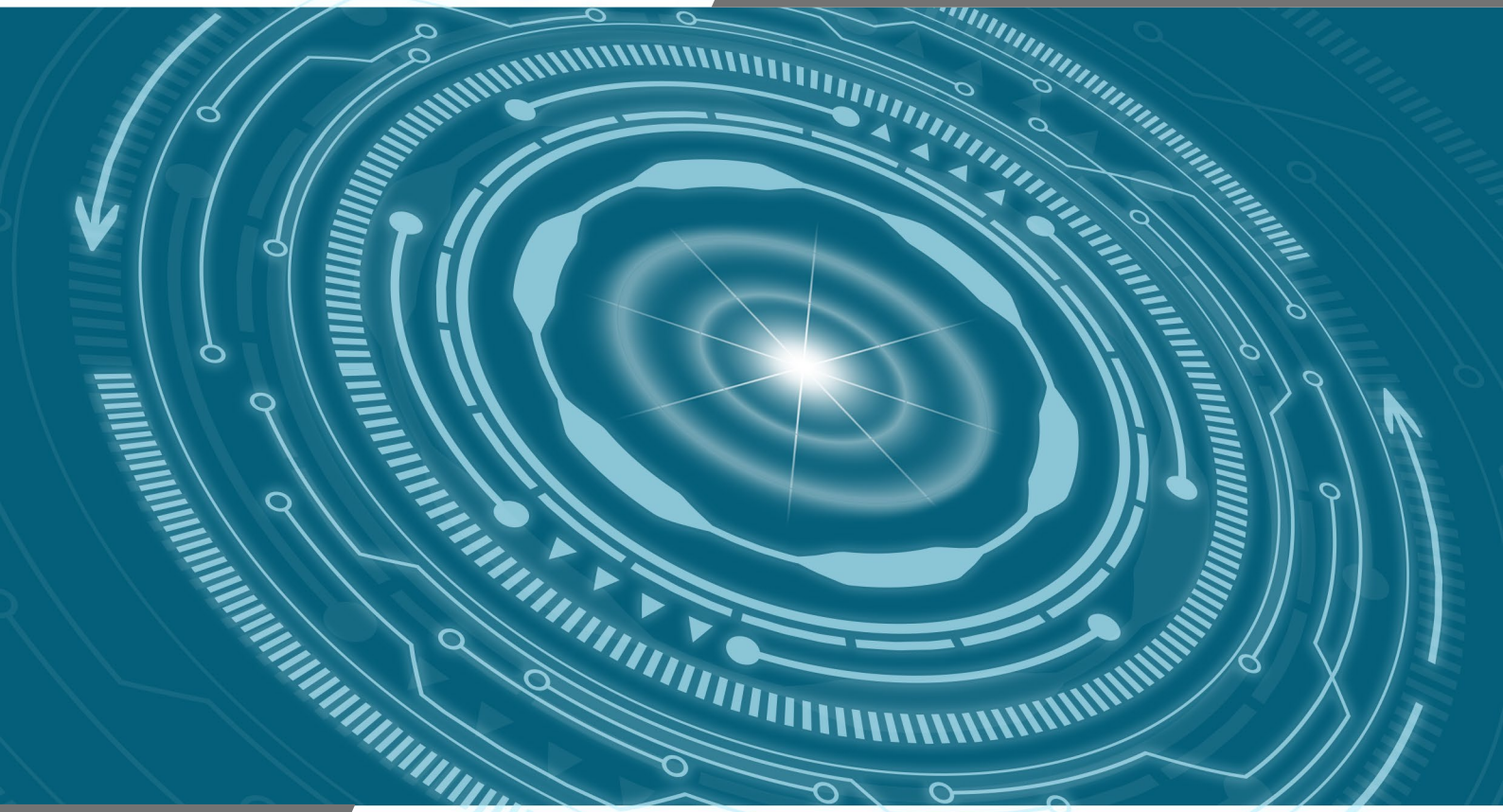
Centre for Economics and Foreign Policy Studies

edam

Cyber Governance and Digital Democracy 2018/1



April 2018

National Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy

Doruk Ergun | Research Fellow, EDAM

National Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy

Doruk Ergun | Research Fellow, EDAM

Executive Summary

Over the years Turkish authorities have accumulated significant legislative, judicial and technical capacity to block and monitor user activity online. Although these initially stemmed from 'safety' related concerns, national security has come to play a major role following significant social, political and security related developments after 2013.

The chronological overview of the surveillance and blocking practices of Turkish government and institutions suggests that the exacerbation and persistence of terrorism and conflict in Turkey and in its neighborhood has increased the demand for tighter control over online activity among Turkish authorities.

However, the increasingly 'security-first' outlook has not been balanced with due concern for rights and freedoms online, including privacy and freedom of expression. As a result, Turkish authorities have received criticism from the European Court of Human Rights, the Venice Commission, and international and domestic human rights organizations.

Furthermore, the existing internet governance architecture lacks adequate safeguards against deliberate or unintentional infringement of personal rights and freedoms online. A sobering display of this has been illegal surveillance, digital evidence tampering, and various other disruptive activities officially linked to the Gülen network – FETÖ.

In acknowledgement that neither national security concerns nor individual rights and freedoms are absolute, this paper presents five recommendations for moving beyond the internet governance vs. un-governance, privacy vs. surveillance, censorship vs. freedom of expression dichotomies, and improving the health of the debate in Turkey.

The public should be empowered as a stakeholder, with more attention paid towards improving overall digital literacy, bettering the dialogue between officials and the public, convincing the public on the economics of surveillance and censorship, and formulating the said decisions with input from the public in the first place.

As this critical issue concerns all Turkish citizens, an all-stakeholder approach to policy and legislation formulation is necessary. Turkish authorities should adopt a more pluralistic stance by empowering civil society, academia, political opposition, and the private sector's role in the debate. Beyond stakeholder engagement, this also entails improving the transparency of official actions online.

The prioritization of security and human rights should be balanced, including by developing non-securitized and less intrusive means of response (such as education on safe practices online instead of content blocking), training policy-makers, implementers, and the judiciary to improve the quality of administrative and legal decisions, and improving appeal mechanisms and remedies in case of any wrongdoing.

Judicial practices and legislation should also be improved in accordance with the recommendations of the Venice Commission, the verdicts of the European Court of Human Rights, and in line with the principles of the European Convention on Human Rights to which Turkey is a party of.

Finally, independent and effective oversight mechanisms should be established to monitor the surveillance and censorship architecture in the country, notably over implementers such as the Information and Telecommunications Authority – BTK, ideally through the equal representation of all political parties in the parliament, and with the ad hoc participation of external experts, such as academics, practitioners, and civil society.

The research has been made possible by funding obtained from the US based Chrest Foundation

1. Introduction

On December 1997, Ankara municipal law enforcement harshly responded to a public protest by visually impaired citizens, who had gathered to protest the municipality for neglecting to secure a public works site at which a visually impaired citizen was injured. 18-year-old Ali Emre Ersoz criticized the response in an online forum, which was reported to the authorities by an individual. Ersoz would subsequently be arrested by counter-terrorism units and receive a delayed 10-month sentence for publicly insulting and denigrating the state's security forces.[1] The incident marked the very first criminal sentence for an online post in Turkey[2] – at a time when the country did not have the legal and regulatory framework designed for publications on the internet.

In time, the country adapted its legal and regulatory infrastructure to better adjust to the transformative role of the internet. However, national security concerns often overrode the prioritization of human rights and freedoms online. Today, Turkey is ranked the 52nd out of 65 countries rated by the Freedom House's Freedom on the Net 2017 index.[3] On the other hand, Turkey faces a plethora of threats, which may indeed justify the prioritization of security concerns – out of 163 countries, Turkey is ranked 9th most impacted in the Global Terrorism Index[4] and the 146th least peaceful country in the Global Peace Index.[5]

This study looks at the national security vs. online rights and liberties nexus in the Turkish context. The paper will first provide a background on the institutional and regulatory developments in the country in its attempts to position itself in this equation. This background will be matched with the socio-political and security related developments in Turkey to provide a contextual understanding of the evolution of surveillance and censorship practices of Turkish authorities. The paper will then focus on the post-2013 period, characterized by one of the most monumental public protests in the country's history and a dual-crisis of corruption allegations and wiretapping of senior figures in 2013 and the reignition of the PKK conflict and expanding ISIS terrorist campaign in 2015-2016. Subsequent analysis will focus on the aftermath of the July 2016 coup attempt and the developments in online surveillance/censorship practices of the Turkish authorities as well as the changing institutional structure in the country.

The paper concludes by providing five mutually reinforcing recommendations for policy makers with an aim to bridge the legitimacy of the government's national security priorities and the rights and liberties of Turkish citizens online. These point to an all-stakeholder approach by strengthening the role of the public, civil society, private sector as well as the political opposition in the debate, acknowledgement of priorities beyond national security in cyber space and finding mechanisms to better limit the negative effects of security-based policies, and the establishment of independent and more effective checks and balances mechanisms for surveillance and censorship decisions. Finally, judicial processes and legislations also deserve a recalibration to better reflect European Convention on Human Rights criteria.

