



Internet censorship in Turkey

Mustafa Akgül

Computer Technology and Information Systems Department, İhsan Doğramacı Bilkent University, Ankara, Turkey, akgul@bilkent.edu.tr

Melih Kırılidoğ

Computer Engineering Department, Marmara University, Istanbul, Turkey, melihk@marmara.edu.tr

Published on 03 Jun 2015 | DOI: 10.14763/2015.2.366

Abstract: Turkey passed an internet censorship law in 2007 with the declared objective of protecting families and minors (Akdeniz, 2010). It established a unit within the regulator BTK (Information and Communication Technologies Authority) responsible for imposing bans and blocks on websites based on nine catalogue crimes defined by other national laws (Akgül 2008, 2009a, 2009b). As of May 2015, 80,000 websites were banned based on civil code related complaints and intellectual property rights violations, reports the independent website Engelliweb. Blocking decisions rendered by penal courts are enforced even when they are based on grounds other than the nine catalogue crimes - such as terrorism, organised crime and crime against the state. Passed in parliament while ignoring the pleas of NGOs and of the internet sector, the Internet Law No. 5651 has since been used to temporarily ban popular platforms such as Blogger, Last.fm, Vimeo, Wordpress and YouTube. At the same time, some blocking decisions by the courts (e.g., Google and Facebook) were not enforced by the authorities. Since its introduction, the European Court of Human Rights has ruled that Law No. 5651 (Council of Europe, 2011) is against the European Convention on Human Rights (ECHR, 2013). This article provides an overview of internet censorship and its social background in Turkey.

Keywords: Censorship, Freedom of information, Filtering, Internet blockings, Law No. 5651

Article information

Received: 16 Aug 2013 **Reviewed:** 11 Nov 2014 **Published:** 03 Jun 2015

Licence: Creative Commons Attribution 3.0 Germany

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: <http://policyreview.info/articles/analysis/internet-censorship-turkey>

Citation: Akgül, M. & Kırılidoğ, M. (2015). Internet censorship in Turkey. *Internet Policy Review*, 4(2). <https://doi.org/10.14763/2015.2.366>

INTRODUCTION

At the beginning of 2015 the Electronic Frontier Foundation (EFF), an advocacy group that

defends civil liberties in the digital world, wrote in one of its reports that “Turkey has been a bastion of Internet censorship for so long that EFF could write a regular feature called This Week in Turkish Internet Censorship and never run out of content” (Galperin, 2015).

The Turkish Republic was founded in 1923 after the collapse of the Ottoman Empire and it has since adopted a Western-oriented and secular strategy as the main pillars of social policy. In the 2002 elections, the AKP (Justice and Development Party) rose to power and its leader, Recep Tayyip Erdoğan, became the Prime Minister (he further became President on 10 August 2014). Although the AKP officially promised to adhere to secular policy, the ever-increasing role of religion under its rule led to widespread concern among the secular parts of society. Increased intervention in the secular lifestyle such as partial alcohol ban and conversion of the secular education system to a religious one were some of the factors that led to the Gezi uprising in mid-2013 - where millions of demonstrators took to the streets in 79 of Turkey’s 81 provinces. The Gezi events started to prevent the construction of a shopping centre in Gezi Park - one of the last few remaining green areas in Istanbul’s city centre. Although the Gezi uprising was the fiercest environmental struggle to date, discontent and anxiety over the government’s policies constituted the backdrop.

Internet blocking in the country accelerated after the Gezi events. Social media venues like Twitter had proven to be effective in organising demonstrations and disseminating news about the events. Website blocking gained a new momentum after corruption revelations about the highest echelons of the government surfaced between 17 and 25 December 2013. Explicit recordings of corruption transactions were broadcast online. As a result, four cabinet ministers had to resign. During that period, the partial blackout of the mass media, directly or indirectly controlled by the government – sometimes through lucrative bids or unexpected tax fines, was mainly bypassed via Twitter. Hence, the perception of the increased importance of the internet became a leading factor in the acceleration of internet censorship in Turkey.

This article attempts to give an account of internet censorship in Turkey. It provides an exploratory analysis of the nature of censorship and tries to analyse the relationship between censorship and the social conditions at play. Details about the legal issues in blocking decisions can be found in Akdeniz (2010) and Akdeniz and Altıparmak (2008). Due to the fact that censorship in the country became more intense and technically more sophisticated in the last few years, we mainly focus on the 2010s. This article also compares the motivations and methods of other countries’ censorship practices, such as those in place in Iran and China.

PREVIOUS WRITINGS ABOUT INTERNET CENSORSHIP

Censorship stems from the word “censor,” the government officer who had a wide range of responsibilities in the Roman Empire, such as overlooking the population census, public morale and government finances. Hence, the word is closely associated with inspection and auditing. In today’s world, censorship is one of the most commonly used concepts in political and social science. Censorship can take many forms such as political censorship, which aims to prevent dissemination of political and social news or, military censorship, which is usually implemented during war or under martial law. Self-censorship is a subtle form of censorship which implies indirect, rather than direct imposition of censorship on one self (Arsan, 2013). This imposition may either stem from avoiding a possible harm from authorities or assuring the continuation of some form of benefit.

While in the last century censorship was often implemented in print or electronic mass media, the ubiquity of the internet in the last few years resulted in the widespread implementation of internet censorship in many countries. Censorship is usually regarded as an indicator of the position of a country in the authoritarian-democratic continuum and it applies to all sorts of media where news and ideas can be disseminated. Although countries like China, Iran and Turkey are criticised for implementing widespread censorship practices on the internet and other media (Arsan, 2013; Wojcieszak and Smith, 2014; Taneja and Wu, 2014), there are also convincing voices which elaborate the subtle censorship practiced in “democratic” countries (Wright and Breindl, 2013). This kind of censorship may either be practiced by corporate mass media (Herman and Chomsky, 2002) or the state (ACLU, 2005). However, the Snowden revelations showed that surveillance intensifies the problem of censorship, particularly in Western countries, to the extent that self-censorship among US writers has increased after the revelations (PEN America, 2014).

ROAD TO EXTENSIVE INTERNET CENSORSHIP IN TURKEY

Turkey has taken a bold step in 2007 in order to regulate, and to ‘clean’ the internet from undesirable content, which resulted in the censorship of websites. The censored sites ranged from child and adult pornography websites to commonly used platforms such as YouTube, Blogger or Alibaba.com.

Before 2007, sporadic censorship of websites did take place, the first well known one being yolsuzluk.com (Turkish for corruption), which was banned by a decision of the Military Court due to the publication of claims of corruption within the military. Then came the banning of websites related to music files due to complaints by the Turkish Phonographic Industry Society. The ban hit those websites that contained a link to other websites hosting audio files or software for downloading audio files (Seçen, 2006).

Turkey joined the internet in April 1993. As early as 1991, drawing on French legislation, Turkey enacted rudimentary computer related criminal law provisions (Yazıcıoğlu, 2011). In 2000-2001 the then government proposed an amendment to the press code with the provision of treating the “Internet as a subject to Press Code.” In order to operate as press, you need to register with the authorities and send two copies of each print issue to the Public Prosecutor for inspection. The proposal included everything involving online communications. This caused widespread uproar. Upon protests from the public, the amendment was softened and later returned by then President Ahmet Necdet Sezer (formerly head of Constitutional Court, nominated by all parties) to the parliament for revision. Yet, the government insisted and the law was enacted. That was the first law specific to the internet passed by parliament. The main philosophy of the code was to increase the penalties by half, whenever the internet was involved in the commitment of a crime; which was already the rule for the press. Detailed information about the code and reactions to it can be found in Draft RTUK Law (2001), RTUK Law (2001), Inet (2001) and Akgül & Pekşirin (2001).

