

<sup>126</sup> Sandvine Intelligent Broadband Networks, “Global Internet Phenomena Report” (2012), p.26.

<sup>127</sup> For example, McAfee SafeEyes (<http://www.internetsafety.com/filter-youtube-and-hulu-videos.php>), Net Nanny (<http://www.netnanny.com/features/im-and-chat-room-monitoring>), PureSight (<http://www.puresight.com/General/control-file-sharing.html>).

## 5.9 ISP-level filtering should not exist.

The state-controlled ISP-level filtering in Turkey is problematic since there are no objective criteria for filtering and the lists prepared by the ITCA are not publicised. Moreover, the content of the filtered websites indicates that the filters might be prepared in line with the views of the Government. However, industry-led ISP-level filtering also poses dangers on its own, as it is apparent in the UK case. Different events, such as the blocking of Wikipedia, raise question marks about the transparency and accountability of such self-regulatory bodies. Furthermore, the *Newzbin* case has shown that once ISP-level filtering is established, the system would want to be used for completely different purposes and could further the restriction on the freedom of speech of individuals.

## 6. Conclusion

All in all, this paper seeks to explore the ways in which the violation of freedom of speech in Turkey is taking place and can be overcome. This evaluation of the internet access regulation in Turkey in the context of freedom of speech suggests that Turkey is far from respecting the international human rights agreements. In fact, the regulation and the practice of this regime indicate censorship.

Accordingly, tracing the internet access regulation in Turkey historically, it is plausible to argue that the same repressive way to regulate the traditional media has been used to regulate the internet access in Turkey. Law No. 5651, which may be regarded as the benchmark in this history, has the potential to maintain Turkey's tradition on being "*the most convicted country in the European Court of Human Rights for freedom of speech and freedom of press*"<sup>128</sup>. However, Turkey, as a party to the UDHR and the ECHR, has to respect the principles of freedom of speech. Ensuring this does not necessarily entail the abandoning of a state-controlled approach in favour of an industry-led one. On the contrary, it should be the active duty of Turkey to provide the environment where individuals can freely exercise their right to freedom of speech. Therefore, the problem in Turkey does not rest on the fact that the internet access regulation is state controlled. Rather, the problem lays in the non-convergence of the regime in Turkey with the international human rights agreements.

The non-convergence is rooted in the justification of Law No. 5651, i.e. "protection of the children, youth and the family" from the "harms" of the internet. Designating a general blocking mechanism on the basis of such justification, the Law restricts everyone's right to freedom of speech. The high rate of administrative blocking decisions, the non-transparency in the practice of blocking, the utilisation of the blocking mechanism as the only method to deal with illegal content on the internet, and usage of techniques that cause over-blocking deteriorate the situation. The other mechanism in the internet access regulation, the filtering mechanism, suffers from similar defects of non-transparency of the process and the choice of filtered contents. Apart from that, there is no justification as to why two different mechanisms to achieve with the same end (protection of the children, youth and the family) should co-exist. Therefore, it is plausible to argue that the restrictions of freedom of speech in Turkey are not "proportionate to the legitimate aims pursued".

Having addressed the ways in which the internet access regime in Turkey violates the right to freedom of speech, the paper tentatively outlines nine steps that can be taken to meet the requirements of international human rights agreements. In order to accomplish these steps, either Law No. 5651 should be changed comprehensively, or the Law should be abolished and a new Law should be prepared in the light of freedom of speech. At this point, it might be useful to remember what the US Federal Court suggested on the necessity of "chaos" on the internet. Accordingly, the "*cacophony of the unfettered speech*"<sup>129</sup> and the multiplicity of voices in receiving and imparting information are the motors of this chaos. However, this "chaotic" environment cannot be formed on the basis of the internal merits of the internet. It is the responsibility of the Turkish state to provide a legal framework that embraces and maintains such "chaotic" environment on the internet in line with the international human rights regime. Turkey can achieve "chaos" on the internet through a comprehensive reform on Law No. 5651 or a new Law written in the light of freedom of speech.