1 Hürriyet (1998, June 7) "İnternet'te Muhbir Var" (There are informants online) http://www.hurriyet.com.tr/internette-muhbir-var-38051055

2 İlkiz, F. (2001, Dec 05) "İnternet Ortamındaki Yayınlarda İki Olay ve İki Mahkumiyet Kararı ve Yasal Çalışmalar Üzerine Görüşler" Accessed from Türkiye Bilişim Şurası web page on 20 September 2014 from: www.bilisimsurasi.org.tr/dosyalar/45.doc also available at Bianet.com https://m.bianet.org/bianet/medya/2410-internet-yayinina-ceza-ve-anlami

3 Freedom House (2017) "Freedom on the Net 2017" https://freedomhouse.org/report/table-country-scores-fotn-2017

4 Vision of Humanity (2017) "Global Terrorism Index" http://visionofhumanity.org/indexes/terrorism-index/

5 Vision of Humanity (2017) "Global Peace Index" http://visionofhumanity.org/indexes/global-peace-index/

2. Security, Safety, Rights and Liberties Online in Turkey: A Brief Chronological Background

2.1. The Evolution of Turkey's Legislative and Institutional Architecture in the Cyber Realm

Turkey first introduced the concept of "Informatics Crimes" in its national legislation in 1991 which penalized the unlawful seizure of programs, data, and other elements from a computer system along with their use, transfer, or copy with the aim of harming an individual.[6] Whereas individuals such as Ali Emre Ersöz were subject to prosecution for their online activity based on existing legislation, it would take over a decade for the Turkish legal system to extend its framework into the cyberspace and develop specially designated legislation.

The scope of informatics crimes was extended in 2004 with the introduction of the new Turkish Penal Code no.5237, which penalized in articles 243 and 244 the illegal access to and the disruption of an IT system and unauthorized data removal and data modification.[7] Also pertinent for the issue at hand, the 2004 Penal Code included a section dedicated to offenses against privacy and secrecy of life. The section details six separate offenses, violation of communicational secrecy (art. 132), tapping and recording conversations (art. 133), violation of privacy (art. 134), recording of personal data (art. 135), unlawful delivery or acquisition of data (art 136.), and destruction of data (art. 138), all of which entail prison sentences. Article 137 asserts that if these crimes are committed a public officer or through the abuse of powers bestowed upon a public office, they are considered qualified crimes and the prison sentence is extended by half.[8]

2005 marked an important milestone towards the establishment of an institutional setting for internet oversight. Formed under the Telecommunications Authority – which would be transformed into the Information and Communications Technologies Authority (BTK) charged with regulating the telecommunications sector on 2008 – the Presidency of Telecommunication and Communication (TİB) would quickly gain the center of the stage as the organization responsible for surveilling, tracking, evaluating, and recording signal information and communications made through telecommunications tools, including the Internet. In essence, TİB acted as the centralized agency tasked with surveillance and interception of communications warrants as per laws No. 2559 on the Law on the Duties and Powers of the Police, No. 2803 on the Organisation, Duties and Powers of Gendarmarie, No. 2937 on State Intelligence Services and National Intelligence Organisation, and No. 5271, the Criminal Procedural Act.[9] TİB was also tasked with dealing the "safety" of the Internet service – regulating content, hosting providers, access/service providers, and public Internet use providers – as well as determining the minimum acceptable criteria for the production of hardware and software for filtering, masking, and surveilling online services. Until being dismantled and its powers transferred to the BTK in 2016, which will be discussed in depth below, TİB rested at the crux of the national security vs. online rights debate in Turkey.

In 2006, the ramifications for cybercrimes were further extended after the introduction of the two articles under the framework of the Anti-Terror Law (Law No. 3713). The law defines terror as:

"Terrorism is any kind of act done by one or more persons belonging to an organization with the aim of changing the characteristics of the Republic as specified in the Constitution, its political, legal, social, secular and economic system, damaging the indivisible unity of the State with its territory and nation, endangering the existence of the Turkish State and Republic, weakening or destroying or seizing the authority of the State, eliminating fundamental rights and freedoms, or damaging the internal and external security of the State, public order or general health by means of pressure, force and violence, terror, intimidation, oppression or threat."[10]

6 Turkish Grand National Assembly (Türkiye Büyük Millet Meclisi), "Law on Amending Certain Clauses of the 765-dated Turkish Penal Code" (765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun), Law No. 3756 Date of approval: 6.6.1991 (Official gazette publication: 14.6.1991, No: 20901) http://www.kanunum.com/files/kanun_tbmm_c074_03756.pdf also see: http://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d18/c061/b127/tbmm180611270516.pdf, Accessed on 16 July, 2014.

7 Turkish Penal Code (Türk Ceza Kanunu) (2004, September 26) Law no. 5237

8 Ibid.

9 Akdeniz, Y. (2009) "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship" Organization for Security and Co-operation in Europe The Representative on Freedom of the Media

10 Terörle Mücadele Kanunu (Anti-Terror Law) Law No. 3713 Published on the Official Gazette dated: 12.4.1991, No: 20843

The 2006 amendment further lists a series of crimes, including articles 243 and 244, and states that these crimes are "considered terror crimes if they are conducted as part of the activities of a terror organization established to carry out criminal actions with the aims listed in Article 1".[11] Beyond citing informatics crimes, it also refers to a series of articles that lie at the nexus of the freedom of expression and national security debate and may apply in the cyberspace as well. These include, article 213 on making threats to incite fear and panic among the public, article 214 on instigating criminal activity, article 215 on praising crime and criminal activity, article 300 on denigrating the symbols of the state's sovereignty, article 318 on alienating the public from military service and article 319 on promoting disobedience among military ranks.

Aside from the evolving cyber security legislation and the introduction of IT related offenses in the anti-terror legislation, the Turkish legal system also included clauses relevant to the freedom of expression and privacy debate that had yet to be adapted to technological developments but still applied to online activity. These included crimes against the state, notable examples of which are the denigration of the state, its symbols, the military and public officials; defamation and crimes against the honor and reputation of individuals; as well as Law No.5816 concerning crimes committed against Ataturk – the founder of the modern Turkish republic. Under crimes against public morality, the circulation of 'indecent' material such as pornography was also curtailed. These laws created the bases for banning access to 'illegal publications', with monetary penalties and/or prison sentences envisioned for those who create or circulate such content. Data from 2001 suggests that the Informatics Crime and Research Unit of the Turkish National Police (TNP) handled 21 cases of online illegal publications in 2000-2001, 40% relating to child pornography, 30% to terrorism, 25% to pornography, and 5% to defamation.[12] Subsequent incidents of blocking access to or taking down websites, ordered by courts and enforced by dial up Internet Service Providers (ISPs), included content on alleged corruption by Turkish officials and military personnel, anti-Turkish sentiments, terrorist propaganda, defamation, and gambling.[13]

The big legislative step shaping the security vs. liberty online debate in Turkey came in May 2007 with Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications – popularly referred to as the Internet Law. Article 8 of the Internet Law lists a catalogue of eight crimes, which form the grounds for blocking decisions if there is 'sufficient suspicion' that the online content constitutes these crimes. These catalogue crimes consist of seven crimes listed in the Turkish Penal Code No. 5237; (1) encouragement of suicide (art. 84), (2) sexual harassment of children (art. 103.1), (3) facilitating the use of drugs (art. 190), (4) supplying substances harmful to health (art. 194) , (5) obscenity (art. 226), (6) prostitution (art. 227), (7) arranging a place for or facilitating gambling (art. 228); plus for violating the Law no. 5816 on Crimes against Ataturk.[14]

Although it has been crucial for the internet freedoms debate in Turkey, the Internet Law and its future amendments which will be mentioned below are not directly at the focus of this analysis. This is because catalog crimes listed in the Internet Law play a little role, if any, in the national security dimension of the equation. Critical pieces of the puzzle that are indeed filtered, blocked, censored for national security purposes, such as online recruitment to terrorist organizations, terrorist propaganda, incitement of violence, are beyond the purview of the Internet Law and covered in separate pieces of legislation, such as the Anti-Terror Law. The Internet Law is perhaps more relevant in the surveillance debate, as it requires access and hosting providers to store traffic information and share it with authorities upon demand. Regardless of its limited application in the national security vs. online freedoms and rights axis, the Internet Law is included in the analysis because of its criticality in explaining the legislative and institutional framework of internet governance in Turkey, and how the Internet Law has been applied by Turkish authorities illuminates the practices and priorities of the Turkish government and judiciary.

[11] Terörle Mücadele Kanununda Değişiklik Yapılmasına Dair Kanun (Law on Amending the Anti-Terror Law) Law No. 5532 Published on the Official Gazette dated: 29.6.2006, No. 26232

[12] Dokurer, S. (2002) "Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri" (Informatics Crimes in our country and Means of Combating them) EGM Bilgi İşlem Daire Başkanlığı Bilişim Suçları Büro Amirliği, http://bilisimsurasi.org.tr/dosyalar/17.doc, Accessed on 23 September, 2014.

[13] Akdeniz, Y. (2009) "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship" Organization for Security and Co-operation in Europe The Representative on Freedom of the Media

[14] "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) Law no. 5851 Published on the Official Gazette dated: 23.5.2007, No: 26530

2.2. The Internet Law: Online Safety vs. Freedom of Expression

The law and subsequent Regulation on the Principles and Procedures of Regulating the Publications on the Internet released by BTK later that year,[15] state that content providers are responsible for all the content they publish online but are not liable for the content of any third party that they provide links to unless they are deemed to endorse or publicize the said content. Hosting providers are not obliged to check whether the pages that they host are involved in any illegal activity but are required to take down any illegal content if notified by a court or TİB. Access providers are similarly not liable for the content that is published using their services but are required to take action if notified by the authorities. Both hosting providers and access providers are required to obtain an "activity certificate" from BTK, and have to keep, secure and ensure the integrity of all traffic data for a period of six months and one year respectively.[16] Mass use providers, such as internet cafes, are required to receive a permission certificate from the local governmental administration and are obliged to take measures to prevent access to illegal content, such as using filtering tools approved by TİB.

