

### **COMPARATIVE STUDY**

ON

## **BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT**

Excerpt, pages 711-727

This document is part of the Comparative Study on blocking, filtering and take-down of illegal internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member states, the Council of Europe's statutory organs or the European Court of Human Rights.

#### Avis 14-067

Lausanne, 20 December 2015 National reports current at the date indicated at the end of each report.

### I. INTRODUCTION

On 24<sup>th</sup> November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

### II. METHODOLOGY AND QUESTIONS

# 1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

### 2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

# 1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

### 2. What is the legal framework regulating:

### 2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - o the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - o preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet Access Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

### 2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - o the prevention of disorder or crime (e.g. child pornography),
  - o the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - o preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

# 3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

# 4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

### 5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the
  requirements of quality (foreseeability, accessibility, clarity and precision) as developed
  by the European Court of Human Rights? Are there any safeguards for the protection of
  human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

### **TURKEY**

Turkey is a country that has, since 2007, had several legal measures for blocking access to websites and Internet content, a filtering policy for schools, Internet cafes and home Internet users, as well as take-down procedures for Internet content. Several well known websites, including social media platforms such as YouTube and Twitter, have been subject to blocking since the enactment of Law No 5651 in May 2007 and the blocking provisions of this law have been subject to a legal challenge at the European Court of Human Rights. In what was its first Internet content access blocking related decision, in *Ahmet Yıldırım v. Turkey*, <sup>1</sup> the European Court, finding a violation of Article 10 of the European Convention on Human Rights, held that restricting access to a source of information is only compatible with the Convention if a strict legal framework is in place regulating the scope of the ban and providing a guarantee of judicial review to prevent possible abuses. Subsequently, in *Cengiz and Others v. Turkey*, the European Court also found a violation of Article 10 concerning the blocking of access to YouTube from Turkey from 5 May 2008 until 30 October 2010.<sup>2</sup>

# 1. Legal Sources

Turkey has extensive blocking, filtering and take down procedures for both illegal and harmful Internet content. Law No. 5651, entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication", is the primary piece of legislation for regulation of this area. Law No. 5651 was enacted in May 2007 and came into force in November 2007. This law was subsequently amended three times during 2014 and once during 2015, extending the scope of the original blocking measures. In its current version, Law No. 5651 includes four separate blocking measures through article 8 (protection of children from harmful content), article 8A (protection of national security, public order, protection of life and property as well as protection of public health and prevention of crime), article 9 (violation of individual rights) and article 9A (violation of privacy of individuals). Furthermore, hosting providers are required by article 5(2) of Law No. 5651 to remove and take down content if legally notified to do so. In addition to the provisions of Law No. 5651, Law No. 5846 on "Intellectual & Artistic Works" through supplemental article 4 includes a blocking measure with regards to intellectual property infringements which is often used to block access to piracy related websites from Turkey.<sup>3</sup>

Access to over 110,000 websites and over 16,500 URLs is currently blocked to Internet users in Turkey by way of these blocking measures and related court and administrative decisions.

In terms of filtering activities, **article 7** of Law No. 5651 requires Internet cafes and other commercial mass use providers to **use government approved blocking and filtering tools**. Infringement of article 7 provisions will result in an administrative fine between 1,000TL (320EUR) and 15,000TL (48,000EUR) or an injunction to cease the relevant activity for up to three days with a decision of a local civilian authority such as a governor or mayor. Furthermore, a country wide optional filtering

Ahmet Yıldırım v. Turkey, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

<sup>&</sup>lt;sup>2</sup> Cengiz and Others v. Turkey, Application Nos. 48226/10 and 14027/11, judgment of 01 December 2015, 01 March 2016 (final).

Other legal provisions such as those included within the Anti-Terror Law (No 3713), the Civil Code (Law No 4721), Law amending the formation and duties of the Presidency of Religious Affairs of the Republic of Turkey, Government Decree on the protection of trade marks are also used for blocking access to websites.

All Mass Use Providers will be responsible for retaining the logs and communication data of their users with regards to access and blocking of illegal content and taking the precautionary measures in accordance with further regulations to be established by secondary legislation.

system for home users was launched with a decision of the Information Technologies and Communication Board ("BTK") on 24 August 2011, annulling an earlier controversial decision of 22 February 2011 which made it compulsory to use a filtering profile for all home users. ISPs are compelled to offer the filtering service to their customers and the filtering database and profiles are controlled and maintained by the government.

In terms of its international commitments, Turkey has signed (10/11/2010) and ratified the (29/09/2014) CoE Convention on Cybercrime (CETS No. 185) and the Convention provisions came into force on 01/01/2015. However, Turkey did not sign or ratify the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189). In terms of the CoE Convention on the Prevention of Terrorism (CETS No. 196), Turkey signed (19/01/2006) and ratified (23/03/2012) the Convention and the provisions of the Convention came into force on 01/07/2012. So far as the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) is concerned, Turkey signed (25/10/2007) and ratified (07/12/2011) the Convention and the provisions of the Convention came into force on 01/04/2012. Finally, Turkey signed (28/01/1981) but it has not yet ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

# 2. Legal Framework

### 2.1. Blocking and/or filtering of illegal Internet content

In 2007, Turkey introduced extensive blocking provisions through Law No. 5651, entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication".

Under **article 8**, access to a websites can be prevented under a blocking order if there is sufficient suspicion that certain crimes are being committed on that website. There are eight specific "catalogue crimes" that are included within article 8 and the aim of this provision is the **protection of children from allegedly harmful content**. The so-called catalogue crimes are:

- encouragement and incitement of suicide (article 84 of the Turkish Penal Code);<sup>5</sup>
- sexual exploitation and abuse of children (article 103(1) of the TPC);<sup>6</sup>
- facilitation of the use of drugs (article 190 of the TPC);
- provision of dangerous substances for health (article 194 of the TPC);<sup>8</sup>
- obscenity (article 226 of the TPC);<sup>9</sup>
- prostitution (article 227 of the TPC);<sup>10</sup>
- gambling (article 228 of the TPC); 11 and
- crimes committed against Atatürk (Law No. 5816, dated 25/7/1951). 12

Article 8 blocking provisions were extended in January 2008 and are also applicable to websites facilitating unlicensed or illegal betting on football and other sports. Government approved sites or

<sup>&</sup>lt;sup>5</sup> Article 8(1)(a)(1).

<sup>&</sup>lt;sup>6</sup> Article 8(1)(a)(2).

<sup>&</sup>lt;sup>7</sup> Article 8(1)(a)(3).

<sup>&</sup>lt;sup>8</sup> Article 8(1)(a)(4).

<sup>&</sup>lt;sup>9</sup> Article 8(1)(a)(5).

<sup>&</sup>lt;sup>10</sup> Article 8(1)(a)(6).

<sup>&</sup>lt;sup>11</sup> Article 8(1)(a)(7).