In 2004, a new penal code was passed, this time including additional provisions on the internet and computer crime. The Penal Procedural Code was consequently renewed but, it did not include any provisions regulating rights and responsibilities of internet actors; mainly internet service providers (ISP). The Ministry of Justice formed a commission in order to prepare an

“Internet law” to accommodate missing parts of criminal law and procedure. The commission started working in early 2006. The committee developing the “Internet law” included members from public institutions, faculty members from law schools and representatives from internet NGOs. It prepared a draft bill named “Law on Network Services and Computer Crimes.” The draft was to be presented to the Prime Minister’s Office (Akgül, 2006).

This could be interpreted as Turkey’s attempt to comply with the Cybercrime Convention. The Budapest Convention on Cybercrime is the first international treaty dealing with internet and computer crime. It was prepared by the Council of Europe, opened to signature in 2001 and came into effect in 2004 (Convention on Cybercrime, 2001). Turkey participated in the preparation of the Cybercrime Convention but chose not to sign it. It is only in 2010 that the government signed on to the Cybercrime Convention. It was finally ratified by parliament in 2014 on insistence of the opposition (Sanal Suçlar Sözleşmesi, 2001).

THE MAKING OF LAW 5651 ABOUT REGULATION OF PUBLICATIONS ON THE INTERNET

As mentioned above, the Justice Ministry Committee for Internet Law prepared a draft entitled “Law on Network Services and Computer Crimes.” A new draft was prepared by the Transportation Ministry with restricted scope. The Justice Ministry draft was published on the website of the Ministry of Justice (Akgül, 2006). It was then opened for comments and contributions and sent to government institutions, with responses collected via official letters. Comments from public institutions and other parties were compiled, and were taken into account. The Justice Ministry Committee evaluated and decided by itself without any public participation.

In the fall of 2006, child abuse and child pornography cases flooded the media. The first Computer Crime Unit was officially established at the Istanbul Police headquarters. It serviced most of the child abuse and child pornography cases that were already available in printed form. The internet pornography issue took such proportions in the media that it looked as if child pornography was one of the most important problems in Turkey. This came across as an orchestrated effort to pass the Internet Censorship Law. Yet, in their assessment of the situation, the Ministers of Interior and of Transportation differed on the magnitude of child pornography in Turkey (Aydilek, 2006).

The Prime Minister asked the Minister of Transportation – rather than the Minister of Justice – to resolve the declared paramount child pornography problem that apparently aimed to introduce broad measures of censorship in Turkey. The Transportation Ministry was responsible for the BTK (Information and Communication Technologies Authority) – the regulatory authority for the telecom sector, while Turkish Telecom is the dominant operator and major ISP.¹ Although a privatised entity, it has an intimate relationship with the state and has an important role in carrying out the practice of censorship in the country.

Although the Ministry of Justice was not happy that it was bypassed, it could not object to the Prime Minister and consequently, lawyers at the Ministry of Transportation prepared what became the “Law for Regulating the Publications on the Internet and Suppression of Crimes Committed on such Publications No. 5651.” The draft of the Transportation Ministry was prepared behind closed doors, and only state institutions were allowed to participate in the preparation process. Government ministers prepared the public opinion by promising a “clean

Internet”, “clean knowledge” and the “protection of children, family and family values” (Sabah, 2007a; Sabah, 2007b). On 29 March 2007 a one-day conference was held in Ankara entitled “Clean Internet”, whose logo was three copies of the letter ‘W’ hanging from a laundry drying string (Sabah, 2007a). The Transportation Minister declared a few times that “Turkey will be a leader in providing a clean and safe Internet. The World will follow our example” (Sabah, 2007a; Sabah, 2007b).

Internet and communication technology related NGOs tried to alert the public, opposition parties, the media and internet users against the intended censorship of the internet. “Defend your Internet!” was the motto of the “İnternette Sahip Çık ... İnternet Yaşamdır” campaign (Internet Kampanyası, n.d.). The draft prepared by the Ministry of **Transportation** was submitted to the parliament. During deliberations of the Justice Committee in parliament, this draft was softened to some extent. The initial draft was more drastic and would have covered all communication media with the aim to monitor, filter and curtail chat and similar services. The draft listed a catalogue of six crimes as defined by the Turkish Penal Code to be banned either by the BTK or by penal courts. This will be explored in detail in the next section. In parliament, the Justice Committee mainly made two additions: i) crimes against the founder of the Republic, Mustafa Kemal Atatürk, were included in the catalogue list, ii) a “Notice and Takedown” clause (TBMM, 2007).

The Justice Committee version passed in parliament upon a 59-minute deliberation with no major opposition on 4 May 2007 (Law 5651, 2007). One opposition MP of the Republican Party, Osman Çoşkunoglu, asserted that ICT-related NGOs were against the Law and suggested that NGO concerns should be dealt with. The Transportation Minister Binali Yıldırım of the AKP stated that they will be taken care of and the law passed quietly. No one talked about the danger of censorship, nor defended freedom of expression, nor again claimed the unconstitutionality of the passed law. The main opposition party, the People Republican Party (CHP), could have brought the Law before the Constitutional Court for annulment, but remained silent. ICT-related NGOs appealed to President Sezer to send the Law back to parliament to be discussed once more, but he did not overturn the decision. Child pornography cases created such an atmosphere that no politician could have adopted a position without the danger of being seen as promoting it.

On 4 May 2007, the Law No. 5651 came into effect. Passing the required secondary regulations took another six months and by the end of November 2007, Law No. 5651 “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” (Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications) was fully in force.

WHAT DID LAW NO. 5651 PROVIDE?

The law provided some definitions and organisational structure, a catalogue of crimes, the legal framework for banning websites and a few procedures. It defined the concepts of information, data, traffic data, publication, internet medium, internet publication, monitoring, access, hosting, access and content providers, and internet usage provider. It classified ISPs as either access providers, host providers, content providers or commercial usage providers; also, it listed their accountability and responsibilities. The Law and secondary regulations requested that access and hosting providers register and acquire a license from the BTK. Commercial usage providers such as internet cafes apply for and get licenses from local authorities. For commercial content providers, a clear listing of contact information and hosting information is required online. There are monetary penalties and invalidation of license if these requirements are not

fulfilled.

A classification of in-country and out-of-country websites and hosting companies was made without any definition. A registered hosting company is regarded as in-country even if the hosting machines are outside the country. If a hosting company located in Turkey is not registered, it is then categorised as out-of-country **for banning purposes**. If the purpose is other, the company is treated as in-country.

Prior to Law No. 5651, a division of the BTK called the Presidency of Telecommunication and Communication (TIB) was established with the mandate of performing legal telephone tapping. In the course of the new legislation, this division progressively evolved in becoming responsible for internet related issues such as blocking websites, along with telephone tapping. Almost hundred positions were reserved for the TIB, 32 of which were filled within a few months in 2007.²

The main task of the TIB is to observe and monitor the internet and take precautions to “clean” it, i.e. to prevent online content relevant to Turkey that is considered harmful from being accessed. The TIB division itself has the authority to determine the level of monitoring and filtering. It also enforces regulation and monitoring of internet cafes, so as to make sure that they keep necessary logs and prevent harmful content to be accessed by customers.

If the web or hosting company is out-of-country, the TIB has the authority to ban harmful content from the catalogued list of crimes without the need to get permission from a court. If the website or hosting is within the country, then the TIB needs a court order to ban it. However, in the case of emergency (such as with child pornography or where human life is in danger) the prosecutor can ban a website due to harmful content. In such a case, a court order within 24 hours is required. The aggrieved party can appeal the ban decision using regular procedures.

The Law provides a procedure for removal of content and right to reply. It is called “notice and takedown.” It starts with a request to ISPs to take down the offending content and could result in imprisonment of the ISP’s head between two months and two years by a Penal Court.³ When the harmful content is removed from the banned site, the decision to ban the particular website is reversed upon the verification of removal of the offensive material by the TIB, court or prosecutor. In some cases, the court appoints an expert witness for this verification.