The law states that if there is sufficient suspicion that a given content online falls under the catalog crimes listed above, the decision to block access to the content rests with the judge at the stage of investigation and with the court at the stage of prosecution. A public prosecutor may also decide on the blocking of access in cases of urgency for up to 24 hours, which can be extended upon the approval of the judge. If access and hosting providers fail to comply with the judge's or the court's decision to block access within 24 hours, they may face a prison sentence between 6 months and 2 years. Access providers who do not comply with TİB's administrative blocking orders may face administrative fines between 10.000 and 100.000 YTL (roughly 2.500 and 25.000 USD), and their activity certificates can be revoked by TİB if they fail to comply 24 hours after the administrative fine is issued. Furthermore, if the content or hosting providers of the content in question are based abroad, the decision to block access rests with TİB. The law also entailed a notice and takedown clause for individuals to appeal directly to content or hosting providers in case they feel that the content violates their personal rights. Unless the issue is resolved, the individual can take the issue to a peace court, which must decide on the matter in 3 days. In case the judge decides on the takedown of the content, failure to comply with the verdict within 48 hours the 'responsible party' can face prison sentences between 6 months and 2 years. As such, the law brought strong legal and financial deterrents for non-compliance with the blocking orders issued by TİB directly or by the judges and courts.

The law and its application have been criticized for a series of reasons. By not defining what 'sufficient suspicion' entails or what kind of content calls for restrictive measures, the law lacks foreseeability, a key principle of the Strasburg criteria.[17] This results in "uncertainty and arbitrary application of Law No.5651".[18] The failure of courts to provide reasons for their blocking decisions in most cases further compounds this issue. Hosting and content providers are not necessarily aware of what triggered the blocking decision as reasoned decisions are the exception rather than the norm according to Akdeniz.[19] This creates issues with transparency as well, especially when coupled with the fact that TİB stopped releasing information about blocked webpages since 2009.

The Media Association's Internet Committee further argues the rules brought for the law go against the free nature of the internet.[20] For example, the ability for TİB to impose

[15] See Regulation on the Principles and Procedures of Regulating the Publications on the Internet available at: https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FCommunique%2FREGULATION%20ON%20THE%20PRINCIPLES%20AND%20PROCEDURES%20OF%20REGULATING%20THE%20PUBLICATIONS%20ON%20THE%20INTERNET.pdf and for the original regulation in Turkish see: http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.11746&MevzuatIliski=0&sourceXmlSearch=internet%20ortam%C4%B1nda%20yap%C4%B1lan

[16] According to BTK's regulation, traffic information of the access provider refers to "information such as the name, identity, name and surname, address, telephone number of the subscriber and his/her date and time of connecting to the system, date and time of disconnecting from the system, the IP address granted for the related connection and the connection points regarding all kinds of access realized on the Internet" (article 3.g) whereas hosting provider traffic information refers to "information such as source IP address, target IP address, connection date and time, the address of the web page requested, process information (GET, POST command details) and result information in connection with all kinds of hosting on the internet." (article 3.ş) Ibid.

[17] See Deniz, Y. (2018) "Online Freedoms and the European Court of Human Rights: A Path Forward for Turkey" Centre for Economics and Foreign Policy Studies for further discussion.

[18] Akdeniz, Y. (2009) "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship" Organization for Security and Co-operation in Europe The Representative on Freedom of the Media p.25

[19] Ibid.

[20] Medya Derneği İnternet Komitesi (2010, July) "Türkiye'nin İnternet Sansürü Sorunu" (Turkey's Internet Censorship Problem)

blocking orders to any web page based abroad without any legal deliberation is in conflict with the international law and European Court of Human Rights (ECtHR) decisions. Akdeniz further argues that the powers bestowed upon TİB are unconstitutional as "decisions that interfere with the freedom of communication and right to privacy can only be given by the judiciary".[21] Precautionary blocking measures based on 'suspicion' often become permanent without the legality or illegality of content being determined by a court of law.[22] Blocking entire web pages over a limited amount of content is problematic as it does not offer a proportional response, and the methods used for blocking are not effective as methods of circumvention are possible.[23] Prime Minister Erdoğan's remark in 2008 when asked about the ongoing YouTube ban at the time "I enter [YouTube], you can too"[24] served to highlight this deficiency in effectiveness. More broadly, the law is criticized for not prioritizing freedom of expression and right to information concerns.[25]

The YouTube ban presents a good case in point for the excessive banning that the law entailed. The platform was banned briefly before the law was enacted over derogatory statements towards Atatürk. After facing short bans in 2007, YouTube faced a ban that lasted over two years starting in 2008. After Google attempted to circumvent the YouTube ban by diverting some of its IP addresses to the service in Turkey, BTK ended up banning the said IP addresses, which resulted in the inaccessibility of even more sites, including Google Maps, Docs, Translate, Code and Analytics.[26] Among other infamous bans were Wordpress, MySpace, Dailymotion, Vimeo, Blogspot[27] and LGBTIQ community webpages such as Gabile.com and Hadigayri.com.[28] Within the first two years of Law No.5651's entry into force, more than 2500 webpages were banned according to TİB statistics, over 80% of which were blocked by TİB's administrative orders and less than 20% blocked by court orders.[29] The majority of the pages were blocked for sexual harassment of children (42%) and obscenity (37%) concerns, followed by gambling and crimes against Atatürk. TİB also issued take down notices for an additional 380 webpages and written warnings to 25 pages during this time. TİB established a hotline for reporting potentially illegal activity and content online as required by Law 5651. By May 2009, it had received 81.691 calls. The majority of the 34,000 actionable calls it received were out of obscenity concerns (61,2%), followed by sexual harassment of children (14,1%), crimes against Atatürk (8.6%) and prostitution (8.3%).[30]

A positive step towards improving the law and addressing the concerns of civil society came in the form of a workshop between official stakeholders, such as TİB, Ministry of Justice, Turkish National Police, military courts, along with service providers, online platforms, media organizations, academia and civil society organizations.[31] After holding the first workshop on June 2008 in Abant, the participants of the second workshop at Kartepe on April 2010, agreed upon 13 principles for internet governance, including those that underline the democratic and pluralistic nature of the internet, call for less restrictive blocking measures such as self-regulation mechanisms, improving transparency, strengthening the legality, proportionality and necessity criteria of blocking decisions, clarifying institutional and legal responsibilities, expanding the online literacy of officials and the general public, restructuring the catalog crimes, joining the Council of Europe's Convention on Cybercrime, establishing specialized courts, and promoting

[21] Akdeniz, Y. (2009) "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship" Organization for Security and Co-operation in Europe The Representative on Freedom of the Media p.34

[22] Ibid.

[23] Ibid.

[24] Hurriyet (2008, November 21) "Başbakan: Ben Youtube'a giriyorum" (Prime Minister: I enter Youtube) http://www.hurriyet.com.tr/basbakan-ben-youtubea-giriyorum-10411487

[25] OSCE.org (2010, January 18) "Turkey's Internet law needs to be reformed or abolished, says OSCE media freedom representative" https://www.osce.org/fom/51828; Akdeniz, Y. (2009) "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship" Organization for Security and Co-operation in Europe The Representative on Freedom of the Media; Medya Derneği İnternet Komitesi (2010, July) "Türkiye'nin İnternet Sansürü Sorunu" (Turkey's Internet Censorship Problem)

[26] Medya Derneği İnternet Komitesi (2010, July) "Türkiye'nin İnternet Sansürü Sorunu" (Turkey's Internet Censorship Problem)

[27] Akgül, M.; Kırlıdoğ, M. (2015, June 3) "Internet censorship in Turkey" Internet Policy Review Vol.4 Issue.2

[28] OSCE.org (2010, January 18) "Turkey's Internet law needs to be reformed or abolished, says OSCE media freedom representative" https://www.osce.org/fom/51828; Akdeniz, Y. (2009) "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship" Organization for Security and Co-operation in Europe The Representative on Freedom of the Media

[29] Akdeniz, Y. (2009) "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship" Organization for Security and Co-operation in Europe The Representative on Freedom of the Media

[30] Ibid.

[31] For list of participant organizations, see https://web.archive.org/web/20100426071608/http://5651calistay.org/calistay-hakkinda/katilimcilar/

free parental control filters.[32] Unfortunately, against the consensus reached by officials and civil society on these critical issues, most of the criteria would not be met in the years to come.

In 2011, TİB and BTK took further action to ensure and enforce safety online. In an attempt to filter obscene content, TİB created a list of 138 keywords (such as hot, naked, escort) and urged Turkish hosting companies to ban domain names that included these words.[33] Under the "Safe Use of the Internet" program, BTK planned to make it mandatory for every user to install an internet filtering system in their computers and choose among the child, family, domestic, and standard packages. Upon mounting criticism from the civil society and academia, BTK revised its plans and created a voluntary program for individual internet users that offered child and family filtering options. The family plan however is voluntary for public use providers such as internet cafes and reportedly blocks more than 1.5 million websites.[34]

2.3. Beyond the Internet Law: The Security Dimension

More pertinent for the security discussion has been the blocking decisions carried out outside the scope of the Internet Law. Blocking decisions for reasons outside of the catalog crimes listed under Law No 5651, such as denigrating Turkish nation, state of the Republic of Turkey, the organs and institutions of the State (Penal Code Art.301) and the Anti-Terror Law were decided upon by civilian and military courts and enforced by TİB. Data on how many such sites were banned are challenging to obtain, as there is limited available information on the reasons for the blocking of a particular webpage, and the primary online platform cataloging blocked webpages in Turkey and one of the primary sources for researchers on the issue, engelliweb.com, has been closed since 2017. However, the usual suspects of such blocking decisions tend to be left-wing, pro-Kurdish, and right-wing fundamentalist websites, such as revolutionary associations, 'alternative' news pages, and online platforms – as well as webpages that are directly linked to terrorist organizations.[35] Such websites are likely blocked under the charges of disseminating terrorist propaganda (or other clauses in the Anti-Terror Law), denigrating Turkishness (Penal Code Art. 301), offences against public peace, such as causing fear and panic among the public (Penal Code Art. 213), praising an offence or offender (Penal Code Art. 215), provoking the public to hatred and hostility (Penal Code Art. 216), as well as discouraging people from performing military service (Penal Code Art. 318).