<sup>&</sup>lt;sup>12</sup> Article 8(1)(b).

systems are excluded from this provision. Additionally, websites that enable users to play games of chance via the Internet, which are based outside the Turkish jurisdiction and lack valid permission from the Turkish authorities, are also susceptible to blocking.<sup>13</sup>

Article 8 provides that **both courts of law and an administrative body**, namely, the Telecommunications Communication Presidency ("TIB"), **can issue blocking orders**. Websites that carry content in breach of article 8 can be taken down if hosted in Turkey, or blocked and filtered through Internet access and service providers if hosted abroad subject to a court decision or subject to an administrative decision issued by the TIB. Once notified, the Internet service providers and hosting providers are required to block/remove content within 4 hours of receipt of the order through TIB.<sup>14</sup>

Under article 8A, which was added to Law No. 5651 in April 2015, access to content can be restricted for the protection of life and property, national security and public order, prevention of crime or for the protection of public health. Compared to the other blocking provisions provided in Law 5651, under article 8A, removal or blocking of such content may be requested by the Prime Ministry Minister and/or relevant ministries ("executive decision") in cases of emergency, in addition to judges issuing such decisions. Once a decision or request is issued, the TIB then would ask the Internet service providers and hosting companies to block and/or remove such content within 4 hours.

Originally, under article 9, a notice based liability for violations of individual rights (including but not limited to the protection of the reputation or rights of others) was provided and individuals could ask content and hosting providers as well as Criminal Courts of Peace to take down content that violated individual rights. The original article 9 provision did not provide for blocking access to such content. However, in February 2014, Law No. 5651 was amended and in its amended version, article 9 includes, in addition (rather than if removal is not possible) to existing notice and take-down provisions for violations of individual rights, URL based blocking orders to be issued by Criminal Judgeships of Peace (single judge) for alleged violations of individual rights. In exceptional cases and when necessary, the Judge may also decide to issue a blocking order for the whole website if the URL based restriction is not sufficient to remedy the alleged individual violation. The blocking decision would be notified to the Association of Access Providers<sup>15</sup> which will then notify all access and Internet service providers. Access providers are then compelled by law to comply with the blocking order of the Judge within 4 hours of notification. In practice, social media platform postings including individual Twitter, Facebook and YouTube accounts and postings may be the subject of such URL based blocking orders to be issued by the Criminal Judgeships of Peace.

Article 9A, which was added to Law No. 5651 in February 2014, includes a new blocking measure in relation to individual privacy violations. According to this new provision, individuals and legal entities who claim that their privacy has been violated through the Internet may apply directly to the TIB to request that access to such content is blocked. Individuals and legal entities are required to provide detailed information with regards to the alleged privacy violation including the exact URL for the violation as well as detailed explanation of the violation. Upon issuing the blocking decision the TIB directly notifies the Association of Access Providers on the matter of the request and the access providers are required to comply with the TIB issued blocking order within 4 hours. The TIB issued blocking order will be URL based and will only involve the exact location of the allegedly infringing content. Individuals and legal entities who claim that their privacy has been violated are

Law Amending Some Acts to Harmonise Criminal Law No 5728, Article 256. Official Gazette, 23.1.2008, No. 26781.

<sup>&</sup>lt;sup>14</sup> Article 8(5).

Established by Article 6A, Law No. 5651 in February 2014.

then required to apply to a Criminal Judgeship of Peace within 24 hours and obtain a Judge-issued blocking order for the content complained of.

All of the above mentioned Law No. 5651 provisions include fast-track blocking procedures. However, a similar fast-track appeal mechanism is not provided by law. Standard appeal procedures subject to the Criminal Procedural Act (Law No. 5271) (allowing appeal within seven days) is applicable for Law No. 5651 blocking provisions and appeal Judges (also at the Criminal Judgeship of Peace level) are not required to decide within a certain period of time by law. Furthermore, in most cases content providers, website owners or users of social media platforms are not notified about the blocking decisions involving themselves even though article 35(2) of the Criminal Procedural Act requires such decisions to be notified to the affected parties. Therefore, in most instances, the blocking authority or the reasons behind a blocking decision remains unknown. Similarly, almost all blocking decisions lack judicial reasoning as to why a certain website, particular URL or social media posting is subjected to blocking decision. That is why the implementation and application of Law No. 5651 provisions has been controversial and triggered litigation at both the European Court of Human Rights and Constitutional Court levels in the last few years.

In December 2012, in *Ahmet Yıldırım v. Turkey* (no. 3111/10), the European Court of Human Rights unanimously held that there had been an interference with the applicant's freedom of expression and a violation of the right safeguarded under article 10 of the Convention. The application involved a Court decision which required complete access blocking to the Google Sites platform from Turkey. A Criminal Court in Denizli issued its decision by relying on article 8(1)(b) of Law No. 5651 on the allegation that some pages included content which violated the provisions of the Law on crimes committed against Atatürk. However, the decision caused collateral damage and the applicant's website hosted by the Google Sites platform was also blocked because of the total access ban ordered by the Court. The European Court concluded that **article 8** of Law No. 5651, which is the basis of the interference (the blocking measure), did not satisfy the requirements under the Convention and the case law of the European Court in terms of the "quality of law" principle prescribing such interference. The European Court also held that the judicial-review procedures concerning the access blocking of Internet sites were insufficient to meet the criteria for avoiding abuse, as **domestic law did not provide for any safeguards to ensure that a blocking order in respect of a specific website was not used as a means of blocking access in general**.

Google Sites was not the only Internet platform for which access blocking becoming a legal dispute at the European Court of Human Rights level. Three separate applications were made with regards to YouTube access blocking, which lasted nearly 2.5 years between May 2008 - October 2010, subject to a court ordered blocking decision relying on article 8(1)(b) of Law No. 5651. The applicants argued that blocking and censorship of the Google owned YouTube platform and website was a significant democratic deficit in Turkey. On 01 December, 2015, the European Court, in the case of Cengiz and Others v. Turkey, found a violation of Article 10 concerning the blocking of access to YouTube from Turkey from 5 May 2008 until 30 October 2010. 16 The decision is very important for establishing rights to Internet users as this was a user based application. The Court accepted that YouTube had been an important means by which the applicants could exercise their right to receive and impart information or ideas and that they could legitimately claim to have been affected by the blocking order even though they had not been directly targeted by it. The Court also noted that usergenerated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression. Within this context, the Court also noted that political information ignored by the mainstream media have often been disclosed through YouTube, which allowed the emergence of citizen journalism.

<sup>&</sup>lt;sup>16</sup> Cengiz and Others v. Turkey, Application Nos. 48226/10 and 14027/11, judgment of 01 December 2015, 01 March 2016 (final).