Secondary regulation specifies banning or “curtailing access” via two methods: i) DNS tampering and, ii) IP blocking. Courts sometimes order both of these measures at the same time. URL blocking is initially not implemented, even though NGOs demand URL blocking for offensive objects only, instead of blocking the entire website. URL blocking, which we will discuss, was put into law in 2013.

THE CATALOGUE CRIMES

Law No. 5651 lists the following as catalogue crimes with reference to the provisions of the Turkish Penal Code (TCK) and other laws (Law 5651, 2007):⁴

1. incitement to suicide (TCK-84)
2. sexual abuse of children (TCK-103), i.e. child pornography
3. facilitation of the use of narcotics (TCK-190)
4. provision of substances harmful to the health (TCK-194)
5. obscenity (TCK- 226)
6. prostitution (TCK-227)
7. facilitation of gambling (TCK-228)

8. the crimes against Atatürk (law 5816)⁵
9. betting/gambling (sports law)

The TIB has the authority to unilaterally block or ban the whole website, when hosted outside of Turkey, via DNS tampering or IP blocking. Whereas the TIB can only block a website for these alleged crimes, independent courts can ban any website for any reason they see fit under the national laws and regulations. After Law No. 5651 was implemented, several social networking and other platforms such as Wordpress, Geocities, Alibaba, Richarddawkins.net or Blogger were banned by invoking Civil Code or Intellectual Property Rights violations. It must also be noted that many of these decisions were later lifted.

CENSORSHIP IN PRACTICE

The following cases, ordered chronologically, provide some insight into Turkey's internet blocking mechanism.

Eksisözlük (sourtimes.com) is a Turkish social networking website which is organised as a dictionary where people can comment on entries. The courts blocked this website, run by a small company, on 6 January 2006 (Andaç, 2006; Eksi Sozluk, n.d.). However, the company appealed and the ban decisions were later removed.

The **Youtube.com** case best exhibits the many flaws of the Turkish censorship system. Youtube.com was first banned in 2007 before the internet censorship law was enacted. The reason was a video insulting Atatürk that was allegedly uploaded by a Greek youngster. The two largest national dailies took this seriously, carried the news to their front pages and set up a letter campaign to protest. Then, the state prosecutor for media intervened and brought the case to court. The judge saw the video on a CD and decided to block Youtube.com. Although Youtube was reopened after several months, it was later banned several times for shorter periods (Youtube Censorship, n.d.). The 2008 Youtube ban lasted more than two years. Until 2014, there were more than 30 court decisions banning Youtube.

The **Wordpress.com** case: In Turkey, Adnan Oktar is a well-known creationist and the head of an Islamic foundation. His lawyers have become known for the rigorous persecution of webpages that contain a defamatory statement about his activities. They have gone to court in various parts of the country to get court orders for banning websites. Following one of these decisions, the whole wordpress.com website was banned in August 2007 (Butt, 2008). After several months, a blogger objected and the ban was lifted.

Ateizm.org is a portal and forum for Turkish atheists. There, an expert, Turan Dursun, was questioning the main concept of Islam. Ateizm.org, turandursun.com and similar websites were banned in 2007 (O'Connor, 2008; Religious Tolerance, 2009). Reflecting the general attitude of the Turkish government against left-wing movements. Anarsist.org, a forum for Turkish anarchists, was banned in 2008 (Önderoğlu, 2008). Both these decisions were later lifted.

Alibaba.com is the largest B2B platform in the world. It is mainly the largest import-export shop in the world. The Turkish government subsidises Alibaba. The website was banned for a trademark dispute between two construction firms. One firm went to court for removal of a picture from the other firm's webpage, claiming violation of trademark. The court decided for the removal of the picture. Upon not removing the picture, the court ordered the blocking of Alibaba.com. The blocking continued for over a week. Although the court could have decided on

a fine, it preferred to ban the whole website in February 2008 (Bilisim ve Hukuk, 2008).

Richarddawkins.net included a comment about Adnan Oktar's book rejecting Darwinian evolution. Adnan Oktar went to court claiming the comments are defamatory. The court banned the site without any trial in September 2008 (Guardian, 2008). Richard Dawkins waited for notice of a trial and a chance to defend himself. The website finally reopened after a long legal fight.

Egitimsen.org.tr is the website of a trade union in the educational sector. The head of the trade union made a statement to the media about a book written by Adnan Oktar. In 2008 Oktar's lawyers went to court claiming that the website of the union carried defamatory statements. The court banned the website (Schleifer, 2008), but trade union lawyers successfully appealed to the court in favour of lifting the ban. The offending statements made two years earlier were removed from the site.

Since 2008, **Geocities.com** is another indefinitely banned website in Turkey. There is no scheduled trial and no appeal for reversal of the decision. It could be accessed within Turkey as of May 2015 but a note indicated that the site was blocked via a court order.

Blogger.com was banned in October 2008 by a Diyarbakır Court upon a complaint by Digiturk, a broadcasting company that had the rights to broadcasting the Turkish Football League matches (Censorship Turkey, n.d.). The company questioned the existence of about 60 blogs that contained links to illegal broadcasting of football matches. Digiturk is an Istanbul company, while Diyarbakır is located in Eastern Turkey. As a result, the court banned the whole blogger.com and blogspot.com platforms. Later, the court suspended its decision, and as of May 2015, the case is still pending.

Sites.google.com was banned after a long process. The site hosted a blog which contained anti-Atatürk remarks and insults. An NGO whose main purpose is to promote the ideas of Atatürk went to the state prosecutor in Ankara and asked for the blocking of the website in 2009 (Open Society, 2011). A different court in Denizli, far away from Ankara, banned the whole sites.google.com in 2010. The court justified its decision by the fact that it was not technically possible to block an individual URL. IP-based blocking had to be made, said the court. A PhD student who published his work on sites.google.com appealed to that decision and went to the European Court of Human Rights (ECHR) and the court found that Turkey violated the European Convention on Human Rights (Convention on Cybercrime, n.d.). Currently, both IP-based and URL-based blockings are made in Turkey.

Facebook was banned in 2009 but the decision was not implemented. A Facebook group was formed that claimed that Kemal Kılıçdaroğlu, president of the main opposition party CHP, was supporting the PKK, the Kurdistan Workers' Party. Kılıçdaroğlu's lawyer went to court asking for the blocking of this group and if not possible, the full blocking of Facebook.com. The court approved the request. The decision of the court was transmitted to the TIB, but the TIB did not implement the decision stating that the insult does not fall within the catalogued crimes. If the decision of the court had been transmitted to ISPs, then it would have been implemented. Kılıçdaroğlu then went to court asking the head of the TIB be tried for not implementing a court decision. As of May 2015, the case is still pending. There are about 500 Facebook groups supporting Kılıçdaroğlu, and just a few groups opposing him. Then again, the CHP has about 500 Facebook groups created by various branches (NTVMSNBC, 2010).

Twitter was an important venue for communication during the Gezi events between May and

June 2013. Twitter usage surged substantially during the Gezi protests. Twitter's role is important when it comes to freedom of expression in Turkey, especially against the backdrop of widespread complaints about the direct and indirect control of mass media by the government (Nielsen, 2013). Then Prime Minister Erdoğan, who has over five million followers on Twitter (@RT_Erdogan), labelled Twitter "a menace to society" (Nielsen, 2013; Huffington Post, 2013). This follows the appearance of corruption-related material⁶ on Twitter about Erdoğan and four cabinet ministers. Erdoğan vowed to eradicate Twitter on 20 March 2014 (Watson & Tuysuz, 2014). Twitter was blocked on that day without a court order (Dockterman, 2014). The ban was lifted three days after the 30 March 2014 elections by the Constitutional Court (BBC, 2014a). In the following months some Twitter accounts (eg. @Haramzadeler333 , @Bascalan and @fuatavni), from where corruption charges were leaked, were also blocked (Musil, 2014).