Some such blocking decisions have received criticism for being "arbitrary and political, and therefore incompatible with OSCE's freedom of expression commitments".[36] While it is beyond the scope and intent of this article to verify the legality and neutrality of court decisions, it is worth mentioning that Turkey has been convicted by the ECtHR for restricting the publication of Özgür Gündem, which has also faced blocking decisions for its online presence. The said newspaper has been a controversial outlet in Turkey and faced restrictions numerous times by Turkish authorities, more recently being shut down temporarily for "making PKK propaganda and serving as the press outlet for the terrorist organization".[37] In the Case of Ürper and Others v. Turkey (2009), ECtHR ruled that the decision of the Turkish courts to block future publications of Özgür Gündem and other outlets over their violation of the Anti-Terror Law "largely overstepped the narrow margin of appreciation afforded to [domestic courts] and unjustifiably restricted the essential role of the press as a public watchdog in a democratic society"[38] and was in violation of Article 10 of the European Convention as the decision "went beyond any notion of "necessary" restraint in a democratic society and, instead, amounted to censorship".[39] Therefore, regardless of whether the content published by the outlet violated the Anti-Terror Law, or whether the decision of Turkish courts

[32] For the list of the criteria please see https://web.archive.org/web/20100430151220/http://5651calistay.org/

[33] Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory

[34] Ibid.

[35] Akdeniz, Y. (2009) "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship" Organization for Security and Co-operation in Europe The Representative on Freedom of the Media

[36] OSCE.org (2010, January 18) "Turkey's Internet law needs to be reformed or abolished, says OSCE media freedom representative" https://www.osce.org/fom/51828

[37] NTV (2016, August 16) "Özgür Gündem gazetesi geçici olarak kapatıldı" https://www.ntv.com.tr/turkiye/ozgur-gundemgazetesi-gecici-olarak-kapatildi,o3ccmDtc_kye3wdsl1v_XQ

[38] European Court of Human Rights (2009, October 20) "Case of Ürper and Others v. Turkey (Applications nos. 14526/07, 14747/07, 15022/07, 15737/07, 36137/07, 47245/07, 50371/07, 50372/07 and 54637/07) Judgment" Art. 44 pp.11-12

[39] Ibid.

was based on national security or political priorities, ECtHR considered the Turkish courts' decision to suspend the publication and distribution of future news outlets even for short periods were "draconian" measures, suggesting "the confiscation of particular issues of the newspapers or restrictions on the publication of specific articles"[40] as more proportionate responses. The case and its verdict may be considered relevant to the practice of blocking access to entire webpages rather than filtering/blocking specific content that is deemed to be illegal, as blocking a webpage not only prevents access to the illegal content but any other existing and future content on the webpage that may not be in violation of any laws. The reliance on blocking webpages rather than content removal has been a main source of the debate in Turkey.

3. From Safety into Security: Turkey's Changing Online and Offline Scene After 2013

3.1. Gezi Park Protests and December 17-25 Events

Whereas the online rights and freedoms debate in Turkey mainly revolved around 'safety' in the first two decades of internet access in Turkey, security concerns came to play a major role in official policies and legal decisions after 2013. Between May and August 2013, Turkey experienced one of the largest public protests in its history, dubbed the Gezi Park Protests. What started out as a small-scale sit in over environmental concerns in Istanbul, quickly grew into a mass movement mobilizing millions across Turkey after images of police brutality towards the original protesters was publicized on social media. Social media played a key role throughout the protests, in facilitating the mobilization of protesters, and in informing (and often misinforming) the public – a fact exacerbated by the lack of traditional media coverage on the protests. The very same year on 17-25 December, Turkey was rocked by a wave of arrests and police investigations surrounding an alleged corruption ring, involving 4 ministers and some of their relatives, as well as a series of businesspeople and officials. The arrests were accompanied by a series of alleged voice recordings leaked over the internet. Over the course of 2014, dozens of such 'tapes' would surface, including alleged wiretap recordings of encrypted telephones belonging to high-profile Turkish politicians and surveillance recordings from secure offices in governmental offices. The tapes have subsequently been linked to the Gülen network.

Both developments convinced Ankara on the need to take further steps to increase its capabilities on regulating online content and surveillance. On the first front, the Internet Law was amended on February 2014. The amended law requires all access providers in Turkey to form become a member of the Access Providers Union, tasked with implementing the blocking decisions within four hours of being notified. The burden of acquiring necessary hardware and software for blocking decisions falls to the access providers – which were to the detriment of small-medium sized providers who could not invest in such technologies according to critics.[41] The law further expanded TİB's authority to impose blocking decisions, such as by granting the TİB President the ability to unilaterally block content for up to 24 hours before receiving approval from a court for the extension of the decision (which in turn has 48 hours to decide on the matter). It necessitates hosting providers to also keep user traffic information for up to two years and share this information with authorities upon demand, drawing criticism for surveillance concerns.

The amendment also took steps to address some criticism towards the proportionality and effectiveness of blocking decisions. The amendment states that webpage blockings should be used as a last resort if content removal can satisfy the issue at hand – though unfortunately the number of blocked webpages has continued to increase. With regards to effectiveness, by introducing new access ban procedures, the law made it harder to bypass its blocking decisions, making it "nearly impossible to access banned content by changing DNS settings".[42]

[40] European Court of Human Rights (2009, October 20) "Case of Ürper and Others v. Turkey (Applications nos. 14526/07, 14747/07, 15022/07, 15737/07, 36137/07, 47245/07, 50371/07, 50372/07 and 54637/07) Judgment" Art. 43 p.11

[41] Gürkaynak, G. et al. (2014, November) "New Era for Turkish Internet Law: Will Turkey Become Another China or Iran?" Journal of Business and Economics Volume 5, No. 11, pp. 1976-1982

[42] Gürkaynak, G. et al. (2014, November) "New Era for Turkish Internet Law: Will Turkey Become Another China or Iran?" Journal of Business and Economics Volume 5, No. 11, p. 1980

The amendment also introduces the right to privacy to the law, allowing individuals to directly apply to the TİB Presidency for the removal of content that allegedly harms their privacy. The individual should provide the specific URL of the content for their claim to be processed. The request is then communicated to the Access Providers Union, which has to act within four hours. However, TİB can also directly block content upon the decision of its President if the decision must be taken without delay for privacy concerns. As with other instances, TİB's decision should be presented to a judge within 24 hours, who then has to decide on the matter on 48 hours, otherwise the blocking decision is automatically nullified. While it introduces privacy into the legislation, this amendment has received criticism for defining a timeframe for implementing a blocking decision – four hours – without providing any time limit for uplifting blocking decisions, meaning that even if they are nullified, blocking decisions may remain in place.[43] Another criticism has been that the amendment gives TİB, an administrative body, judicial powers which should solely rest with judicial bodies.[44] Another amendment passed in March 2015 further expanded TİB's powers by giving it the right to control the removal of content and prevention of access to web pages "in cases where the delay of a decision could endanger the protection of the right to life, the protection of the life and private property of the people, the protection of national security and public order, prevention of crime or the preservation of the public health, upon demand by the Prime Ministry or ministries dealing with national security and the protection of the public order, prevention of crime or the preservation of public health."[45] After TİB decides to remove content or block access to a page, it notifies the related access, content, and hosting providers, who then must take action within four hours. Failure to comply with TİB's request results in an administrative penalty ranging from 50,000 to 500,000 TL ($13,000-130,000 USD).

On the surveillance front, the Turkish government also amended the Law on State Intelligence Services and the National Intelligence Agency after the developments in 2013. The amendment dated 17 April 2014 gives the National Intelligence Agency (MIT) the ability to use any technical and human intelligence means necessary to collect, record, analyze and share information, documents, news and data pertaining to foreign intelligence, national security, counterterrorism, international criminal acts, and cyber security.[46] It also gives MIT the mandate to research, develop and procure modern intelligence methods and technologies that can improve the capacity, quality and effectiveness of intelligence services.[47] The amendment gives MIT the authority to collect data on foreign intelligence, national security, terrorism, international crime and cyber security matters transmitted through telecommunication channels. MIT furthermore gained the authority to prevent the acts of 'foreign elements' that threaten the security of communications of the country and its citizens.[48] Furthermore, all institutions and entities, public and private, have to comply with MIT's requests for access to their data and archives, lest they face a prison sentence between 2 and 4 years. The law also takes strong measures against any sort of whistleblowing activity, punishable with prison sentences up to 9 years. Moreover, a 2015 amendment to the Law on the Duties and Responsibilities of the Police expanded the timeframe for the Turkish National Police (TNP) to surveil telecommunications in urgent conditions from 24 hours to 48 hours.[49]

In addition to the legislative steps, Turkish authorities also gradually expanded their technical capacities on the surveillance front. Reports suggest that Turkish agencies and companies used numerous spyware programs, though it is unclear which agencies or companies used these spywares and the data gathered through them, and the duration that they were used. These include;
"1) Phorm, a program that "collects information on users' online behavior without their knowledge, performs deep-packet inspection (DPI) to monitor a user's connection line, and creates a profile of the individual's online activities," 2)

[43] Akgül, M.; Kırlıdoğ, M. (2015, June 3) "Internet censorship in Turkey" Internet Policy Review Vol.4 Issue.2

[44] Gürkaynak, G. et al. (2014, November) "New Era for Turkish Internet Law: Will Turkey Become Another China or Iran?" Journal of Business and Economics Volume 5, No. 11, pp. 1976-1982; also see European Commission for Democracy Through Law (2016, June 15) "Turkey: Opinion on Law No. 5651" Opinion No. 805 / 2015 Adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)

[45] Law No. 5651 Article 8/A (Amendment made on 27 March 2015 - 6639/29) Accessible from: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

[46] "Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun" (Law on Changing the Law on the State's Intelligence Services and the National Intelligence Agency) Law No: 6532 Art 4.i, published on Official Gazette dated 26 April 2014 No. 28983

[47] Ibid. Art. 4.j.