The Court by reference to its previous decision of *Ahmet Yıldırım v. Turkey* stated that Law no. 5651 did not authorize the blocking of access to an entire Internet site because of some of its contents. According to the Court, under section 8(1), a blocking order could only be imposed on a specific publication where there were grounds for suspecting an offence. It therefore emerged that in the YouTube case there had been no legislative provision allowing the Ankara Criminal Court of First Instance to impose a blanket blocking order on access to YouTube. The Court, finding a violation of Article 10, concluded that the interference had not satisfied the condition of lawfulness required by the Convention and that the applicants had not enjoyed a sufficient degree of protection.

More recently, with an administrative decision of the TIB, access to the Twitter platform was blocked from Turkey on 21 March 2014, prior to an important local election that took place on 30 March 2014. With the TIB issued blocking decision, the government aimed to prevent the circulation of graft allegations before the local elections. An individual application was made to the Constitutional Court by two law professors<sup>17</sup> to overturn the blocking decision on 24 March 2014. The application was made without exhausting available national legal remedies and the applicants asked for priority treatment as well as an injunction from the Constitutional Court, arguing that this was a continuing violation case and the TIB lacked authority to issue a decision to completely block access to the social media platform. The Second Section of the Constitutional Court issued a historic unanimous decision<sup>18</sup> on 2 April 2014, stating that blocking access to the Twitter platform was clearly unlawful and constituted a grave intervention on the freedom of expression of all users of social media platforms. According to the Constitutional Court the complete blocking of access to the Twitter platform was not only a far-reaching measure but also had no legal basis. Therefore, the Court ordered access blocking to be lifted immediately.

Similarly, access to the YouTube platform was blocked from Turkey on 27 March 2014. Several individual applications were made to the Constitutional Court immediately to lift the ban. The General Assembly of the Constitutional Court, with a 14-2 majority decision, ordered access blocking to be lifted immediately on 29 May 2014. The Constitutional Court concurred with the findings of the European Court in Ahmet Yıldırım v. Turkey that the provisions of Law No. 5651 did not meet the requirement of foreseeability and were not clear in terms of scope and substance in setting out the procedure for blocking access to websites. According to the Constitutional Court, in both cases, blocking access to the Twitter and YouTube platforms were not based on a domestic court decision and the reasons provided in the TIB's administrative decisions for blocking access did not fall within the scope of article 8 of Law No. 5651. Therefore, TIB's decisions to block access to these two platforms were clearly unlawful.

The Law No 5651 was further amended by article 127 of Law No. 6552 in September 2014 to provide further administrative blocking powers to the head of TIB with regards to national security, for the protection of public order and prevention of crime. Article 8(16) of Law No. 5651 was annulled by the Constitutional Court in early October 2014. Subsequently, the government amended the law yet again and article 8A was added to Law No. 5651.

Furthermore, in April 2015, an individual application which requested the annulment of article 8A was lodged with the Constitutional Court. In addition to this application, the daily newspaper

By Yaman Akdeniz of Istanbul Bilgi University and Kerem Altıparmak of Ankara University.

Yaman Akdeniz and others, Application No: 2014/3986, 2/4/2014, Judgment of the Second Section of the Constitutional Court.

Youtube Llc Corporation Company and others (Plenary), Application No: 2014/4705, 29/5/2014, Judgment of the Constitutional Court.

<sup>&</sup>lt;sup>20</sup> Constitutional Court, General Assembly decision no 2014/151, date 2.10.2014.

Cumhuriyet published images of weapons carried by the National Intelligence Organization ("MIT") trucks to extremists fighting the regime of President Bashar al-Assad in Syria on its front page and on its website. Istanbul 8<sup>th</sup> Criminal Judgeship of Peace issued a URL based blocking order by relying on article 8A of Law No. 5651.<sup>21</sup> Appeals against the blocking order were rejected by the Istanbul 9<sup>th</sup> Criminal Judgeship of Peace without any reasoning. Subsequently, applications were made to the Constitutional Court. Subsequent to the General Elections of June 2015, an escalation of violence (predominately in the south-east of the country) occurred. This led to the breakdown of solution process negotiations between the Kurds and the government, resulting in an end to a two-year ceasefire.<sup>22</sup> During this conflict, on the request of the Prime Ministry, initially the TIB and subsequently a Criminal Judgeship of Peace at Gölbaşı (Ankara) issued several article 8A based orders to block access to several Kurdish and left-wing news websites as well as several Twitter accounts associated with Kurdish journalists and activists. 23 The Judge cited in all decisions the protection of national security and prevention of public order. Some decisions referred to protection of life and property and other more recent cases referred to "glorification of terrorism" and "incitement to violence and commitment of crime" even though these reasons are not included in the wording of article 8A. The blocked news websites include Rudaw, BasNews, Dicle News Agency ("DİHA") which was blocked 35 times, ANHA, daily Özgür Gündem, daily Azadiya Welat, Yüksekova Haber, Sendika.Org (was blocked by 10 separate decisions) and RojNews among others. Several appeals against these blocking orders were rejected. Subsequently, more than 35 individual applications were made to the Constitutional Court. However, as at the date of writing, the Constitutional Court is yet to assess these applications.

So far as case-law related to article 9 of Law No. 5651 is concerned, over 3,000 blocking decisions involving over 16,500 URLs were issued by the Criminal Judgeships of Peace during 2014 only. <sup>24</sup> Out of all these decisions, more than 700 of them are related to Twitter and more than 200 are related to YouTube. Ahmet Davutoğlu, the PM of Turkey requested around 100 blocking decisions and Recep Tayyip Erdoğan, the President of Turkey requested around 50 decisions as of this writing.

Furthermore, access to intellectual property infringements including piracy related content can be blocked subject to the provisions of supplemental article 4 of Law No. 5846 on "Intellectual & Artistic Works". This particular measure, which was introduced in March 2004, provides a two-stage approach. Initially, the law requires the hosting companies, content providers, or access providers to take down the infringing article from their servers upon "notice" given to them by the right holders. The providers need to take action within 72 hours. If the allegedly infringing content is not taken down or there is no response from the providers, the right holders may ask a public prosecutor to provide for a blocking order, which would be executed within 72 hours. This legal

Decision no 2015/1330 D.İş. dated 29.05.2015.

Tim Arango, "As Turkey Targets Militants, War Grips Kurdish Lands Once Again," The New York Times, 24 August, 2015, at http://www.nytimes.com/2015/08/25/world/europe/as-turkey-targets-militants-war-grips-kurdish-lands-once-again.html.

In total, 50 separate "copy-cat" decisions were issued by the Gölbaşı Judge and 1537 Internet addresses including websites, links to newspaper stories, Twitter accounts and individual tweets, Facebook content as well as YouTube videos were blocked between July and end of December 2015. The Gölbaşı decision no. are: 2015/646, 2015/647, 2015/648, 2015/650, 2015/662, 2015/672, 2015/682, 2015/691, 2015/705, 2015/710, 2015/713, 2015/720, 2015/723, 2015/728, 2015/751, 2015/759, 2015/763, 2015/765, 2015/769, 2015/771, 2015/774, 2015/779, 2015/792, 2015/810, 2015/828, 2015/837, 2015/839, 2015/840, 2015/845, 2015/860, 2015/861, 2015/878, 2015/887, 2015/891, 2015/897, 2015/898, 2015/899, 2015/902, 2015/903, 2015/930, 2015/931, 2015/947, 2015/955, 2015/972, 2015/1003, 2015/1012, 2015/1015, 2015/1021, 2015/1169, 2015/1197.