Websites supporting ISIS and al-Qaeda derivatives, however, are not blocked in Turkey. Sites like takvahaber.net and mustaqim.net, which openly disseminate ISIS propaganda, function as a recruiting tool and call to violence operate freely in the country (Arango, 2015).

The Turkish government is demanding that Google, Twitter and Youtube open an office in Turkey, issue invoices from Turkey, pay due taxes, and more importantly, respond swiftly to the demands of internet censorship whether they be issued by a court or the TIB. Such demands are usually declined.

Engelliweb, a watchdog website that monitors the blocked websites in Turkey reports **as of May 2015** roughly 80,000 blocked websites. The real figure is well above these numbers, as Engelliweb only reports the blocked websites signalled by internet users. The real number and the list of blocked websites are never disclosed by the government. About 93% of the sites registered by Engelliweb are blocked by a decision of the TIB, i.e. without a court order. The majority of the blocked sites contain pornographic material. The second group contains the websites of dissident political groups and Kurdish insurgent movements. Almost all of the pornographic websites are international and do not specifically target Turkish audiences. On the contrary, the banned political websites target the audience in Turkey and can only be accessed by VPN.

DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) is one of the primary surveillance and blocking methods on the internet. Data travels as small units called 'packets' over the internet. Each packet includes an address portion and a data portion that contains the real content (e.g. part of a photo to be displayed on a website). Normally, routers located at ISPs check only the address portion of each packet and direct the packets to their destination addresses. This *modus operandi* is one of the features of "net neutrality," one of the main tenets of the internet. DPI systems form the basis for violations of net neutrality. By checking not only the address portion of a packet but all of it, DPI enables discriminatory treatment of traffic. As such, these systems facilitate the monitoring of the content of a message as it travels through the ISP hardware. DPI systems can also be used for some other tasks such as network optimisation, blocking or throttling down content.

Phorm, a company specialised in behavioural advertisement systems over the internet, uses TTNET, the largest ISP in Turkey, as its infrastructure partner. It implements the DPI technology which profiles internet users by assigning unique ID numbers to them. Through these ID numbers, every action of the user is recorded for the declared objective of displaying

relevant advertisements to him/her. However, such profiling also helps determine the political, religious and sexual orientation of the user as well as his/her membership to political parties, trade unions and other communities.⁷

TTNET was fined by the regulatory body BTK for supporting Phorm's activities in Turkey, which mislead internet users (Aru, 2013). Phorm's operations were stopped for about four months, before resuming in April 2013.

FILTERING THE “SECURE” INTERNET

On 22 February 2011, the BTK announced that the “Secure Usage of Internet” project would be implemented on 22 November 2011. All Internet subscribers were obliged to choose one of four profiles to access the internet, namely “family”, “standard”, “children” or “domestic” (in-country).

This caused a major uproar in the country and on 15 May of that year, a major demonstration was held in Turkey's major cities. The BTK withdrew the decision and introduced a modification which included voluntary “family” and “child” profiles only. These profiles worked as a voluntary filter that blocked “unwanted” material. The child profile consisted of a “white list” of URLs that are determined by the BTK. The family profile blocked a set of websites, in other words a “black list.” All lists were determined by the BTK and the ISPs were obliged to apply filtering to the subscribers that had opted for these profiles.

As of the summer 2013, 1.4 million subscribers had opted for a filter. They thereby agreed to voluntarily limit their internet access according to the above-mentioned lists. While the length and content of lists are unknown, one can check whether a website is listed or not. There are no defined procedures for listing a website or remove it from a list.

LACK OF TRANSPARENCY AND THE RULE OF LAW

At the end of 2008 the BTK published a report providing statistics on the number of websites blocked by the TIB and by court orders during that year, by categories of offense. Since then, the agency has stopped providing details. Attempts to dig out the reasons by means of freedom of information requests have systematically been unfruitful (Palabiyik, 2015). As stated above, the TIB blocks websites according to decisions given either by the court or the TIB, without attempting to dialogue. In other words, civil servants are often those deciding on the blocking of websites, i.e. restricting several freedoms, such as the freedom of expression. Very rarely does a ban result in a trial. The TIB publishes not the numbers but percentages of blocked websites in terms of categories. As of September 2014, child related blocks are at 10%, prostitution at 4.6%, obscenity at 84%, Atatürk-related blocks close to 0.04%, and the remaining categories make up the remaining 1.2% (Güvenliweb, 2014).

International media covered the wave of “Gezi protests” (May-June 2013) live and the number of Twitter users jumped from 2 million on 28 May to 8 million on 10 June (Yalçıntaş, 2015). Government responded with attempts to discourage usage of social media in relation to the protests. At the peak of the demonstrations, the police raided youngsters at night for their Twitter usage (Harding and Letsch, 2013). Partly due to the effect of social media on the Gezi protests, an amendment to Law No. 5651 was passed by parliament on 5 February 2014,

and approved by President Abdullah Gül, a founder of the AKP. The new amendment envisaged even harsher measures against freedom of expression on the internet (Järvinen, 2014a; Frosio, 2014). The amendment was passed as a package of laws and amendments, and regular procedures of consulting with state actors and outside stakeholders have not been followed. The amendment introduced fast banning of websites in relation to privacy and personality rights, access by the TIB to logs of all user activities on the internet, URL and IP blocking, and a new government-controlled ISP union. URL blocking was justified by preventing blocking of whole website for just a few “harmful contents”. For privacy or private life violation, a proper application to the TIB is enough for immediate banning (**within four hours**) of the offending URL. The complaint will also go to court within 24 hours, and the court will decide within 48 hours. Even top TIB management can render such a decision, as long as it then goes to court **for approval** within 24 hours. Although there is a time limit of four hours for implementing a blocking decision, there is none for uplifting it. In addition, ISPs are obliged to implement data retention, i.e. they have to log user activity and store the data between one and two years, and submit to officials when requested by a court.

A union of ISPs was formed to centralise and speed up the process of banning a website. Bylaws of this union are approved by the BTK. Once a court decides to order the ban of an undesirable content, that decision is valid for all websites containing that content. The costs related to URL blocking and other filtering is left to corresponding ISPs. Collective access providers, of commercial nature or not (universities, firms, even large families) are forced to prevent access to “unlawful” content. ISPs are asked to prevent any attempt to bypass blocking restrictions, while bypassing blocking is not criminalised.

Internet cafes are subject to stringent regulations, which extend beyond limits defined by this law. After Erdoğan's election as President, another amendment came into force on 8 September 2014, just after the United Nations Internet Governance Forum took place in Turkey. The amendment was justified as “protecting the esteem and honour of individuals against defamation on the Internet,” but it must be noted that this justification came to Turkish political scenery only after the internet became an efficient medium for disseminating corruption scandals in the highest echelons of politics. On 2 October 2014, the Constitutional Court overturned critical parts of the amendment (Järvinen, 2014b). Unperturbed by the Constitutional Court's decision, the government simply waited for the retirement process of some key members of the Constitutional Court and brought the same amendments to the parliament on 20 January 2015, “reinforced” by some harsher measures. By the newly added amendments, authority for blocking decisions was widened to cabinet ministers who can justify their decisions by invoking the protection of national security, public order, public health, prevention of crime, and protection of life and property. The new amendments were adopted by the parliament on 19 March 2015 (CPJ, 2015a). Currently, the new bill and accompanying new laws, such as the Internal Security Bill (Al-Monitor, 2015), are applied in full force. The application of the law is seemingly arbitrary, sometimes with bizarre consequences. For example, a university student was sentenced to one year for retweeting an article from the popular satirical website Zaytung, which “reported” that a provincial governor declared autonomy from Turkey. The article had the picture of the governor in a military vehicle and surrounded by guards in a parade during a national holiday (Bolton, 2015) where it is customary for governors to appear in such parades. Zaytung was not prosecuted for that article.