[48] Ibid. Art. 6.h.

[49] "Polis Vazife ve Salâhiyet Kanunu, Jandarma Teşkilat, Görev ve Yetkileri Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" (The Law on Amending the Law on Police Duties and Responsibilities of the Police, Law on Gendarmerie Duties and Responsibilities, and other laws) Law No: 6638 published on Official Gazette dated 4 April 2015

Package Shaper, a program used for internet filtering and surveillance; 3) Remote Control Systems that is produced by the Italian company Hacking Team, and FinFisher that is produced by the UK-German company Gamma International, both of which enable the interception of passwords and emails as well as the remote control of a device's microphone to record conversations, and 4) Deep Packet Inspection (DPI) technology provided by Procera Networks that Turk Telekom (the largest [internet service provider] in Turkey) has used since at least 2014 for mass surveillance of internet traffic."[50]

Indeed in 2012, Turk Telekom, or rather its subsidiary TTNET was fined 1.5 million TL ($390.000) by BTK for its partnership with Phorm, which it used to collect data from and push targeted advertisements, even from users that did not opt for TTNET's travel services.[51] The verdict was praised for officially documenting TTNET and Phorm's collection of data without consent, deliberately misleading users, stating that TTNET and Phorm resorted to phishing and ordering this practice to be terminated, and requesting TTNET to remove all users it registered to its travel service (many without their consent) and properly inform and receive the consent of future users.[52] Against the precedent it served, the verdict was also criticized for failing to mention the Deep Package Inspection infrastructure – which allows tracking data traffic online and establishing user profiles – that Phorm had set up for TTNET and the threat this poses to privacy and private data.[53] Indeed, such profiling may not only be used for targeted advertisement purposes, but also "to determine the political, religious and sexual orientation of the user as well as his/her membership to political parties, trade unions and other communities".[54] Phorm's operations were shut down briefly as a result of the verdict, only to resume in April 2013.

3.2. The (In)Security in 2015-2016

In the 2013-2014 timeframe, increasing potential for social unrest, and an internal adversary aiming to undermine the Turkish government (namely, the Gülen network which will be discussed in more depth below) triggered the government to expand its control and monitoring over the Internet. The next two years, however, would be characterized with an (in)security situation engulfing the country, marked with terrorism, conflict, and a bloody coup attempt. Between June 2015 and January 2017, over 500 people lost their lives to terrorist attacks perpetrated by the PKK, ISIL and others, and around 2100 were wounded[55] – this excluding ISIL's rocket attacks and the PKK's reignited conflict in the southeast.

On the one hand, following the breakdown of the Kurdish peace process in 2015, the Kurdistan Workers' Party (PKK) resumed its terrorist campaign. The PKK followed a two-pronged approach of triggering a low-intensity conflict in its traditional area of activity in south-eastern/eastern Turkey, while the organization and its off-shoots conducted major terrorist attacks against government and civilian targets in major cities throughout the country. The former resulted in a prolonged, sporadic conflict between Turkish security forces and the PKK that continues to this day, albeit at a much lower pace compared to the second half of 2015 and first half of 2016. According to official sources, the operations resulted in the death of over 3,500 militants and 400 Turkish security forces.[56] According to OHCHR,

[50] Yeşil, B.; Sözeri, E.K. (2017) "Online Surveillance in Turkey: Legislation, Technology and Citizen Involvement" Surveillance & Society 15(3/4) p. 546; also see Forbes (2016, October 25) "Is An American Company's Technology Helping Turkey Spy On Its Citizens?" https://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francis-co-partners-turkey-surveillance-erdogan/#631780404434 ; Hurriyet Daily News (2015, July 9) "Turkish police paid 440,000 euros to hackers for spyware" http://www.hurriyetdailynews.com/turkish-police-paid-440000-euros-to-hackers-for-spyware-85183 ; The Citizen Lab (2018, March 9) "BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?" https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

[51] For more, see Türkiye Büyük Millet Meclisi (2013, June) "Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması Komisyon Raporu" (The Report of the Parliamentary Research Commission on Determining and Taking Preventative Measures for Violations to the Freedom of Communication and Privacy) available at: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss489.pdf

[52] BThaber.com (2012, December 17) "BTK'nın TTNET ve Phorm soruşturmasında karar açıklandı" (The verdict of BTK's inquiry on TTNET and Phorm was declared) http://www.bthaber.com/bilisim-dunyasi/btk%E2%80%99nin-ttnet-ve-phorm-sorusturmasinda-karar-aciklandi/1/6732

[53] Ibid.

[54] Akgül, M.; Kırlıdoğ, M. (2015, June 3) "Internet censorship in Turkey" Internet Policy Review Vol.4 Issue.2 p.10

[55] Diken (2016, December 12) "Bir buçuk yılda 33 bombalı saldırıda 461 kişi hayatını kaybetti; 363'ü sivil" (In a year and half, 461 people lost their lives in 33 bomb attacks, 363 of which were civilians) http://www.diken.com.tr/bir-bucuk-yilda-33-bombali-saldirida-461-kisi-hayatini-kaybetti-363u-sivil/ ; NTV (2017, January 2) "Reina gece kulübüne terör saldırısı: 39 kişi hayatını kaybetti" (Terrorist attack on the Reina night club: 39 lost their lives) https://www.ntv.com.tr/turkiye/reina-gece-kulubune-teror-saldirisi-39-kisi-hayatini-kaybetti,ZiTsOjXOJE-yOXaDjQ8WqQ

[56] Milliyet (2016, May 23) "TSK: 7 bin 78 terörist öldürüldü" (TSK: 7078 terrorist killed) http://www.milliyet.com.tr/tsk-7-bin-78-terorist-olduruldu-gundem-2250378/ ; Hurriyet (2016, May 24) "10 aylık operasyon bilançosu: 7 bin 78 PKK'lı etkisiz hale getirildi" (The result of 10 months of operations: 7078 PKK members were neutralized) http://www.hurriyet.com.tr/gundem/10-aylik-operasyon-bilancosu-7-bin-78-pkkli-etkisiz-hale-getirildi-40108080

citing government sources, 323 civilians lost their lives and 2040 were wounded, with another 231 kidnapped by the PKK and over 350,000 displaced.[57]

On the other hand, the Islamic State of Iraq and the Levant (ISIL) also followed a two-pronged terrorism campaign against Turkey through its cells based in Turkey and militants that crossed into Turkey to conduct attacks. The organization initially targeted politically and societally sensitive targets as the country was nearing a contentious election cycle, such as political gatherings, and later a peace rally in Ankara on 10 October 2015 that marked the biggest terrorist attack in the country's history, claiming over 100 lives and wounding over 500. It then targeted Turkish security forces, touristic destinations, such as Taksim Square and Sultanahmet, critical infrastructure, such as the Istanbul Ataturk Airport, as well as the facets of everyday life, including a wedding in Gaziantep and a nightclub in Istanbul during New Year's Eve celebrations. Turkish authorities prevented a further 22 attacks in 2016 alone.[58] In the following year, Turkish authorities arrested 739 and detained 4765 suspects with alleged ties to ISIL.[59] Another leg of ISIL's terrorist campaign consisted of rocket attacks into Turkish border towns, launched from ISIL held territories in Syria. Over 20 civilians were killed by over 70 rockets fired from ISIL held territories before the Turkish military operations in Syria.[60]

An increasingly visible practice of the Turkish authorities during this period was limiting access to social media and news webpages through a practice called bandwidth throttling – intentionally slowing down (or speeding up) available bandwidth (internet speed) by internet access/service providers. Throttled webpages would not be blocked but essentially inaccessible due to the bottlenecks created by the service providers. Another mean employed to this end was DNS poisoning, which renders the given webpage inaccessible by redirecting users to incorrect IP addresses. Allegedly, Turk Telekom hijacked Google DNS servers in 2014 "to "comply with [the] government's banning of [Twitter and YouTube]" by "giving users false information." Not only were users blocked from their intended destination, but also the "IP addresses of [their] devices attempting to reach the two services using foreign DNS servers" were also logged by the government."[61] These practices reportedly followed significant political and security developments, some examples of which are listed in the table below. Turkish media sources have also reported instances where curfews imposed on mostly southeastern towns as part of the counterterrorism operations against the PKK were also coupled with cutting access to the internet and mobile networks.[62] The Turkish Radio and Television Supreme Council (RTÜK) often imposed bans on broadcasting images pertaining to security incidents.[63] Yet the Freedom House notes that:

"Facebook, Twitter, and YouTube were briefly blocked or throttled until they complied with court orders to remove "criminal" content, including images and videos related to deadly bombings in Suruç, Ankara, and Istanbul… Restrictions on social media platforms occurred within 1-2 hours of each incident, indicating authorities may have sent more informal orders to ISPs prior to the official orders."[64]

[57] Office of the United Nations High Commissioner for Human Rights (2017, February) "Report on the human rights situation in South-East Turkey: July 2015 to December 2016" http://www.ohchr.org/Documents/Countries/TR/OHCHR_South-East_TurkeyReport_10March2017.pdf

[58] Barrett, R. (2017, October) "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees" The Soufan Center