See Diken, "Bir yıl içinde tam 3 bin 94 mahkeme kararıyla 16 bin 600 'adres' hakkında işlem yapıldı!" 04.03.2015, at http://www.diken.com.tr/bir-yilda-tam-3-bin-94-mahkeme-karariyla-16-bin-600-adres-hakkında-islem-yapıldı/.

remedy is therefore predominantly issued with regards to websites related to piracy and IP infringements. In most cases, websites such as the Pirate Bay are indefinitely blocked from Turkey by reference to this provision. However, these provisions have also been used to block access to popular social media platforms such as Blogspot, Myspace, Last.fm and Scribd in the past few years and Last.fm remains currently blocked from Turkey.

Access blocking involving Last.fm and Myspace on the grounds that these two websites allegedly streamed music without respecting copyright legislation was taken to the European Court of Human Rights by a law professor as a user of the Last.fm and Myspace websites, complaining in particular of a violation of his freedom of expression. In its decision on admissibility, in the case of *Akdeniz v. Turkey* (no. 20877/10),<sup>25</sup> the European Court declared the application **inadmissible** (incompatible *ratione personae*), finding that the applicant could not claim to be a "victim" in the sense of article 34 (right of individual application) of the Convention.<sup>26</sup> While stressing that the rights of Internet users are of paramount importance, the Court nevertheless noted that the two music streaming websites had been blocked because they operated in breach of copyright law. As a user of these websites, the applicant had benefited from their services and he had only been deprived of "one way among others of listening to music". The Court further observed that the applicant had at his disposal many means to access to a range of musical works, without thereby contravening the rules governing copyright.<sup>27</sup> Despite this decision, it should be emphasized that there was no criminal investigation or prosecution with regards to the alleged allegations involving Last.fm or Myspace.

In terms of filtering activities, Internet cafes and other mass use providers are required to deploy and use filtering tools approved by the Telecommunications Communication Presidency ("TIB"). Under the *Regulations Governing the Mass Use Providers*, <sup>28</sup> providers are also required to record daily the accuracy, security, and integrity of the retained data using the software provided by the TIB and to keep this information for one year. <sup>29</sup> The TIB is responsible to determine the minimum criteria for filtering programs and the procedure that will be followed by Internet cafes and other mass use providers to install filtering programs. <sup>30</sup> According to the above mentioned regulations, all mass use providers are required to use one of the filtering programs approved by the TIB. <sup>31</sup> Approved programs are published on the TIB's website. <sup>32</sup> The TIB criteria for filtering is not made public, nor is there any official indication on what is filtered out. In 2011, news reports suggested that over one million websites are filtered through Internet cafes. <sup>33</sup> The filter blacklist includes, in addition to so-called "harmful websites", websites of a number of associations, NGOs' and Turkish companies with .com.tr domain names. Furthermore, the blacklist reportedly included websites of model agencies, radio stations, and news portals. The Wikipedia entry for "Kurdish people" is also among the filtered pages.

Decision of 1 March 2014 (decision on the admissibility).

However, the Court should have regard to the fact that the applicant was a party to the domestic proceedings (see *Micallef v. Malta* [GC], no. 17056/06, § 48, ECHR 2009). In other words, the status of the applicant in domestic law should have been taken into consideration.

As stated in *Donald Ashby and others v. France* (No. 36769 / 08, § 39, 10 January 2013), the Court considers that State's margin of appreciation is wider in commercial speech.

Published on 01 November 2007 on the Official Gazette, No. 26687.

<sup>&</sup>lt;sup>29</sup> Article 5(1)(e).

<sup>&</sup>lt;sup>30</sup> See Law No. 5651, article 10 (4)(ç) and (e).

Regulations 2, article 5(1)(c).

See <a href="http://www.tib.gov.tr/onayli\_filtreleme\_yazilimlari.html">http://www.tib.gov.tr/onayli\_filtreleme\_yazilimlari.html</a>.

Milliyet, "There is no Internet Censorship; however one-million websites are banned," 23.05.2011, at <a href="http://privacy.cyber-rights.org.tr/?p=1466">http://privacy.cyber-rights.org.tr/?p=1466</a>>.

Furthermore, a country wide optional filtering system for home users was launched with a decision of the Information Technologies and Communication Board ("BTK") on 24 August 2011. ISPs are compelled to offer the filtering service to their customers and the filtering database and profiles are controlled and maintained by the government authority.

The filtering lists for each profile, including the domain names, IP addresses, port numbers and/or web proxy addresses, will be provided by BTK to the access and Internet service providers. Furthermore, under article 11, the access and Internet service providers are required to prevent filter circumvention methods<sup>34</sup>, used by users for deactivating filters. Access and Internet service providers are also required to periodically report any filter circumvention activities to BTK. The filtering system became operational on 22 November 2011 and it includes two optional profiles, namely, the family and child profiles. Despite being operational for almost four years, there is little publicly available information about usage as well as criteria for filtering. The BTK decision and the filtering policy is currently subject to two legal challenges at the Council of State, which is the highest administrative court in Turkey.<sup>35</sup>

### 2.2. Take-down/removal of illegal Internet content

Content and hosting providers may be required to take down content subject to the provisions of Law No. 5651. **Content providers** are regulated through article 4 of Law No. 5651 and this provides that content providers are **responsible for all the content that they share through the Internet**. However, content providers are **not liable for third party content that they link to**. <sup>36</sup> According to article 4(2), if it can be understood from the presentation that the content provider adopts the content as its own or aims to deliberately make the content reachable, the content provider can be held responsible according to the general principles of law. Content providers may be served with article 8 or article 8A administrative orders or court decisions through the TIB.

As mentioned previously, article 8 removal/blocking criteria is based on protection of children from harmful content and the "catalogue crimes" under article 8 thus include encouragement and incitement of suicide (Article 84 of the Turkish Penal Code), sexual exploitation and abuse of children (Article 103(1) of the TPC), facilitation of the use of drugs (Article 190 of the TPC), provision of dangerous substances for health (Article 194 of the TPC), obscenity (Article 226 of the TPC), prostitution (Article 227 of the TPC), gambling (Article 228 of the TPC), and crimes committed against Atatürk (Law No. 5816, dated 25/7/1951). On the other hand, subject to article 8A, content involving protection of life and property, national security and public order, prevention of crime or the protection of public health can be ordered for removal/blocking.