---

<sup>128</sup> As stated by Isil Karakas, European Court of Human Rights Judge. For more information, please see, <http://www.ntvmsnbc.com/id/25300906/> (in Turkish).

<sup>129</sup> *ACLU, et al. v. Janet Reno*, 929 F Supp 824 (1996).

## Acknowledgment

The author wishes to express his gratitude to Ms. Judith Rauhofer for her valuable comments and guidance in developing this paper.

## Reference

- Akdeniz, Y and Altinparmak, K *Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (2008), available at [http://www.cyber-rights.org/reports/internet\\_restricted\\_colour.pdf](http://www.cyber-rights.org/reports/internet_restricted_colour.pdf) [last accessed 12 August 2012]
- Akdeniz, Y “To Block or Not to Block” (2010), *Computer Law & Security Review*, vol.26, pp.260-272
- Best, M L “Can the Internet be a Human Right?” (2004), *Human Rights and Human Welfare*, vol.4, pp.23-31
- Clayton, R “Failures in a Hybrid Content Blocking System” (2005), available at <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf> [last accessed 12 August 2012]
- Commission of the European Communities, Communication from the Commission, “Illegal and harmful content on the Internet” (1996), available at <http://aei.pitt.edu/5895/1/5895.pdf> [last accessed 12 August 2012]
- Department of Justice, Equality and Law Reform (of the Republic of Ireland), First Report of the Working Group, “Illegal and Harmful Use of the Internet” (1998), available at [http://ec.europa.eu/avpolicy/docs/reg/minors/useinternet1streport\\_ie.pdf](http://ec.europa.eu/avpolicy/docs/reg/minors/useinternet1streport_ie.pdf) [last accessed 12 August 2012]
- Edelman, B “Web Sites Sharing IP Addresses: Prevalence and Significance” (2003), available at [http://cyber.law.harvard.edu/archived\\_content/people/edelman/ip-sharing/](http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/) [last accessed 12 August 2012]
- Edwards, L “From Child porn to China in one Cleanfeed” (2006), *Script-ed*, vol.3(3), pp.174-175
- Freedom House, “Freedom on the Net 2011: A Global Assessment of Internet and Digital Media” (2011), available at <http://www.freedomhouse.org/sites/default/files/FOTN2011.pdf> [last accessed 12 August 2012]
- Gemalmaz, S “Insan Haklari Hukuku Acisindan Ifade Ozgurlugu” (1999), *Kitle Iletisim Ozgurlugu Baro Gundemi Dergisi Eki*
- Goldsmith, J and Wu, T *Who Controls the Internet?: Illusions of a Borderless World* (2006), New York: Oxford University Press
- Gunaydin, B *Internet Yayinciligi ve Ifade Ozgurlugu* (2010), Ankara: Adalet Yayınevi
- International Telecommunication Union, “The World in 2011: ICT Facts and Figures” (2011), available at <http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf> [last accessed 12 August 2012]
- Kaya, M B *Teknik ve Hukuki Boyutlariyla Internete Erisimin Engellenmesi* (2010), Istanbul: On İki Levha Yayıncılık A.S.
- Keyder, C “The Turkish Bell Jar” (2004), *New Left Review*, vol.28, available at <http://newleftreview.org/II/28/caglar-keyder-the-turkish-bell-jar> [last accessed 12 August 2012]
- Kortlander, J “Is filtering the new silver bullet in the fight against child pornography on the internet? A legal study into the experiences of Australia and Germany” (2011), *Computer and Telecommunications Law Review*, vol.17(7), pp.199-208
- La Rue, F “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” (2011), available at [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf) [last accessed 12 August 2012]
- Lessig, L *Code: version 2.0* (2006), New York: Basic Books
- McIntyre, TJ “Child Abuse images and Cleanfeeds: Assessing Internet Blocking Systems” (2011), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1893667](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1893667) [last accessed 12 August 2012]
- OFCOM, “Site Blocking” to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act” (2011)
- Organization for Security and Co-operation in Europe, “Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship” (2010), available at <http://www.osce.org/fom/41091> [last accessed 12 August 2012]
- Organization for Security and Co-operation in Europe, The Office of the Representative on Freedom of the Media, “Freedom of Expression on the Internet” (2010), available at <http://www.osce.org/fom/80723> [last accessed 12 August 2012]
- Sandvine Intelligent Broadband Networks, “Global Internet Phenomena Report” (2012)
- Turkish Grand National Assembly, “Session No. 99” (2007), *Journal of Minutes*, vol.156
- Petley, J *Censorship* (2009), Oxford: Oneworld Publications
- United Nations, “Report of the Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action on its fourth session” (2006), available at <http://www.upeace.org/news/newsflash/2006/24april06/Durham%20Final%20Report.pdf> [last accessed 12 August 2012]