[59] Hurriyet Daily News (2018, January 3) "739 arrested, 4,765 detained in Turkey's 2017 fight against ISIL" http://www.hurriyetdailynews.com/739-arrested-4-765-detained-in-turkeys-2017-fight-against-isil-125193

[60] BBC (2016, May 29) "Syria conflict: Kilis, the Turkish town enduring IS bombardment" http://www.bbc.com/news/world-europe-36245505

[61] Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory p.12

[62] Hurriyet (2015, September 5) "Sokağa çıkma yasağı uygulanan Cizre'de büyük operasyon" (Major operation in Cizre where a curfew is in place) http://www.hurriyet.com.tr/gundem/sokaga-cikma-yasagi-uygulanan-cizre-de-buyuk-operasyon-29996079

[63] For some examples: Independent (2015, 10 October) "Ankara terror attack: Turkey censors media coverage of bombings as Twitter and Facebook 'blocked'" http://www.independent.co.uk/news/world/europe/ankara-terror-attack-turkey-censors-media-coverage-of-bombings-as-twitter-and-facebook-blocked-a6689036.html ; Hürriyet (2015, 31 March) "Savcı Mehmet Selim Kiraz'ın rehin alınması olayına yayın yasağı" (Broadcast ban on prosecutor Mehmet Selim Kiraz's kidnapping) http://www.hurriyet.com.tr/gundem/savci-mehmet-selim-kirazin-rehin-alinmasi-olayina-yayin-yasagi-28607510

[64] Freedom House (2016) "Freedom On The Net 2016: Turkey" https://freedomhouse.org/report/freedom-net/2016/turkey

Date	Incident	Content Restriction
3 April 2015	A prosecutor in Istanbul taken hostage and killed by left-wing terrorist organization DHKP-C	166 URLs blocked including news articles, and Facebook, Twitter, YouTube content
20 July 2015	Suicide bombing in gathering in Suruç by ISIL	173 URLs blocked including 38 news websites
10 October 2015	Twin suicide bombing in peace rally in Ankara by ISIL	Facebook and Twitter throttled
12 January 2016	Suicide bombing attack in touristic Sultanahmet area in Istanbul by ISIL	RTÜK issued media and broadcasting blackout
17 February 2016	Car bombing by PKK offshoot TAK targeting military personnel in Ankara	Facebook and Twitter throttled
13 March 2016	Car bombing by TAK in a bus stop in Ankara	Facebook and Twitter throttled, 214 URLs blocked
19 March 2016	Suicide bombing by ISIL in touristic Taksim are in Istanbul	Facebook and Twitter banned for 24 hours
28 June 2016	Shooting and suicide bombing attack in Istanbul Ataturk Airport by ISIL	Facebook and Twitter throttled
15 July 2016	Coup attempt	Facebook and Twitter briefly throttled
11 September 2016	28 elected mayors in southeastern Turkey are removed from office and replaced by government appointed administrators	Landline and mobile internet access cut in 15 cities
8 October 2016	Email archive of the Energy Minister leaked	Google Drive, GitHub, Dropbox, One Drive blocked
04 November 2016	Arrests of members of parliament from pro-Kurdish opposition party HDP	Facebook, Twitter, YouTube, WhatsApp, Skype, Instagram throttled
04 November 2016	Car bombing in Diyarbakır by PKK (claimed also by ISIL)[65]	Social media blocks intensify, reportedly some GSM operators shut down mobile internet access temporarily.[66] Access to VPN services banned.[67]
19 December 2016	Assassination of Andrei Karlov, Russian Ambassador to Turkey	Facebook, Twitter and YouTube throttled

Table 1: Examples of internet restrictions after significant political and security related events[68]

[65] T24.com.tr (2016, December 12) "Gün gün 2016'daki bombalı saldırılar ve failleri" (Every bomb attack in 2016 and their perpetrators) http://t24.com.tr/haber/gun-gun-2016daki-bombali-saldirilar-ve-failleri,376359

[66] Hurriyet (2016, November 4) "İnternet erişimi engellendi" (Internet access blocked) http://www.hurriyet.com.tr/ekonomi/internet-erisimi-engellendi-40268817

[67] Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory p.14

[68] Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory pp.12-14; Turkey Blocks (2016, November 4) Facebook, Twitter, YouTube and WhatsApp shutdown in Turkey https://turkeyblocks.org/2016/11/04/social-media-shutdown-turkey/

Freedom House further notes that "Turkey accounted for almost 90 percent of all content that was locally restricted by Twitter in the second half of 2015. Turkey's regulator fined the company TRY 150,000 (US$ 51,000) for refusing to remove what it termed "terrorist propaganda" from the site",[69] and that Turkish authorities also resorted to temporary filtering of specific hashtags related to bombing sites from Instagram. Some critics argue that these measures were aimed at "suppress[ing] critical reporting and to prevent citizens from mobilizing"[70] whereas others suggest that these methods are essentially blocking decisions but those that cannot be appealed legally because they are not taken based in any administrative decisions or court decisions.[71]

Government sources maintain however, that these measures are taken as national security precautions. Speaking about the inaccessibility of social media during the arrests of HDP MPs, Turkish Prime Minister Binali Yıldırım noted that "These precautions can be resorted to for security reasons from time to time. These are temporary measures. Once the threat is overcome, things will return to normal."[72] Others have suggested that instead of a deliberate slowdown, these were mere congestions from high demand to social media platforms: "in the wake of major developments, including terror attacks, more users try to access social media platforms and the increased demand inevitably slows down the Internet" according to a senior official interviewed by Reuters.[73] On the other hand, BTK has noted on at least one occasion[74] that sharing content about terrorist attacks serves to advance terrorist causes and propaganda, urging citizens to take necessary steps to refrain from sharing such content, and asserting that BTK will take legal means necessary against those that spread such content. According to the BTK press release after the terrorist attack at Istanbul Ataturk Airport:

"It is assessed that sharing these images [of the moment of the attack and the victims], the broadcasting of which are also banned by the court's orders, serves the purpose of this vile terrorist attack intentionally or unintentionally. Therefore, we expect our citizens to show the necessary sensibility about sharing such content (tweet, retweet etc.) on the internet and especially on social media, which also have legal liabilities. Those who deliberately share content aimed at provoking the public and terrorizing the public are liable legally. Under the relevant legislation on protecting national security, public order, and safety, every legal measure will be taken through the pertinent institutions against those who serve the aim of terrorism by broadcasting or sharing these images."[75]

3.3. The 15 July 2016 Coup Attempt and its Ramifications for the Debate

The coup attempt of 15 July 2016 caused yet another shocking deterioration in the security situation in the country. 248 people lost their lives, along with 24 coup plotters,[76] with over 2,100 people wounded in the bloody attempt.[77] The Turkish government maintains that the coup attempt was orchestrated by Fetullah Gülen and his network, which Turkey recognizes as the Fetullahist Terrorist Organization (FETÖ).[78] In the still ongoing process to crackdown on alleged suspects of the network and its affiliates in Turkey, 169.013 people underwent legal action,

[69] Freedom House (2016) "Freedom On The Net 2016: Turkey" https://freedomhouse.org/report/freedom-net/2016/turkey

[70] Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory p.11

[71] Voice of America (2016, June 29) "Türkiye'de Sosyal Medyaya Neden Erişilemiyor?" (Why Is Social Media Inaccessible in Turkey?) https://www.amerikaninsesi.com/a/turkiye-de-sosyal-medya-ya-neden-erisilemiyor/3397085.html

[72] Hurriyet (2016, November 4) "İnternet erişimi engellendi" (Internet access blocked) http://www.hurriyet.com.tr/ekonomi/internet-erisimi-engellendi-40268817

[73] Reuters (2016, July 7) "Turkey appears to be in vanguard of 'throttling' social media after attacks" https://www.reuters.com/article/us-mideast-crisis-socialmedia/turkey-appears-to-be-in-vanguard-of-throttling-social-media-after-attacks-idUSKCN0ZM2O3

[74] HaberTurk (2016, August 21) "BTK Başkanı Sayan'dan terör saldırısı sonrası sosyal medya uyarısı" (Warning from BTK Head Sayan on social media after the terror attack) http://www.haberturk.com/gundem/haber/1285189-btk-baskani-sayandan-teror-saldirisi-sonrasi-sosyal-medya-uyarisi

[75] Republic of Turkey Information and Communication Technologies Authority (2016, June 28) "Basın Açıklaması: Terör Saldırısına İlişkin Paylaşımlar" (Press Release: Sharing Content Related to the Terrorist Attack) https://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fBas%C4%B1n+B%C3%BClteni%2fBASIN+A%C3%87IKLAMASI+28.06.2016.pdf

[76] CNNTurk (2016, July 19) "15 Temmuz darbe girişiminin bilançosu: 240 şehit, 8 bin 660 gözaltı" (The toll of the 15 July coup attempt: 240 martyrs, 8660 arrests) https://www.cnnturk.com/turkiye/15-temmuz-darbe-girisiminin-bilancosu

[77] Altıok, Z. (2016, July) "OHAL Bilançosu Hak İhalleri Raporu" (Report on the toll of the State of Emergency and Rights Violations) Republican People's Party https://www.chp.org.tr/Public/0/Folder//66594.pdf

[78] Anadolu Agency (2017, March 29) "Darbe girişiminde FETÖ'ye işaret eden deliller" (The evidences that point to FETO in the coup attempt) https://aa.com.tr/tr/info/infografik/5458

with 50.513 arrested.[79] 139.356 government employees were also subject to administrative proceedings, with 111.240 expulsed, many of which were from the Ministry of Education, Turkish National Police, Turkish Armed Forces, Ministry of Health, Ministry of Justice and members of academia.[80] The 3-month state of emergency declared after the coup attempt has been successively extended and continues to this day, and has had significant ramifications for the surveillance and censorship debate.