Equally, content providers may be served with an article 9 notice from a person or company claiming violations of individual rights or they may be served a court issued article 9 removal/blocking decision. Content providers are required by article 9(2) to respond to violation of individual rights requests within 24 hours. Furthermore, non-compliance of court issued article 9 removal/blocking

See generally How to Bypass Internet Censorship, FLOSS Manuals, 2<sup>nd</sup> Edition, 2011, at <a href="https://www.howtobypassinternetcensorship.org/">https://www.howtobypassinternetcensorship.org/</a>.

The first case was initiated by IPS Communication Foundation which owns the alternative media website Bianet at the Council of State level (10. Division, 2011/5435, commenced on 10.04.2011). The second case has been initiated by the Alternatif Bilişim Derneği (Alternative Information Technologies Association), a Turkish NGO on 04 November 2011 at the Council of State level. As in the case of Bianet, AITA requested a stay of execution order and the annulment of the 24 August 2011 decision from the Council of State. Both cases are on-going as of this writing.

<sup>&</sup>lt;sup>36</sup> Article 4(2).

decisions can trigger administrative fines between 500 to 3000 days fines, converting into up to 30,0000 TLs (approx. 95,000EUR). Non-compliance with article 8A orders or decisions can trigger an administrative fine between 50,000TRY (approx. 15,000EUR) and 500,000TRY (approx. 151,000EUR) for content providers.<sup>37</sup>

In terms of hosting provider liability, article 5 of Law No. 5651 introduced a notice-based liability system and the provision states that there is no general obligation to monitor the information which hosting companies store, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity.<sup>38</sup> This provision is consistent with article 15 of the EU E-Commerce Directive. However, subject to article 5(2) hosting companies are obliged to take down illegal or infringing content once notified. Notices can be sent through the TIB with regard to article 8 or 8A related administrative orders or court decisions. Similarly, as in the case of content providers, hosting companies may be served with an article 9 notice by a person or company claiming violations of individual rights, or they may be served a court issued article 9 removal/blocking decision. As in the case of content providers, hosting providers are also required by article 9(2) to respond to violation of individual rights requests within 24hrs. Hosting providers are also required to retain traffic data (communication data) in relation to their hosting activities for between 1 and 2 years.<sup>39</sup> In case of non-compliance with article 5 requirements, administrative fines will be applied between 10,000TRY (approx. 3,000 EUR) and 100,000TRY (approx. 30,000 EUR). 40 Furthermore, noncompliance with court issued article 8 or 9 removal/blocking decisions can trigger administrative fines for hosting providers between 500 to 3,000 days fines, converting to up to 30,0000 TRY (95,000 EUR). Finally, non-compliance with article 8A orders or decisions can trigger an administrative fine between 50,000TRY (approx. 15,000EUR) and 500,000TRY (approx. 151,000EUR) for the hosting providers as in the case of content providers.<sup>41</sup>

In terms of notification of content and hosting providers, a notification process is provided by article 3(3) of Law No. 5651. Those who carry out activities falling within the scope of Law No. 5651 can be notified via e-mail and other communication means gathered from the content and hosting providers' Internet websites, IP address, domain name and other similar sources.

In practice, subject to the hosting providers related provisions of Law No. 5651, in addition to Turkish content and hosting providers, social media platforms such as Facebook, Twitter, YouTube and Google are regularly notified about removal and blocking orders and decisions through their legal representatives based in Turkey. In 2014, Facebook removed 5517 pieces of content from its platform subject to Law No. 5651 related orders. Twitter, removed or withheld 2003 individual tweets and 79 accounts from Turkey during 2014. When Twitter's 2015 transparency report is assessed, it is revealed that the company has received 928 court ordered removal requests worldwide during 2015. 858 of these requests, therefore, the majority came from Turkey. Furthermore, there were a total of 4692 other removal requests from government agencies, the police etc. during 2015. Of these, majority with 2071 requests came from Turkey. Within the same period Twitter received requests to close down or withhold a total of 14.686 accounts. Of these, majority with 10.070 requests came from Turkey. In terms of accounts withheld, Twitter withheld a

Article 8A(5).

<sup>&</sup>lt;sup>38</sup> Article 5(1).

Article 5(3). Hosting providers will also be required to provide the accuracy, integrity and secrecy of the information requested by the Presidency (the TIB) and should also comply with the required measures that are requested by the Presidency (Article 5(5)).

<sup>&</sup>lt;sup>40</sup> Article 5(6).

Article 8A(5).

See generally https://govtrequests.facebook.com/.

See generally https://transparency.twitter.com/

total of 590 accounts during 2015. Of these, majority with 539 accounts were from Turkey. Finally, in terms of number of tweets withheld, Twitter withheld a total of 4890 tweets worldwide during 2015. Of these, the majority with 4670 were from Turkey.

Official statistics for articles 8, 8A, 9 and 9A related administrative orders or court decisions for removal and blocking of Internet content are not published by TIB or by the Association of Internet Access Providers. As mentioned previously, over 3,000 removal/blocking decisions involving over 16,500 URLs were issued by the Criminal Judgeships of Peace in relation article 9 of Law No. 5651 during 2014 only.<sup>44</sup> A majority of these decisions involve social media platforms. However, a breakdown of these decisions is not available.<sup>45</sup>

### 3. Procedural Aspects

In its current version, Law No. 5651 includes four separate blocking measures through articles 8 (protection of children from harmful content), 8A (protection of national security, public order, protection of life and property as well as protection of public health and prevention of crime), 9 (violation of individual rights) and 9A (violation of privacy of individuals). In terms of procedural matters, all these provisions involve separate and different legal procedures for removal and/or blocking decisions. These procedures will be assessed separately below.

Subject to **article 8** provisions, blocking orders can be issued by a judge or by an administrative body, the Telecommunications Communication Presidency ("TIB"). Judicial blocking orders can be issued by a judge during a preliminary investigation and by the courts during trial. During preliminary investigation the public prosecutor can also issue a blocking order through a precautionary injunction if a delay could be prejudicial to the investigation. Article 8(2) states that the public prosecutor must take his injunction decision to a judge within 24 hours and the judge needs to then decide on the matter within 24 hours. The precautionary injunction would be immediately lifted by the public prosecutor and access to the website in question restored, if the decision is not approved within the said time period.

Furthermore, if during preliminary investigation it is decided that no prosecution will take place, the blocking order issued through a precautionary injunction would be automatically removed.<sup>47</sup> Similarly, if a provider is found not guilty, the blocking order issued by the court would be removed.<sup>48</sup> Finally, if the content deemed to be unlawful and thereby the subject matter of the blocking order is removed from the Internet, the blocking order would be then removed by the Public Prosecutor during investigation and by the court during prosecution.<sup>49</sup>

Subject to article 8(2), objections to the blocking decision rendered as a precautionary measure should be brought to the Court or Judge that issued the blocking order, pursuant to the Criminal Procedure Act (Law No. 5271) by the interested parties. However, identification of an interested party is not clearly specified by law. Usually, an interested party would be the owner of a website, or the author of a blog but in practice user based applications have also been made to the courts to

See Diken, "Bir yıl içinde tam 3 bin 94 mahkeme kararıyla 16 bin 600 'adres' hakkında işlem yapıldı!" 04.03.2015, at http://www.diken.com.tr/bir-yilda-tam-3-bin-94-mahkeme-karariyla-16-bin-600-adres-hakkında-islem-yapıldı/.