## Cases and Administrative Decisions

- ACLU, et al.v. Janet Reno*, 929 F Supp 824 (1996)  
Ankara 6<sup>th</sup> Criminal Court of Peace, Decision No. 2012/253, dated 27.02.2012  
Ankara 11<sup>th</sup> Criminal Court of First Instance, Decision No. 2004/31  
Information Technologies and Communications Authority Decision, No. 2012/DK-59/19, dated 18.01.2012  
Istanbul 3<sup>rd</sup> Criminal Court of Peace, Decision No. 2005/1870  
Istanbul 4<sup>th</sup> High Criminal Court, Main No.1999/225, Decision No.2001/56, dated 27.03.2001  
Istanbul Chief Public Prosecutor's Office, Press Bureau, Main No.1999/280, Accusation No.1999/348, dated 28.07.1999  
*Janet Reno, Attorney General of the United States, Et Al., Appellants V. American Civil Liberties Union Et Al*, Supreme Court of the United States, [1997] 521 U.S. 844  
*The Observer and the Guardian v. The United Kingdom*, Application No. 13585/88, Judgement of the European Court of Human Rights, 26 November 1991  
The Plenary of Criminal Chambers of the Supreme Court of Turkey, Main No.2004/8-201, Decision No.2005/30, dated 15.03.2005  
*The Sunday Times v. The United Kingdom (No.2)*, Application No. 13166/87, Judgement of the European Court of Human Rights, 26 November 1991  
*Thorgeirson v. Iceland*, Application No. 13778/88, Judgement of the European Court of Human Rights, 25 June 1992  
*Twentieth Century Fox and others v British Telecommunications plc*, [2011] EWHC 1981 (Ch)