The first among the impacted was TİB, which was shut down one month after the coup attempt, and its powers and responsibilities, including on the surveillance and website blocking front, transferred to the BTK. The Turkish authorities note that TİB was used as a hub for FETÖ for surveillance and wiretapping purposes, with the President of BTK arguing in 2017 that 85% of TİB personnel and one thirds of BTK personnel had ties to the network.[81] Indeed, the TİB was embroiled in a surveillance controversy exposed in 2014, which discovered that 509.516 people had been surveilled in 2012 and 2013 alone, with surveillance data from previous years wiped from TİB archives.[82] Later that year, it was alleged under another legal investigation over espionage and illegal wiretapping suspicions that a number of high profile officials, including the Undersecretary of the Turkish Intelligence Agency were surveilled under fake code names.[83] Another investigation revealed that encrypted phones of high profile officials, such as President Erdoğan and former Prime Minister Davutoğlu were surveilled, and high ranking TİB officials were arrested as part of the investigation on January 2015.[84] On July 2015, 49 judges and prosecutors were barred from office[85] and the Turkish press reported that over 500 police officers were taken under custody and 63 were arrested as part of ongoing operations.[86] The investigations later revealed that TİB's databases were used to illegally surveil 949 telephones belonging to 48 'VIPs' including journalists, politicians and businesspeople.[87] Turkish authorities suggest that these cases, along with the 17-25 December events and previous high-profile cases going as far as 2008 and targeting members of the armed forces, politicians, journalists, among many others, were orchestrated by FETÖ, and based on illegal surveillance,[88] fraudulent witness statements, and fabricated evidence.[89]

Interception of digital communications played a key role in the case against FETÖ after the coup attempt. Emergency Decree No. 670, the fourth emergency decree to be released after the coup attempt, entailed public and private institutions to provide any files and information pertaining to FETÖ suspects, their spouses and children, including their digital communications, to authorities without delay.[90] The subsequent Emergency Decree No. 671, shut down TİB and transferred its powers and responsibilities to BTK, including the authority to take any measure it deems necessary to uphold "national security and public order; prevent crime; protect public health and public morals; or protect the rights and freedoms"[91] and inform operators,

[79] Altıok, Z. (2016, July) "OHAL Bilançosu Hak İhalleri Raporu" (Report on the toll of the State of Emergency and Rights Violations) Republican People's Party https://www.chp.org.tr/Public/0/Folder//66594.pdf

[80] Ibid.

[81] Güngör, D. (2017, March 20) "Batı'nın çifte standardı internette de var" (The West's double standards exist in the internet as well) Star https://www.sabah.com.tr/yazarlar/dilek-gungor/2017/03/20/batinin-cifte-standard-internette-de-var

[82] Hürriyet (2014, March 7) "TİB: 2012 ve 2013'de 509 bin kişi dinlendi" (TİB: 509 thousand people surveilled in 2012 and 2013) http://www.hurriyet.com.tr/gundem/TİB-2012-ve-2013de-509-bin-kisi-dinlendi-25959220

[83] Anadolu Ajansı (2014, July 23) "MİT Müsteşarı Fidan'ı "Emin" kod adıyla dinlediler" (They surveilled MIT Undersecretary Fidan under the code name of "Emin") https://aa.com.tr/tr/turkiye/mit-mustesari-fidani-emin-kod-adiyla-dinlediler/138606

[84] Sabah (2015, January 22) "Kriptolu ihanette Şen'e tutuklama" (Şen arrested in the encrypted treason) https://www.sabah.com.tr/gundem/2015/01/22/palaz-ve-sen-icin-tutuklama-talebi

[85] Anadolu Ajansı (2017, July 14) "17-25 Aralık'tan 15 Temmuz'a FETÖ" (FETÖ from 17-25 December to 15 July) https://aa.com.tr/tr/15-temmuz-darbe-girisimi/17-25-araliktan-15-temmuza-feto-/861258

[86] Hurriyet (2015, July 12) "Edirne'den Van'a dinleme haritası" (The surveillance map from Edirne to Van) http://www.hurriyet.com.tr/gundem/edirneden-vana-dinleme-haritasi-29527628

[87] Hurriyet (2017, April 22) "Dinleyenler de dinlenmiş" (The surveillers were surveilled too) http://www.hurriyet.com.tr/gundem/dinleyenler-de-dinlenmis-40434559

[88] Hurriyet (2015, December 15) "Telekulağa 2. Tazminat" (The second compensation to wiretapping) http://www.hurriyet.com.tr/gundem/telekulaga-2-tazminat-40027516

[89] Anadolu Ajansı (2017, April 7) "Hakim ve savcılara FETÖ'den ilk iddianamede yeni deliller) "New evidence in the first indictment on FETÖ to judges and prosecutors) https://aa.com.tr/tr/15-temmuz-darbe-girisimi/hakim-ve-savcilara-fetoden-ilk-iddianamede-yeni-deliller/791584

[90] Emergency Decree No: 670 Art.3 Published on Official Gazette No:29804 dated 17 August 2016

[91] Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory p.13

access providers, data centers, hosting providers and content providers of the said measure, who then need to take action within two hours.[92] BTK has to present its case to a peace court for approval within 24 hours, which then has to decide within 48 hours lest the decision is rendered void. Emergency Decree No. 680 further expanded the authority of the Turkish National Police to "detect, surveil, evaluate the signals information, and record data transferred through telecommunications and internet, as well as traffic information between internet sources" without requiring a court approval for 24 hours.[93]

Indeed, telecommunications surveillance played a major part in the case the Turkish authorities have built against alleged FETÖ members. Authorities attribute their swiftness in arresting and expelling FETÖ suspects in the tens of thousands after the coup attempt to the suspicion that an end-to-end encrypted messaging application ByLock was used by members of the organization. The first indictment on ByLock users stated that ByLock had 215.000 users and over 17 million encrypted messages.[94] The indictment concluded that while guised as a global application, ByLock was actually used by FETÖ members for internal communications, with over 60.000 users sending or receiving at least one message and over 46.000 using the application for voice conversations.[95] ByLock communications served as a key reason for arrests over alleged FETÖ membership. By the end of 2017 however, authorities concluded that FETÖ took measures to direct unsuspecting internet users to ByLock IPs to make it seem as though they were ByLock users in an attempt to divert investigations.[96] Up to 11.480 people were believed to be wrongly accused by the diversion, with 1.823 being reinstated to their jobs in January 2018 as a result.[97]

In addition to aforementioned legal and technical developments surrounding content regulation and surveillance online, Turkish authorities also increased efforts to take legal action against internet users for the content they share. In a press release in 24 December 2016, roughly six months after the coup attempt, the Ministry of Interior noted that 1656 individuals were arrested for "inciting the public to hatred and enmity, praising terrorist organizations, making the propaganda of terrorist organizations, openly declaring cohesion with terrorist organizations, insulting state officials, undermining the indivisible unity of the state, and threatening public security".[98] 3710 individuals in total were subject to some sort of legal action (arrest, detaining for questioning, probation etc.), and investigations and legal action of over 10,000 individuals were ongoing at the time of the press release.[99] Authorities also promote citizen reporting of 'activities supporting terrorism' on social media through email tip lines.[100] Individuals can also use the Turkish National Police's tip application – available on Android and iOS – to report activity online, akin to reporting any other criminal activity or suspicious event.[101]

On a more recent security development, Turkey initiated a military operation in Syria against the PKK affiliated Democratic Union Party (PYD) and its armed wing People's Protection Units (YPG) on 20 January 2018. Due to the international – such as the fact that the PYD-YPG has received political and military support from Turkey's NATO allies – and domestic sensitivities (notably with regards to

92 Emergency Decree No: 671 Art.25 Published on Official Gazette No:29804 dated 17 August 2016

93 Emergency Decree No: 680 Art.28 Published on Official Gazette No:29940 dated 6 January 2017

94 Diken (2017, January 21) "'ByLock'la ilgili kapsamlı ilk iddianameden: 215 bin kullanıcı, 15 milyon mesaj var" (In the first comprehensive against ByLock: There are 215 thousand users, 15 million messages) http://www.diken.com.tr/bylockla-ilgili-kapsamli-ilk-iddianameden-215-bin-kullanici-15-milyon-mesaj-var/

95 Ibid.

96 Sözcü (2017, December 27) "Mor Beyin nedir: Binlerce kişi yanlışlıkla indirdi" (What is the Purple Brain: Thousands downloaded it my mistake) https://www.sozcu.com.tr/2017/gundem/mor-beyin-nedir-binlerce-kisi-yanlislikla-indirdi-2149644/

97 Posta (2018, January 13) "'Mor Beyin' nedir? Nasıl Bylock tuzağına düştüler?" (What is the Purple Brain? How did they fall into the Bylock trap?) http://www.posta.com.tr/mor-beyin-nedir-nasil-bylock-tuzagina-dustuler-haberi-1366539

98 Republic of Turkey Ministry of Interior Press Center (2016, December 24) "Basın Açıklaması No: 2016/133" (Press Release No: 2016/133) https://www.icisleri.gov.tr/basin-aciklamasi24122016

99 Ibid.

100 Republic of Turkey Office of the Prime Minister Directorate General of Press and Information official Twitter account, 17 July 2016: https://twitter.com/byegm/status/754682443458895872 ; Yeni Şafak (2016, December 12) "Emniyet Genel Müdürlüğü'nden Önemli Uyarı" (Important Warning by the Turkish National Police) https://www.yenisafak.com/teknoloji/emniyet-genel-mudurlugunden-onemli-uyari-2579166