TURKEY IN THE CONTEXT OF INTERNATIONAL CENSORSHIP PRACTICES

Disregarding crimes such as child pornography, which are unacceptable in all cultures, internet censorship is usually justified by protecting the so-called “existing social system” in any given country. In this context, the social system implies the social and economic relationships between social classes and individuals. There is also a second implication for the social system which has personal overtones in the context of censorship. Adult pornography is an example which is regarded as a threat to this perception of social system. Many countries either apply varying degrees of censorship or develop measures for enforcing self-censorship to protect their social systems. Albeit with much harsher measures, Turkey is no exception in this matter. Internet censorship in Turkey used to have mainly two pillars: preventing “undesired” political messages and fighting pornography. Indeed, the majority of blocked websites reported by Engelliweb are related to pornography. There are also websites of political nature which are regarded to be harmful. However, it must be stated that the phrase “existing social system” is getting increasingly vague in Turkey due to the fervent efforts of the ruling AKP party and President Erdoğan to transform the country into what he calls “new Turkey.” This provokes a sizeable tension in the deeply divided society where more than half of the population is anxious, perceiving the country as being dragged into a fundamentalist abyss experienced already by countries such as Afghanistan, Iraq, Yemen, Syria and Libya. This in turn results in a higher level of struggle against the current trend and thus, an increased level of internet censorship.

Beyond the usual practices of internet censorship which aim to protect the existing social system, Turkey has made a significant “contribution” in this area since the 17-25 December 2013 events: internet censorship in Turkey is applied *en masse* for preventing the dissemination of news about corruption and for “protecting the esteem and honour” of corrupt politicians (The Center for Internet and Society, n.d.; ARTICLE 19, Committee to Protect Journalists, English PEN, Freedom House, P24 and PEN International, 2014; Amnesty International, 2014). This type of censorship is not as easy as blocking individual websites with tiny audiences. Corruption news is usually broadcast through venues such as Twitter and Youtube which have millions of users and operate under the spotlight of the international community. For this reason, occasional blockings of global platforms in Turkey result in increasingly strong backlashes from all over the world.

As a result of the government's fervent efforts in internet blocking and censorship, the Removal Request Report by Twitter, covering the period July-December 2014, shows that requests from Turkey are higher than from all other countries combined (Twitter, n.d.). This measurable attribute gives an idea about the level of censorship in the country. However, this seemingly does not make sense, because technical bypass measures such as changing DNS settings and using VPN are widely used in the country. As a result, sometimes Twitter usage increases in Turkey after Twitter bans take effect (BBC, 2014a). So why does the government, which must be well aware of the “Streisand effect”, take such measures that harm its reputation? One explanation is an attempt to criminalise social media usage (Tufekci, 2014). Although this interpretation may have some merit, a more plausible explanation is related with the profile of the internet users in the country. The users who have the proficiency to bypass the ban are, by definition, comparatively more educated. The AKP government, however, mainly relies on comparatively less educated and conservative masses from rural and urban areas (Tillman, 2014) who turn to TV channels - most of which are government-controlled - when internet sources are blocked.

IRAN

Iran is another country where the internet is heavily censored. Platforms like Twitter and Facebook are banned and there are attempts to block VPN software as well as Tor, which is widely used to circumvent the censorship (Franceschi-Bicchierai, 2015). Attempts like these have been made in the past, most of which were then successfully circumvented later (Arma, 2011; O'Neill, 2014). Due to the strictly religious nature of the regime, Iran has introduced a filtering system called "Halal Internet" (O'Neill, 2014). Aryan and Halderman (2013) have technically analysed the Iranian censorship mechanism under various lights: http host-based blocking, keyword filtering, DNS hijacking, and protocol-based throttling. The authors argue that the mechanism possibly relies on centralised equipment which they believe is easier to circumvent in the future. This seems to contrast with the Turkish experience which relies on ISPs as intermediaries to perform the blocking. As stated above, the amendments in Law No. 5651 led to the establishment of an ISP union with compulsory membership. The most important function of this union is to execute blocking orders by the TIB within four hours. It is not clear why the blocking orders are not simply fulfilled by TTNET, which runs the backbone.

CHINA

China also blocks the internet widely through the Great Firewall of China (Feng and Guo, 2013). Contrary to Turkey, where access to the banned sites through VPN or Tor cannot be technically prevented, the Chinese government can block Tors - a sophisticated privacy tool commonly used for circumventing internet blockings (MIT Technology Review, 2012). It is not clear whether the technology used by China is commercially available. King, Pan and Roberts (2013) analysed the internet censorship practices in China and found that, against general understanding, criticism of the Chinese government, its policies and leaders are not likely to be censored. The authors argue that the posts which contain calls for collective action and social mobilisation against the government and its policies are the ones that are blocked. This is more or less the same in Turkey where, except for sporadic cases that seem to stem from some overzealous officers like in the Zaytung case, individual criticism of the **government** is not likely to be censored. Like in China, calls for social mobilisation appear likely to attract much harsher responses from the Turkish government. However, unlike China, technical and institutional weaknesses prevent most of such calls to be censored, let alone punished. This results in arbitrariness of the "law enforcement" where some of such calls are harshly punished and some go unnoticed.

As an element of context here, institutional and technical weaknesses of the government cannot be understood without analysing the bitter fight of now President Erdoğan with Fethullah Gülen, a religious leader who lives in exile.⁹

The power struggle led to important consequences: firstly, Turkey has become the first and only country where computer fraud was effectively used to topple a ruling class and its ideology (in power since 80 years). Secondly, purges of "old guards" and Gülen followers from bureaucracy resulted in the loss of well-trained staff and led to increasingly severe technical and institutional weaknesses which have had implications for censorship. And thirdly, beyond specific issues such as internet censorship, the fierce fight for power adversely affected almost all public institutions, many of which became much less effective compared to ten years ago. For example, the Scientific and Technological Research Council of Turkey (TÜBİTAK), which has become a boxing ring between Gülenists and AKP followers (Anadolu Ajansı, 2015; Today's Zaman, 2015), had to decline requests for expertise in specific issues like digital forensics, mainly because of the loss of qualified personnel (Saymaz and Çelikkan, 2015).

Getting back to the comparison of Turkish and Chinese internet censorship practices, there is an

important difference between the two countries: King, Pan and Roberts (2013) argue that posts about corruption are usually not censored in China. However, this does not mean that all of such posts are tolerated. On the contrary, some of them are subject to censorship as Richet (2013) reports. While China demonstrates some level of tolerance to corruption news, posts about corruption of high-ranking government officials are fervently blocked in Turkey. For example, the government went to great lengths to block Twitter accounts @Haramzadeler333 and @Bascalan, which were instrumental in disseminating the corruption recordings of 17-25 December 2013.

CONCLUSION

Internet has become a very important medium of communication, entertainment and business in today's society. This is true for not only the so-called developed countries, but also for developing countries. The "Arab Spring" has demonstrated that the internet can play a role in mobilising people, eventually even leading to the toppling of authoritarian governments (note: what comes after, is another story). Unlike mass media - which is easier to control due to its centralised nature, internet is a truly decentralised and chaotic environment which is very difficult to control. Additionally, there is no technical tool that guarantees hundred percent control over the internet. As the examples in this article show, attempts to control the internet may result in little success, while harming the reputation of rulers all over the world.

Turkey's recent history is marked by severe turbulences that came one after the other. After AKP's ascend to power in 2002, the anxiety and suspicion of the military and civil bureaucracy did not result in a coup, due to the lack of support from the Western world. After the AKP and its allied Gülen movement (which have exactly the same ideological-religious background) managed to eliminate the possible threat of the bureaucracy, they started the infighting. All these events were associated with redesigning the society according to religious rules, resulting in an increasingly divided population. This in turn paved the way to increasingly high tensions in the society. Turkey's internet censorship practices followed this course, albeit with little success in preventing free speech for all. It is, however, open to discussion whether the internet censorship has been successful to prevent the conveying of free speech to those parts of Turkish society which have lower levels of education.