## Internet Sources

- Anonymous Emniyet ve MIT'e saldırdı, available at <http://hurarsiv.hurriyet.com.tr/goster/printnews.aspx?DocID=21026552> [last accessed 12 August 2012]  
Anonymous Joins Marxist RedHack Group against Turkey Internet Censors, available at <http://www.ibtimes.co.uk/articles/332422/20120424/anonymous-join-marxist-redhack-group-against-turkey.htm> [last accessed 12 August 2012]  
Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı, İhbar İstatistikleri – Erisim Engelleme İstatistikleri, available at [http://www.guvenliweb.org.tr/istatistikler/files/pdf/ihbar\\_istatistikleri\\_01.03.2010.pdf](http://www.guvenliweb.org.tr/istatistikler/files/pdf/ihbar_istatistikleri_01.03.2010.pdf) [last accessed 12 August 2012]  
Binali Yıldırım, "Güvenli internette sansur yok", available at <http://www.ntvmsnbc.com/id/25299546/> [last accessed 12 August 2012]  
Binali Yıldırım, "İnternette yasak falan yok", available at <http://ekonomi.haberturk.com/teknoloji/haber/631128-internette-yasak-falan-yok> [last accessed 12 August 2012]  
CHP Bilgi ve İletişim Teknolojileri Genel Başkan Yardımcısı Emrehan Halici 2011 Bilisim Raporunu Açıkladı, available at <http://www.chp.org.tr/?p=60839> [last accessed 12 August 2012]  
EngelliWeb, "İstatistikler: Erimiş Engellenen Websiteleri", available at <http://engelliweb.com/istatistikler/> [last accessed on 12 August 2012]  
Güvenli İnternet, Alan Adı Profil Kontrolü, available at [http://www.guvenlinet.org.tr/domain\\_sorgula.html](http://www.guvenlinet.org.tr/domain_sorgula.html) [last accessed 12 August 2012]  
Güvenli İnternet, Sıkça Sorulan Sorular, available at <http://guvenlinet.org.tr/tr/sss.html> [last accessed 12 August 2012]  
İhbarWeb, Sıkça Sorulan Sorular, available at <http://www.ihbarweb.org.tr/sss.html> [last accessed 12 August 2012]  
İnternet Gerçekti Hayal Oldu, available at <http://www.chp.org.tr/?p=25120> [last accessed on 12 August 2012]  
İnternet Watch Foundation, About Us, available at <http://www.iwf.org.uk/about-iwf> [last accessed 12 August 2012]  
İsil Karakas, "Vicdani Ret Mutlaka Uygulanmalı" available at <http://www.ntvmsnbc.com/id/25300906/> [last accessed 12 August 2012]  
RedHack bu kez Disisleri'ni hack'ledi, available at <http://www.hurriyet.com.tr/planet/20904391.asp> [last accessed 12 August 2012]  
RedHack, "Mouse ve Klavyeden Baska Kaybedecek Bir Seyimiz Yok", available at <http://www.hurriyet.com.tr/gundem/21094255.asp> [last accessed 12 August 2012]  
Sansüre Karsi Yuruyus, available at <http://www.sansurekarsiyuruyus.com> [last accessed 12 August 2012]  
Sansüre Sansur, "İnternetin İçin Yuru", available at <http://www.sansuresansur.org/internetin-icin-yuru/> [last accessed 12 August 2012]  
Telekomünikasyon İletişim Başkanlığı, Başkanlığın Görevleri, available at [http://www.tib.gov.tr/tr/menu-3-baskanligin\\_gorevleri.html](http://www.tib.gov.tr/tr/menu-3-baskanligin_gorevleri.html) [last accessed 12 August 2012]  
Telekomünikasyon İletişim Başkanlığı, Güvenli İnternet Hizmeti Hakkındaki Sorular, available at [http://www.tib.gov.tr/tr/menu-76-guvenli\\_internet\\_hizmet\\_hakkindaki\\_sorular.html](http://www.tib.gov.tr/tr/menu-76-guvenli_internet_hizmet_hakkindaki_sorular.html) [last accessed 12 August 2012]  
Televizyon, "Bölüm 19: TIB İnternet Daire Başkanı Osman Nihat Sen ile Raporaj", available at <http://televizyon.com/p/2509/tib-internet-daire-baskani-osman-nihat-sen-ile-roportaj/> [last accessed 12 August 2012]

*Evaluating the Regulation of Access to Online Content in Turkey in the Context of Freedom of Speech*

Turkey again takes top spot in ECHR violation in 2011, available at [http://www.todayszaman.com/newsDetail\\_getNewsById.action?newsId=269732](http://www.todayszaman.com/newsDetail_getNewsById.action?newsId=269732) [last accessed 12 August 2012]

YouTube, Frequently Asked Questions, available at <http://www.youtube.com/t/faq> [last accessed 12 August 2012]

. \* \* \* \* \*

 © 2014 This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works. Cite as: Kinnikoglu, Batu. Evaluating the Regulation of Access to Online Content in Turkey in the Context of Freedom of Speech. *Journal of International Commercial Law and Technology*, Vol.9 No.1 (January,2014)