<sup>&</sup>lt;sup>45</sup> Case-law involving social media platforms is described and discussed in the blocking section.

<sup>&</sup>lt;sup>46</sup> Article 8(2).

<sup>&</sup>lt;sup>47</sup> Article 8(7).

<sup>&</sup>lt;sup>48</sup> Article 8(8).

<sup>&</sup>lt;sup>49</sup> Article 8(9).

challenge blocking orders.<sup>50</sup> Despite, the availability of these general measures for challenging blocking orders, the procedure followed under Law No. 5651 does not give an opportunity to the content providers to have knowledge about the charges or the removal or blocking orders and decisions. The law does not require the authorities to inform the accused about the article 8(2) procedure. No other procedural guarantee to counterbalance this deficiency is envisaged either. Although an objection can be made pursuant to the general appeal provisions of the Criminal Procedural Act, an interested party that wants to invoke this legal provision will not be able to know the details of such an accusation or the details of the blocking decision. Content providers are generally caught by surprise when they learn that their websites, social media accounts or postings are inaccessible from Turkey.

In terms of **article 8A** blocking provisions, if the removal or blocking decision is requested by the Prime Ministry or the relevant ministries ("executive decision"), the TIB would notify the content, hosting and access providers about its administrative removal or blocking decision. The providers are required to remove or block content within 4 hours of notification. The TIB is then required to obtain judicial approval from a Judge within 24 hours. Article 32 Judges are required to issue their decisions within 48 hours. Article 34 requires the removal or blocking decisions to be URL based. However, when necessary and technically not feasible to issue a URL based blocking order, access to a whole domain may be blocked by the TIB and Judges. The law also requires the TIB to report the alleged offenders to the relevant Public Prosecutors' Office for criminal investigation. Content, hosting and access providers may be fined in the case of non-compliance with onerous administrative fines between 50,000TRY (approx. 15,000EUR) and 500,000TRY (approx. 151,000EUR) for the hosting providers as in the case of content providers. As in the case of article 8, there is no fast-track appeal mechanism and interested parties may appeal against article 8A related blocking decisions pursuant to the general appeal provisions of the Criminal Procedure Act. In practice, article 8A blocking decisions are not notified to content providers and website owners.

Within the scope of **article 9**, in addition to existing notice and takedown provisions for violations of individual rights, this measure also includes URL based blocking orders to be issued by a Judge at a Criminal Judgeship of Peace in relation to the allegedly infringing content. Individuals or companies claiming violations of individual rights may notify content and/or hosting providers and ask for the removal of allegedly infringing content. Content and hosting providers are also required by article 9(2) to respond to violation of individual rights requests within 24 hours. Individuals or companies claiming violations of individual rights may also apply directly to a Criminal Judgeship of Peace and ask the Judge to issue a blocking decision. <sup>57</sup> The Judge is required by law to issue a decision within 24 hours. <sup>58</sup> Primarily, the Judge is required to consider a URL based blocking decision concentrating on the allegedly infringing content. However, in exceptional and necessary cases, the Judge may decide to issue a blocking order for the whole website if the URL based restriction is not sufficient to remedy the alleged violation. Judge issued orders will be sent directly to the Association of Access Providers for the execution of the order.

Note the Twitter decision of the Second Section of the Constitutional Court: *Yaman Akdeniz and others*, Application No: 2014/3986, 2/4/2014 and YouTube decision of the General Assembly: *Youtube Llc Corporation Company and others* (Plenary), Application No: 2014/4705, 29/5/2014.

Article 8A(1).

<sup>&</sup>lt;sup>52</sup> Article 8A(2).

Article 8A(2).

Article 8A(3).

<sup>55</sup> Article 8A(4).

<sup>&</sup>lt;sup>56</sup> Article 8A(5).

<sup>&</sup>lt;sup>57</sup> Article 9(1).

<sup>&</sup>lt;sup>58</sup> Article 9(6).

With the amendments made to Law No. 5651 in February 2014, an Association of Access Providers was set up.<sup>59</sup> The main purpose of the Association is to centrally ensure compliance with blocking decisions that are outside the scope of Article 8.<sup>60</sup> The Association is recognized as a private legal entity and the headquarters of the Association is based in Ankara. The by-laws of the Association are subject to approval of the Information and Communication Technologies Authority. The Association is composed of all Internet service providers (within the ambit of the Electronic Communication Law No. 5809) and other corporations that provide Internet access from within Turkey. Membership to the Association is compulsory. Access providers who do not become members of the Association will not be able to provide access services within Turkey.

Although article 9 provides a fast-track mechanism for blocking access to Internet content by the Criminal Judgeships of Peace, a similar fast-track appeal mechanism is not envisaged by law. Interested parties, content providers or website owners can only challenge these decisions pursuant to the general appeal provisions of the Criminal Procedure Act. In practice, the majority of article 9 blocking decisions are not notified to content providers and website owners.

If content that is subject to a removal or blocking order is removed by the time it is notified to the Association, the decision of the judge will be void. Otherwise, access providers should comply with the order of the Judge within 4hrs of notification by the Association.<sup>61</sup> Just fines will be applied in case of violation of the above mentioned requirements. As it is in Article 8 this fine can be from 500 days to 3,000 days which means that it can be up to 300,000 TLs (90,000 EUR).

In practice, individuals or companies apply directly to Criminal Judgeships of Peace requesting blocking decisions rather than going after content and hosting providers for the removal of alleged violations of their individual rights.

Finally, with regard to **article 9A** blocking procedure, individuals and legal entities who claim that their privacy has been violated through the Internet may request the blocking of access to such content by applying directly to the TIB. Individuals and legal entities are required to provide detailed information with regard to the alleged privacy violation including the exact URL for the violation as well as a detailed explanation of the violation. Upon issuing the blocking decision the TIB directly notifies the Association of Access Providers on the matter of the request and the access providers should comply with the TIB issued blocking order within 4 hours of notification. The TIB issued blocking order will be URL based and will only involve the exact location of the allegedly infringing content. Individuals and legal entities who claim that their privacy has been violated are then required to apply to a Judge at a Criminal Judgeship of Peace within 24 hours. The judge is required to issue a decision within 48 hours. In case of no decision being taken by a judge or if the application is rejected, the administrative blocking decision issued by the TIB would be nullified.

Furthermore, if any possible delay is deemed to result in adverse consequences with regards to protection of privacy or rights and freedoms of others then the Director of the TIB can ex officio issue a blocking order. <sup>65</sup> In this case the TIB would execute the blocking decision directly rather than

<sup>59</sup> Article 6A.