Internet censorship is usually practiced to protect the social order. Social order, however, is a complicated term which has different meanings in different contexts. In the case of Turkey, to complicate the matter even further, a new "source" for internet censorship has been added to the list since December 2013: protecting individuals at the highest echelons of politics from "defamation" resulting from the use of the internet for broadcasting explicit corruption recordings. This again demonstrates the power of the internet *vis-à-vis* mass media that is controlled directly or indirectly by the government.

FOOTNOTES

¹. The role of Turkish Telecom is important in this context, because it runs the internet backbone in Turkey via its subsidiary TTNET.

². As a counterpoint meant to put these numbers in perspective, a unit within the State Planning Organisation – responsible for coordinating efforts for transforming Turkey into an "Information Society" – was established in 2003 with only five members of staff. Four years later, in 2007, it grew to a mere 15 staff. The unit acted as the secretariat of the "E-

transformation Executive Committee,” which consisted of cabinet ministers, high-level bureaucrats and representatives of NGOs with observer status. The unit is currently responsible for preparing the “Information Society Strategy 2014-2018” which was published in March 2015 (Bilgi Toplumu Stratejisi, 2015).

3. Imprisonment was removed in 2014.

4. Items 7 and 9 were added later.

5. Turkey is very sensitive with regard to Atatürk, the founder of the Turkish Republic. Law No. 5816, which penalises insults to Atatürk, was passed in 1951 and it has not changed since then. “Defamatory material against Atatürk” was included as a catalogue crime to Law No. 5651 on April 12, 2007 during the deliberations of the Justice Commission in the Parliament.

6. The material contained links to Youtube videos.

7. Due to this blatant violation of personal privacy (Cellan-Jones, 2008; Fuchs, 2012), Phorm has been ousted from almost all countries it had previously operated in. The list includes the United States, some European Union member states, and South Korea. The European Commission went to court in 2009 against the UK government for allowing Phorm to operate in the UK (EC, 2009). It is not known how these profiles are used along with advertisement.

8. Tor can be found under <http://www.torproject.org>

9. Gülen has established a semi-clandestine organisation in the last forty years and used to have an increasingly stronger power base in Turkey. His followers have established schools and universities in more than one hundred countries. AKP and Gülen had been close allies since 2002 and their cooperation resulted in the elimination of the traditional power of Western-oriented, secular and authoritarian military and civil bureaucracy which ruled the country since the foundation of the republic. AKP provided votes of the masses and Gülen provided well-trained cadres in the police force and judiciary in this cooperation. A series of trials against the “old guard” started in 2010 and resulted in hundreds of military officers, including top generals, to be sent to prison with the accusation of planning a coup against the government (Arsu, 2012). As a result, about twenty percent of the generals who were in active duty were put into prison along with hundreds of lower ranking officers (Butler, 2012). The most important evidence in these trials were computer hard disks and DVDs that contained some files hinting towards preparations for a coup. Some convincing arguments by the defendants who claimed that electronic evidence was fabricated (Rodrik, 2012; Doğan and Rodrik, 2011) were disregarded in the trials. After the power of the military was broken in 2013 the former allies started a bitter fight for acquiring the sole power in the country. During this fight, Erdoğan suddenly “recalled” that it was Gülen followers who hatched a plot by fabricating the false electronic evidence against the accused officers. He blamed Gülen and his followers of establishing a “parallel state” within the bureaucracy. This resulted in a hunt against the Gülenists within the bureaucratic apparatus. At the same time, the cases against the military were reopened and almost all of the accused military were acquitted in 2015 due to the fraudulent electronic evidence (BBC, 2015; The New York Times, 2015). It was now Gülen followers' turn to be put in prison. An arrest warrant had been issued for Gülen himself on 19 December 2014 (BBC, 2014b) and many of his followers in the bureaucracy including some of the judges and prosecutors who had sent the generals to prison were either fired from their duties or arrested in the first half of 2015 (Diclehaber, 2015; Dailysabah, 2015).

REFERENCES

- ACLU. (2005). 30,000 National Security Letters Issued Annually Demanding Information about Americans: Patriot Act Removed Need for FBI to Connect Records to Suspected Terrorists. Retrieved from <https://www.aclu.org/news/30000-national-security-letters-issued-annually-demanding-information-about-americans-patriot>
- Akdeniz, Y. (2010). Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship. Organization for Security and Co-operation in Europe. Retrieved from <http://www.osce.org/fom/41091>
- Akdeniz, Y., & Altıparmak, K. (2008). Internet: Restricted Access. A Critical Assessment of Internet Content Regulation and Censorship in Turkey. Retrieved from http://www.cyber-rights.org/reports/internet_restricted_bw.pdf
- Akgül, M. (2006). Bilişim Taslak. Retrieved from <http://akgul.bilkent.edu.tr/bilisim-taslak.html>
- Akgül, M. (2008). İnternet Yasakları ve Hukuk, Türkiye Barolar Birliği Dergisi, 78, (2008), pp 352-377.
- Akgül, M. (2009a). Türkiye'nin İnternetle Savaşı: Harakiri, Donkişot ve Devekuşu. Retrieved from http://ab.org.tr/abo9/kitap/akgul_ABo9.pdf
- Akgül, M. (2009b), İnternet Yasakları: Bir Hukuk ve Adalet Faciası mı?, Türkiye Barolar Birliği Dergisi 84, pp 401-416.
- Akgül, M. & Pekşirin, H. (2001). İnternetin Yasal Düzenlemesi. Bilişim STK Platformu. Retrieved from <http://bt-stk.org.tr/yeni-duzenleme.htm>
- Al-Monitor (2015). Is Turkey becoming a police state?. Retrieved from <http://www.al-monitor.com/pulse/originals/2015/02/turkey-becoming-police-state.html>
- Amnesty International. (2014). Amnesty International public statement. Retrieved from <http://www.amnesty.ch/de/laender/europa-zentralasien/tuerkei/dok/2014/internetzensur-praesident-guel-muss-veto-einlegen/internationale-medienmitteilung-englisch>
- Andaç, Ş. (2006). 'Ekşisözlük'ün esrarı çözüldü! Milliyet. Retrieved from <http://www.milliyet.com.tr/2006/05/30/yasam/axyas01.html>
- Anadolu Ajansı. (2015). Turkey: Three arrested for Erdogan 'political spying'. Retrieved from <http://www.aa.com.tr/en/turkey/487271--turkey-three-arrested-for-erdogan-political-spying>
- Arango, T. (2015). Islamist Websites in Turkey Manage to Evade Strict Internet Censorship. New York Times. Retrieved from <http://www.nytimes.com/2015/03/14/world/europe/islamist-websites-in-turkey-manage-to-evade-strict-internet-censorship.html>
- Arma. (2011). Iran blocks Tor; Tor releases same-day fix. TorProject. Retrieved from <https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix>
- Arsan, E. (2013). Killing me softly with his words: Censorship and self-censorship from the perspective of Turkish journalists. Turkish Studies, 14(3), 447-463.

Arsu, S. (2012). Turkish Court Convicts 330 From Military in Coup Case. The New York Times. Retrieved from <http://www.nytimes.com/2012/09/22/world/europe/turkish-court-convicts-330-military-officers-in-coup-plot-trial.html>

ARTICLE 19, Committee to Protect Journalists, English PEN, Freedom House, P24 and PEN International. (2014). Joint Submission to the UN Universal Periodic Review of Turkey. Retrieved from <http://www.pen-international.org/wp-content/uploads/2014/07/PEN-International-joint-submission-to-the-UPR-Turkey.pdf>

Aru, Ç. (2013). BTK, Phorm Soruşturmasında TTNet'e 1,5 Milyon TL Ceza Verdi. Turk-Internet. Retrieved from <http://www.turk-internet.com/portal/yazigoster.php?yaziid=42248>

Aryan, S., Aryan, H., & Halderman, A.J. (2013). Internet censorship in Iran: a first look. Paper presented at the 3rd USENIX Workshop on Free and Open Communications on the Internet, Washington, D.C. Retrieved from <https://jhalderm.com/pub/papers/iran-foci13.pdf>

Aydilek, O. (2006). Çocuk pornosu hükümeti böldü. Retrieved from <http://arsiv.sabah.com.tr/2006/12/16/siy102.html>

BBC. (2014a). Officials in Turkey 'lift Twitter ban'. Retrieved from <http://www.bbc.com/news/world-europe-26873603>

BBC. (2014b). Turkey issues Fethullah Gulen arrest warrant. Retrieved from <http://www.bbc.com/news/world-europe-30552148>

BBC. (2015). Turkish 'Sledgehammer' coup plot trial collapses. Retrieved from <http://www.bbc.com/news/world-europe-32136809>

Bilisim ve Hukuk (2008). İnternet Sitelerine Erişimin Engellenmesi. Ankara Barosu Bilgi İşlem Merkezi Yayınları. Retrieved from <http://www.ankarabarusu.org.tr/Siteler/1944-2010/Dergiler/BilisimveHukukDergisi/2008-3.pdf>, p.22-23.

Bolton, D. (2015). Turkish student gets suspended jail sentence for retweeting satirical article on Twitter. The Independent. Retrieved from <http://www.independent.co.uk/news/world/europe/turkish-student-gets-suspended-jail-sentence-for-retweeting-satirical-article-on-twitter-10198146.html>

Butler, D. (2012). Insight: Turkish generals look to life beyond prison bars. Reuters. Retrieved from <http://in.reuters.com/article/2012/06/29/us-turkey-army-idINBRE85SoC620120629>

Butt, R. (2008). Turkish court bans Richard Dawkins website. The Guardian. Retrieved from <http://www.theguardian.com/world/2008/sep/18/turkey>

Cellan-Jones, R. (2008). Web creator rejects net tracking. BBC. Retrieved from <http://news.bbc.co.uk/2/hi/technology/7299875.stm>

Censorship Turkey. (n.d.). In Wikipedia. Retrieved May 22, 2015 from https://en.wikipedia.org/wiki/Censorship_in_Turkey

Committee to Protect Journalists (CPJ). (2015a). Turkish parliament passes restrictive Internet

bill. Retrieved from <https://cpj.org/2015/03/turkish-parliament-passes-restrictive-internet-bil.php>

Convention on Cybercrime. (2001). In Wikipedia. Retrieved May 22, 2015 from https://en.wikipedia.org/wiki/Convention_on_Cybercrime

Council of Europe. (2011). Cybercrime legislation - country profile. Strasbourg. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_Turkey_2011_January.pdf

Cumhuriyet. (2015). MIT Tırları haberine yasak geldi. Retrieved from http://www.cumhuriyet.com.tr/haber/turkiye/287767/MiT_TIR_lari_haberine_yasak_geldi.html

Dailysabah. (2015). Turkey's top judicial body HSYK investigates Gülen-linked judges, prosecutors. Retrieved from <http://www.dailysabah.com/politics/2015/04/15/turkeys-top-judicial-body-hsyk-investigates-gulenlinked-judges-prosecutors>

Diclehaber. (2015). 'Parallel' prosecutors and judges dismissed from profession. Retrieved from <http://www.diclehaber.com/en/news/content/view/456645?from=1923065108>

Dockterman, E. (2014). Turkey Bans Twitter. Time. Retrieved from <http://time.com/32864/turkey-bans-twitter/>

Doğan, P., & Rodrik, D. (2011). A guide to Sledgehammer in 15 questions. Retrieved from <https://cdogangercekler.files.wordpress.com/2011/03/faq-sledgehammer.pdf>

Draft RTUK Law (2001). RADYO VE TELEVİZYONLARIN KURULUŞ VE YAYINLARI HAKKINDA KANUN, BASIN KANUNU, GELİR VERGİSİ KANUNU İLE KURUMLAR VERGİSİ KANUNUNDA DEĞİŞİKLİK YAPILMASINA DAİR KANUN. Retrieved from <http://bt-stk.org.tr/ss682m.htm>

European Commission (EC). (2009). Telecoms: Commission launches case against UK over privacy and personal data protection. Brussels. Retrieved from http://europa.eu/rapid/press-release_IP-09-570_en.htm

European Court of Human Rights (ECHR). (2013). Case of Ahmet Yildirim v. Turkey. Strasbourg. Retrieved from [http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=001-115705#{%22itemid%22:\[%22001-115705%22\]}](http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=001-115705#{%22itemid%22:[%22001-115705%22]})

Eksi Sozluk. (n.d.). In Wikipedia. Retrieved May 22, 2015 from https://tr.wikipedia.org/wiki/Ek%C5%9Fi_S%C3%B6zl%C3%BCk

Feng, G. C., & Guo, S. Z. (2013). Tracing the route of China's Internet censorship: An empirical study. *Telematics and Informatics*, 30, 335-345.

Franceschi-Bicchierai, L. (2015). Iran Is Trying to Block Tor. Motherboard. Retrieved from <http://motherboard.vice.com/read/iran-is-trying-to-block-tor>

Frosio, G. (2014). Turkey Enlists Intermediaries to Censor and Surveil Internet Users. Center for Internet and Society at Stanford Law School. Retrieved from

<https://cyberlaw.stanford.edu/blog/2014/02/turkey-enlists-intermediaries-censor-and-surveil-internet-users>

Fuchs, C. (2012). Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society. The Privacy & Security Research Paper Series. Centre for Science, Society & Citizenship, Uppsala. Retrieved from http://www.projectpact.eu/privacy-security-research-paper-series/%231_Privacy_and_Security_Research_Paper_Series.pdf

Galperin, E. (2015). Facebook Caves to Turkish Government Censorship. Electronic Frontier Foundation. Retrieved from <https://www.eff.org/deeplinks/2015/01/facebook-caves-turkish-government-censorship>

Guvenliweb (2014) Blocking Statistics. Retrieved from <http://www.guvenliweb.org.tr/istatistikler/files/ISTATISTIK.pdf>

Harding, L., & Letsch, C. (2013). Turkish police arrest 25 people for using social media to call for protest. The Guardian. Retrieved from <http://www.theguardian.com/world/2013/jun/05/turkish-police-arrests-social-media-protest>

Herman, E. S., & Chomsky, N. (2002). Manufacturing consent: The political economy of the mass media. NY: Pantheon Books.

Hubbard, B., & Shoumali, K. (2015). Fertilizer, Also Suited for Bombs, Flows to ISIS Territory From Turkey. The New York Times. Retrieved from http://www.nytimes.com/2015/05/05/world/europe/fertilizer-also-suited-for-bombs-flows-to-isis-territory-from-turkey.html?_r=0

Huffington Post. (2013). Turkey Protests: Recep Tayyip Erdogan Slams 'The Menace Of Twitter'. Retrieved from http://www.huffingtonpost.co.uk/2013/06/03/turkey_recep-tayyip-erdogan-twitter-social-media_n_3377233.html

Inet (2001). Retrieved from <http://bt-stk.org.tr/rtuk-inet-basin-ilkiz.htm>

Internet Kampanyası (2007). Retrieved from <http://internetim.kampanya.org.tr/>

Järvinen, H. (2014a). Internet censorship and surveillance in Turkey. European Digital Rights. Retrieved from <https://edri.org/internet-censorship-surveillance-turkey/>

Järvinen, H. (2014b). Turkey: Constitutional Court overturns Internet law amendment. European Digital Rights. Retrieved from <https://edri.org/turkey-constitutional-court-overturns-internet-law-amendment/>

King, G., Pan, J., & Roberts, M. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, 107(2), pp. 326-343.