Article 8A was added to Law No. 5651 subsequent to the formation of the Association of Access Providers. As explained in this chapter article 8A decisions are not notified to the Association.

<sup>&</sup>lt;sup>61</sup> Article 9(8).

Article 9A(3).

Article 9A(5).

<sup>64</sup> Article 9A(5).

<sup>&</sup>lt;sup>65</sup> Article 9A(8).

notifying the Association of Access Providers.<sup>66</sup> The TIB is then required to submit the ex officio blocking decision for review by a judge at a Criminal Judgeship of Peace within 24 hours.<sup>67</sup> The Judge is required to issue a decision within 48 hours. As in the case of article 9, article 9A provides a fast-track mechanism for blocking access to Internet content by TIB and by the Criminal Judgeships of Peace. However, a similar fast-track appeal mechanism is not envisaged by law. Interested parties, content providers or website owners can only challenge these decisions pursuant to the general appeal provisions of the Criminal Procedure Act. In practice, article 9A blocking decisions are not notified to content providers, website owners or to the Association of Access Providers.

# 4. General Monitoring of Internet

The Telecommunications Communication Presidency ("TIB") is the entity in charge of monitoring Internet content in Turkey. As was previously mentioned in this chapter the Presidency has the authority subject to articles 8, 8A and 9A of Law No. 5651 to issue administrative blocking decisions. Article 10 of Law No. 5651 also establishes the duties and responsibilities of the Presidency. According to article 10(4)(b) the Presidency can monitor the content of publications on the Internet. If it is determined by the Presidency that any crimes that fall within the scope of Law No. 5651 are committed, then the Presidency can take the necessary measures provided by law in order to prevent access to such publications allegedly publishing or distributing unlawful content. The Presidency, by law, can also determine the level, time frame and manner of monitoring of Internet content. Furthermore, the law enables the Presidency to set up a hotline to report allegedly unlawful content as well as establish the necessary technical infrastructure to prevent the commission of catalogue crimes listed in article 8 of Law No. 5651. A hotline to report article 8 catalogue crimes was launched at http://www.ihbarweb.org.tr in November 2007.

The **criteria for assessment** is provided by article 8 of Law No. 5651 and the TIB monitors Internet content with regards to the catalogue crimes provided in article 8. **If the Presidency deems any website in breach of article 8 provisions, then the Presidency issues a domain and IP address based blocking decision**. The Presidency does not publish the official blocking statistics but according to Engelliweb, over 110.000 websites are blocked by the Presidency from Turkey as of this writing.<sup>71</sup> The Presidency's actions have been subject to legal controversy during 2014 as the Presidency blocked access to both Twitter and YouTube by its administrative decisions prior to the local elections of March 2014 as was previously mentioned in this chapter. Both cases were taken to the Constitutional Court, which found that the applicants' rights under Article 26 of the Constitution on freedom of expression have been violated as a result of the administrative act of the Presidency which amounted to a grave interference in the freedom of expression of all users who make use of the Twitter and YouTube social media platforms.<sup>72</sup> According to the Constitutional Court, the interference enabling the blocking of the entire social media platforms lacked a sufficiently clear and precise legal basis.

Article 9A(8).

Article 9A(9).

<sup>&</sup>lt;sup>68</sup> Article 10(4)(b).

<sup>69</sup> Article 10(4)(c).

<sup>&</sup>lt;sup>70</sup> Article 10(4)(d).

<sup>&</sup>lt;sup>71</sup> See http://engelliweb.com/.

See the Twitter decision of the Second Section of the Constitutional Court: *Yaman Akdeniz and others*, Application No: 2014/3986, 2/4/2014 and YouTube decision of the General Assembly: *Youtube Llc Corporation Company and others* (Plenary), Application No: 2014/4705, 29/5/2014.

# 5. Assessment as to the case law of the European Court of Human Rights

In its first access blocking related decision, in *Ahmet Yıldırım v. Turkey*, <sup>73</sup> the European Court, assessed whether the blocking provisions of article 8 of Law No. 5651 meet the requirements of quality of law (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights as well as whether there are any safeguards for the protection of freedom of expression). The European Court of Human Rights, finding a violation of article 10 of the European Convention on Human Rights, held that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework is in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses.

Ahmet Yıldırım v. Turkey<sup>74</sup> involved a court decision to block access to Google Sites, which hosted an Internet site whose owner was facing criminal investigation for insulting the memory of Atatürk. The court issued its blocking decision subject to article 8(1)(b) of Law No. 5651. As a result of the court decision, access to all other sites hosted by Google Sites was also blocked including the applicant's websites hosted on Google Sites. The TIB made it technically impossible to access any content on Google Sites in order to implement the measure ordered by the local court. The measure in question therefore amounted to interference by the public authorities with the applicant's right to freedom of expression. The European Court concluded that article 8 of Law No. 5651, which is the basis of the interference (the blocking measure), did not satisfy the requirements under the Convention and the case law of the Court in terms of the "quality of a law" prescribing such interference. More importantly, the Court stated that the blocking of all access to Google Sites affected the applicant, who owned another website hosted on the same domain. The Court was of the opinion that such a measure substantially restricted the rights of Internet users and had a significant collateral effect, which should have been taken into consideration by the Turkish Court issuing the blocking decision. On this issue, the European Court stated that domestic courts "should have taken into consideration, among other elements, the fact that such a measure, by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect."75

Furthermore, in *Ahmet Yıldırım v. Turkey*, the Court noted that there was no indication that the judges considering the application sought to weigh up the various interests at stake, in particular, by assessing the need to block all access to Google Sites. In the Court's view, this shortcoming was simply a consequence of the wording of article 8 of Law No. 5651 itself, which did not lay down any obligation for the domestic courts to examine whether the wholesale blocking of Google Sites was necessary, having regard to the criteria established and applied by the Court under article 10 of the Convention. Therefore, Law No. 5651 provisions including the new blocking provisions added to this law since the European Court of Human Rights decision does not provide any safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights. In fact, the amended version of the Law No. 5651 also shields the Telecommunications Communications Presidency staff from prosecution if they commit crimes during the exercise of their duties within the TIB. Criminal investigations can only be initiated subject to an authorization from the TIB Director for the TIB staff and from the relevant Minister for the TIB Director. The European Court echoed these criticisms in the case of *Cengiz and Others v. Turkey*,

Ahmet Yıldırım v. Turkey, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

<sup>74</sup> Ibid

Ahmet Yildirim v. Turkey, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final), para. 66.

<sup>76</sup> Ibid.

<sup>&</sup>lt;sup>77</sup> Supplemental Article 1(6).

with regards to the blocking of the YouTube platform from Turkey confirming *Ahmet Yıldırım* and accepting a broader user based application.