Law 5651 (2007). Retrieved from <http://bt-stk.org.tr/k5156.html>

MIT Technology Review. (2012). How China Blocks the Tor Anonymity Network. Retrieved from <http://www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network/>

- Musil, S. (2014). Two anonymous Twitter accounts blocked in Turkey. CNET. Retrieved from <http://www.cnet.com/news/two-anonymous-twitter-accounts-blocked-in-turkey>
- Nielsen, N. (2013). 'Turkish Spring' tests Erdogan's rule. Euobserver. Retrieved from <http://euobserver.com/foreign/120345>
- NTVMSNBC (2010). Facebook her an kapanabilir. Retrieved from <http://www.ntvmsnbc.com/id/25142952>
- O'Brien, D. (2012). Sidebar: Online Censors Sharpen Tactics. Committee to Protect Journalists. Retrieved from <https://www.cpj.org/reports/2012/10/turkeys-press-freedom-crisis-sidebar-online-censors-sharpen-tactics.php>
- O'Connor, K. (2008). Muslims suppressing atheism in Turkey. OpEdNews. Retrieved from http://www.opednews.com/articles/genera_kelly_o__080115_muslims_suppressing_.htm
- O'Neill, P. H. (2014). Iran blacklists Tor network, knocking 75 percent of users offline. The Daily Dot. <http://www.dailydot.com/politics/iran-censors-tor-75-percent/>
- Önderoğlu, E. (2008). Adnan Oktar İstedikçe Yasaklı Siteler Listesi Uzuyor. Bianet. Retrieved from <http://bianet.org/bianet/ifade-ozgurlugu/110016-adnan-oktar-istedikce-yasakli-siteler-listesi-uzuyor>
- Open Society Foundations (2011). Yildirim v. Turkey. Retrieved from <http://www.opensocietyfoundations.org/litigation/yildirim-v-turkey>
- Palabiyik P. (2015). Bilgi edinme: Türkiye’de hak değil, istisna. HaberVesaire, İstanbul Bilgi Üniversitesi. Retrieved from <http://www.habervesaire.com/news/bilgi-edinme-turkiye-de-hak-degil-istisna-2799.html>
- PEN America (2014). Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor. Retrieved from http://www.pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20with%20Color%20cover-UPDATED.pdf
- Religious Tolerance (2009). Religious intolerance - In Turkey. ReligiousTolerance.org. Retrieved from http://www.religioustolerance.org/rt_turkey.htm
- Richet, J. (2013). Overt censorship: a fatal mistake? Communication of the ACM, 56(8), pp. 37-38.
- Rodrik, D. (2012). Why do we accuse the Gülen movement? Balyoz Davası ve Gerçekler. [Weblog] Retrieved from <http://balyozdavasivegercekler.com/2012/05/21/why-do-we-accuse-the-gulen-movement/>
- RTUK Law (2001). RADYO VE TELEVİZYONLARIN KURULUŞ VE YAYINLARI HAKKINDA KANUN, BASIN KANUNU, GELİR VERGİSİ KANUNU İLE KURUMLAR VERGİSİ KANUNUNDA DEĞİŞİKLİK YAPILMASINA DAİR KANUN. Retrieved from <http://bt-stk.org.tr/k4676.html>
- Sabah. (2007a). 'Temiz İnternet' için Ankara'da buluşalım. Retrieved from

<http://arsiv.sabah.com.tr/2007/03/29/gun110.html>

Sabah. (2007b). Binalı Yıldırım: Türkiye örnek teşkil edecek. Retrieved from <http://arsiv.sabah.com.tr/2007/03/29/gnd87.html>

Sanal Suclar Sozlesmesi (n.d.). In Wikipedia. Retrieved May 22, 2015 from http://tr.wikipedia.org/wiki/Sanal_Su%C3%A7lar_S%C3%B6zleşmesi

Saymaz, İ., & Çelikkan, E. (2015). Turkey's top scientific body has no digital analysts left amid 'political' layoffs. Daily News. Retrieved from <http://www.hurriyetdailynews.com/turkeys-top-scientific-body-has-no-digital-analysts-left-amid-political-layoffs.aspx?pageID=238&nID=79394&NewsCatID=341>

Schleifer, Y. (2008). 'There are more people working on censoring the Internet than developing it'. Index on Censorship. Retrieved from <http://www.indexoncensorship.org/2008/10/there-are-more-people-working-on-censoring-the-internet-than-developing-it/>

Seçen, T. (2006). Müyap'ın Kapattırmaları İsyan Ettiriyor. Türk İnternet. Retrieved from <http://www.turk-internet.com/portal/yaziyaaz.php?yaziid=14551>

T.C. Kalkınma Bakanlığı. (2015). Bilgi Toplumu Stratejisi ve Eylem Planı. Retrieved from http://www.kalkinma.gov.tr/Lists/Yaynlar/Attachments/640/20152018_bilgi_toplumu_stratejisi_ve_eylem_plani.pdf

Taneja, H., & Wu, A. X. (2014). Does the Great Firewall really isolate the Chinese? Integrating access blockage with cultural factors to explain web user behavior. *Information Society*, 30(5), pp. 297-309.

The Center for Internet and Society. (n.d.). Wilmap: Turkey. Retrieved June 3, 2015 from <https://cyberlaw.stanford.edu/page/wilmap-turkey>

The New York Times (2015). Expediency in Turkey. The New York Times. Retrieved from http://www.nytimes.com/2015/04/03/opinion/expediency-in-turkey.html?_r=0

Tillman, E. R. (2014). The AKP's working class support base explains why the Turkish government has managed to retain its popularity during the country's protests. London School of Economics and Political Science. Retrieved from <http://blogs.lse.ac.uk/europpblog/2014/05/29/the-akps-appeal-to-the-working-class-explains-why-the-turkish-government-has-managed-to-retain-its-support-during-the-countrys-protests/>

Today's Zaman. (2015). Prosecutor orders detention of 28 from TÜBİTAK in new gov't-orchestrated operation. Retrieved from http://www.todayszaman.com/latest-news_prosecutor-orders-detention-of-28-from-tubitak-in-new-govt-orchestrated-operation_379171.html

Tufekci, Z. (2014). Everyone Is Getting Turkey's Twitter Block Wrong. Retrieved from <https://medium.com/message/everyone-is-getting-turkeys-twitter-block-wrong-cb596ce5f27>

Türkiye Büyük Millet Meclisi (TBMM). (2007). Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 Sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı ve İstanbul Milletvekili Gülseren Topuz'un; Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla

Mücadele Hakkında Kanun

Teklifi ile Adalet Komisyonu Raporu (1/1305, 2/958). Retrieved from <http://www.tbmm.gov.tr/sirasayi/donem22/yilo1/ss1397m.htm>

Twitter. (2015). Transparency Report. Retrieved May 22, 2015 from <https://transparency.twitter.com/removal-requests/2014/jul-dec>

Watson, I., & Tuysuz, G. (2014). Turkish PM vows to 'eradicate' Twitter, users see service disruptions. CNN. Retrieved from <http://edition.cnn.com/2014/03/20/world/europe/turkey-twitter-blackout/>

Wojcieszak, M. Smith, B. (2014). Will politics be tweeted? New media use by Iranian youth in 2011. *New Media & Society*, 16(1), pp. 91-109.

Wright, J. & Breindl, Y. (2013). Internet filtering trends in liberal democracies: French and German regulatory debates. *Internet Policy Review*, 2(2). DOI: 10.14763/2013.2.122

Yalçıntaş, A. (2015). Intellectual Disobedience in Turkey. In: Yalçıntaş, A. (ed) *Creativity and Humour in Occupy Movements*. New York, Palgrave MacMillan, pp.6-29.

Yazıcıoğlu, Y. (2011). In Panel: Bilişim Şuçları, Adalet Bakanlığı Hakim ve Savcı Adayları Eğitim Merkezi, p.31. Ankara.

Youtube Censorship (n.d.). In Wikipedia. Retrieved May 22, 2015 from https://en.wikipedia.org/wiki/Censorship_of_YouTube#.C2.AoTurkey