Despite the decisions of the European Court of Human Rights, the practice of banning access to websites continues in Turkey and at the time of writing more than 110,000 websites are blocked in Turkey, 35,000 of which were blocked during 2014 and more than 26,000 during 2015. The February 2014 amendments introduced further restrictions that raise major concerns rather than bringing the current law in line with international human rights standards. Following the February 2014 amendments to Law No. 5651, two separate administrative decisions were issued by the TIB to block wholesale access to the websites of Twitter and YouTube platforms on 18 and 27 March 2014 respectively. The fact that these decisions resulted in the complete blocking of access to the websites of Twitter and YouTube platforms is a clear indication that the amended Law No. 5651 is still not in compliance with the European Court's findings in the *Ahmet Yıldırım v. Turkey* decision. In both cases, the Constitutional Court stated that blocking of both Twitter and YouTube constitutes a grave intervention on the freedom of expression of all users of these social media platforms. <sup>78</sup>

In its decision related to the blocking of YouTube, the Constitutional Court stated that

"social media platforms provided by the Internet are indispensable to individuals for expressing, sharing, spreading and communicating information and ideas. It is, therefore, evident that the state and administrative bodies must demonstrate great sensitivity in regulations and practices with regard to social media, since these have become one of the most effective and widespread methods not only for imparting thoughts but also for obtaining information." <sup>79</sup>

Furthermore, the Constitutional Court concurred with the findings of the European Court in *Ahmet Yıldırım v. Turkey* that the provisions of Law No. 5651 did not meet the requirement of foreseeability and were not clear in terms of scope and substance in setting out the procedure for blocking of access to websites.

Additionally, the Constitutional Court, in its YouTube decision, with regards to the Presidency's ex officio blocking power provided by article 8(4) of Law No. 5651 stated that:

"It is understood that there is no provision whatsoever in the Law allowing the administration to block an entire website rather than blocking specific URLs. Furthermore, the Law does not clearly specify which methods of restriction are to be employed by the administration in blocking access (blocking access by domain name, by IP address, blocking access to content, and similar blocking methods). Therefore, it is understood that the scope and limits of the powers conferred on the administration are unforeseeable. In addition, it is unclear whether the authority vested in the judge to block access in multiple stages under Article 9(4) also applies to the administration. For this reason, since the legal basis of the powers conferred on TIB in issuing blocking orders fails to meet the minimum criteria of the principle of being prescribed by law, namely being understandable, clear and precise, it is understood that those powers are indefinite with respect to their scope and limits."

Despite this strong statement, the **Constitutional Court did not go as far as annulling the Presidency's blocking power** under article 8(4) of Law No. 5651.

See the Twitter decision of the Second Section of the Constitutional Court: *Yaman Akdeniz and others*, Application No: 2014/3986, 2/4/2014 and YouTube decision of the General Assembly: *Youtube Llc Corporation Company and others* (Plenary), Application No: 2014/4705, 29/5/2014.

Youtube Llc Corporation Company and others (Plenary), Application No: 2014/4705, 29/5/2014, para 52.

Youtube Llc Corporation Company and others (Plenary), Application No: 2014/4705, 29/5/2014, para63.

Regardless of these significant decisions at the Constitutional Court level, access blocking to Internet content and social media platforms continue erratically and access to Twitter, YouTube and Facebook has been blocked more than once since these decisions were issued during 2015. Therefore, the systemic problem observed by the European Court in Ahmet Yıldırım v. Turkey as well as in Cengiz and Others v. Turkey decisions is continuing, due to vague and disproportionate nature of various blocking provisions of Law No. 5651. More importantly, the Law No. 5651, despite several amendments since the Ahmet Yıldırım decision, 81 does not provide a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression.<sup>82</sup> Without changing or amending article 8, three further blocking measures were introduced through articles 8A, 9 and 9A to Law No. 5651 since Ahmet Yıldırım. Fast-track blocking procedures of Law No. 5651 are not matched by fast-track appeal mechanisms and in practice thousands of blocking decisions are not notified to the content providers, website owners or social media account holders. The whole system is designed to block access to Internet content disregarding any due process mechanisms and concerns for freedom of expression and information. It should be reminded that the European Court found a violation of Article 10 of the Convention in its procedural aspect in circumstances where the scope of the measure restricting freedom of expression was vague, or was motivated by an insufficiently precise reasoning and its application was not subject to adequate judicial review.<sup>83</sup> According to the European Court, a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power especially with regards to restrictions on freedom of expression.<sup>84</sup> Three years apart during which several amendments squeezed into Law No. 5651, Ahmet Yıldırım and Cengiz and Others decisions of the European Court show that nothing has changed much in terms of blocking practices in Turkey.

Finally, it is worth mentioning that the **CoE Committee of Ministers**, during its meeting of September 2014, 85 examined the state of implementation of judgments of the European Court of Human Rights including that of *Ahmet Yıldırım v. Turkey*. In the decision adopted with regards to the execution of the *Ahmet Yıldırım v. Turkey*, the Deputies "considered that the legislative amendments made to Law No. 5651, in February 2014 do not satisfy the foreseeability requirement of the Convention and that **the legislative framework is still not in compliance with the Court's findings in the present case."** More importantly, the Deputies stressed that "these amendments do not respond to the concerns raised by the Court as to the arbitrary effects of decisions on wholesale blocking of access to websites since access to the host websites, Twitter and YouTube, were blocked after these legislative amendments came into force." The Committee of Ministers continues to monitor the *Ahmet Yıldırım v. Turkey* decision with an Enhanced Supervision status. The European Court's YouTube blocking related *Cengiz and Others v. Turkey* decision of December 2015 further confirmed that amendments made since the *Ahmet Yıldırım* decision did not take into account the requirements of ECtHR and rather introduced further restrictions by way of blocking.

Professor Yaman Akdeniz, Faculty of Law, Istanbul Bilgi University

The Law No. 5651 was amended by Law No. 6495 on 12/07/2013, by Law No. 6518 on 06/02/2014, by Law No. 6527 on 26/02/2014, by Law No. 6552 on 10/09/2014 and by Law No 6639 on 27/03/2015.

Note *RTBF v. Belgium*, no. 50084/06, § 114.

Saygılı and Seyman v. Turkey, no <u>51041/99</u>, §§ 24-25, 27 June 2006; and Lombardi Vallauri v. Italy, no 9128/05.

Association Ekin v. France, no. 39288/98, § 58.

<sup>&</sup>lt;sup>85</sup> 1208DH meeting of the Ministers' Deputies, 23-25 September 2014.

<sup>86</sup> Case No. 23, <u>DH-DD(2014)916</u>; <u>DH-DD(2014)161</u>; <u>DH-DD(2014)820</u>.

<sup>&</sup>lt;sup>87</sup> Decision of 25.09.2014, para 2.

<sup>&</sup>lt;sup>88</sup> Decision of 25.09.2014, para 3.

Revised on 03.05.2016 taking into consideration comments from Turkey on this report