101 A Haber (2016, December 18) "Teröristi cep telefonundan ihbar et" (Report the terrorist on your phone) https://www.ahaber.com.tr/webtv/teknoloji/teroristi-cep-telefonundan-ihbar-et ; Yeni Şafak (2016, Aralık 23) "Sosyal medyada teröre destek verenler nasıl ihbar edilir?" (How can you report people who support terrorism on social media?) https://www.yenisafak.com/teknoloji/sosyal-medyada-terore-destek-verenler-nasil-ihbar-edilir-2585434 ; Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory

the Kurdish political movement and feelings of solidarity with the PYD among Turkish citizens of Kurdish origin – which have boiled over to violent episodes in the past)[102] involved, managing the information flow has been a priority of the Turkish government during the operations. Some media sources report that Turkish authorities met with press representatives at the outset of the operations to share a list of requests on how to cover the operations to avoid undermining national security.[103] These alleged guidelines include items ranging from refraining to quote foreign news sources verbatim and checking with government officials for correct information, to emphasize the priority that Turkish forces devote to limiting civilian casualties, and to avoid highlighting incidents of public protests and remarks by PKK and affiliated political organizations against the Afrin operation.[104]

Beyond traditional media, Turkish authorities have also shown a willingness to control the flow of information on social media about Operation Olive Branch. In addition to blocking decisions,[105] legal action against content sharers on social media spiked, as displayed in the table below. The Ministry of Interior suggests that these legal actions were taken against profiles and users that "make the propaganda of terrorist organizations, praise these organizations, openly declare their alignment with terrorist organizations, instigate public hatret and enmity, insult state officials, threaten the state's indivisible unity and public security, and contain hate speech".[106]

Date	No. of social media accounts investigated	No. of individuals subject to legal action
15-22 January 2018	1138	364
22-29 January 2018	571	208
29 January – 5 February 2018	934	260
5-12 February 2018	655	243
12-19 February 2018	1296	392
19-26 February 2018	423	251
26 February – 5 March 2018	690	169
5-12 March 2018	635	290
2-Month Total	6342	2177

Table 2: Legal action towards social media users/content providers after Operation Olive Branch[107]

[102] See for example: BBC (2014, October 8) "Turkey Kurds: Kobane protests leave 19 dead" http://www.bbc.com/news/world-middle-east-29530640

[103] Diken (2018, January 21) "Medyaya 15 maddelik 'Zeytin Dalı' listesi: Dış basındaki haberleri aynen taşımayın" (Olive Branch list consisting of 15 items to the media: Do not report foreign news reports verbatim" http://www.diken.com.tr/medyaya-15-maddelik-zeytin-dali-listesi-dis-basindaki-haberleri-aynen-tasimayin/ ; Middle East Eye (2018, January 22) "Turkey imposes restrictive 'guidelines' on reporting Afrin battle" http://www.middleeasteye.net/news/turkey-press-restrictions-afrin-olive-branch-1109543029

[104] Diken (2018, January 21) "Medyaya 15 maddelik 'Zeytin Dalı' listesi: Dış basındaki haberleri aynen taşımayın" (Olive Branch list consisting of 15 items to the media: Do not report foreign news reports verbatim" http://www.diken.com.tr/medyaya-15-maddelik-zeytin-dali-listesi-dis-basindaki-haberleri-aynen-tasimayin/

[105] For example, liveuamap.com a website that gathers updates on conflicts across the world, including in Syria, was reportedly banned shortly after the Turkish operation began, see https://twitter.com/Liveuamap/status/956649270932852736

[106] Republic of Turkey Ministry of Interior (2018) "Basın Açıklamaları ve Tekzipler: Son Bir Hafta İçerisinde 15-22 Ocak 2018" (Press Releases and Corrections: Over the Last Week 15-22 January 2018) https://www.icisleri.gov.tr/15012018-22012018-tarihleri-arasinda-yurutulen-operasyonlar

[107] Republic of Turkey Ministry of Interior (2018) "Basın Açıklamaları ve Tekzipler: Son Bir Hafta İçerisinde …" (Press Releases and Corrections: Over the Last Week…) For 15-22 January: https://www.icisleri.gov.tr/15012018-22012018-tarihleri-arasinda-yurutulen-operasyonlar ; for 22-29 January https://www.icisleri.gov.tr/22012018-2922012018-29012018-tarihleri-arasinda-yurutulen-operasyonlar012018-tarihleri-arasinda-yurutulen-operasyonlar ; for 29 January – 5 February https://www.icisleri.gov.tr/29012018-05022018-tarihleri-arasinda-yurutulen-operasyonlar ; for 5-12 February https://www.icisleri.gov.tr/05022018--12022018-tarihleri-arasinda-yurutulen-operasyonlar ; for 12-19 February https://www.icisleri.gov.tr/12022018-19022018-tarihleri-arasinda-yurutulen-operasyonlar ; for 19-26 February https://www.icisleri.gov.tr/19022018-26022018-tarihleri-arasinda-yurutulen-operasyonlar; for 26 February – 5 March https://www.icisleri.gov.tr/26022018-05032018-tarihleri-arasinda-yurutulen-operasyonlar ; for 5-12 March https://www.icisleri.gov.tr/05032018-12032018-tarihleri-arasinda-yurutulen-operasyonlar

4. Moving Beyond the National Security vs. Liberties Dichotomy in Turkey

4.1. A General Overview: What Do the Numbers Say?

As things stand today, the Turkish case presents a pessimistic scenario from the online rights and freedoms perspective. Turkish authorities have tended to take a security-first approach when it comes to the extension of national security to the internet, which has often come at the expense of online freedoms. An indicator of this has been the Freedom on the Net Index by Freedom House, which assesses 65 countries that represent over 85 percent of the world's internet population under three main criteria: obstacles to access, limits on content, and violations of user rights (including surveillance). Turkey's ranking has gradually worsened since 2011, where its Freedom on the Net score was 45/100 (0 being the best and 100 being the worst possible score). In line with the aforementioned developments, Turkey's score worsened to 49/100 in 2013, 55/100 in 2014, 58/100 in 2015, 61/100 in 2016 where the country's status deteriorated from 'partially free' to 'not free', and finally down to 66/100 in the 2017 Index.[108]

Although incomplete, the number of blocked webpages in Turkey and official requests of content removal from Google, Facebook and Twitter are also frequently quoted data in the debate. According to the now defunct engelliweb.com, Turkish authorities had blocked 114257 websites by October 2016. TİB was behind the blocking decision of 93.2% or 106.833 websites whereas decisions by courts and judges represented 4.6% or 5.204 websites and BTK blocked 0.6% or 655 websites.[109]

Year	Websites blocked annually	Websites blocked in total
2006	4	4
2007	39	43
2008 (Law No.5651 enters into force)	1.014	1.057
2009	5.146	6.203
2010	1.723	7.926
2011	7.488	15.414
2012	8.697	24.111
2013 (Gezi protests)	19.715	43.826
2014 (leaks & legislation change)	36.287	80.113
2015 (terrorist attacks, elections)	27.812	107.925
2016 – until October	5.212	113.137

Table 3: Blocked websites in Turkey (1436 websites the blocking dates of which are unknown are not represented)[110]

[108] Freedom House (2017) "Freedom on the Net 2017: Turkey Country Profile" https://freedomhouse.org/report/freedom-net/2017/turkey

[109] See engelliweb.com capture by WayBack Machine dated 24 October 2016 https://web.archive.org/web/20161013103821/https://engelliweb.com/istatistikler/

[110] See engelliweb.com capture by WayBack Machine dated 24 October 2016 https://web.archive.org/web/20161013103821/https://engelliweb.com/istatistikler/

Similar patterns are observable on social media platforms. Data released by Twitter suggests a gradual increase in Turkish requests for account information and content removal, with a major spike in the latter on the July-December 2015 period and onwards – during the election cycle in Turkey and the rise in terrorist attacks. At that time frame, the rise in Turkish requests along with requests from Russia resulted in a spike in global removal requests from Twitter (from 561 to 4.131, Turkey accounting for 1.761 and Russia accounting for 1.729 of them).[111] Twitter claims that it did not comply with any account information requests by the Turkish government, and its compliance rates with Turkish content removal requests is also falling. Nonetheless, Twitter began using its Country Withheld Content tool[112] in Turkey since March 2014 to block content and users from being seen in Turkey instead of removing them.[113] In the last period reported by Twitter, January-June 2017, Turkish removal requests accounted to 45% of the requests globally, and information requests amounted to 8.5% of the total requests.

Date	Account information requests	Removal requests by courts	Removal requests by gov. agencies, police, etc.	Percentage where some content withheld	Accounts reported
January-June 2013	1	3	4	0%	30
July-December 2013	1	2	0	0%	2
January-June 2014	24	65	121	30%	304
July-December 2014	356	328	149	50%	2.642
January-June 2015	412	408	310	34%	1.978
July-December 2015	403	450	1.761	23%	8.902
January-June 2016	280	712	1.781	23%	14.953
July-December 2016	493	844	2.232	19%	8.417
January-June 2017	554	715	1.995	11%	9.289

Table 4: Twitter Transparency Report[114]

Facebook is similarly criticized for shutting down pages of Kurdish politicians, newspapers, and pro-Kurdish content in general repeatedly based on community complaints.115 According to an internal guideline, allegedly first leaked in 2012, Facebook urges its content editors to block content that allegedly supports the PKK or denigrates Ataturk.116 The increase in the requests of Turkish authorities from Facebook can also be seen in the table below.

111 Twitter Transparency Report "Removal Requests" https://transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2015 accessed on 15 March 2018

112 Twitter Help "About country withheld content" https://help.twitter.com/en/rules-and-policies/tweet-withheld-by-country accessed on 15 March 2018

113 Twitter Blog (2014, March 26) "Challenging the access ban in Turkey" https://blog.twitter.com/official/en_us/a/2014/challenging-the-access-ban-in-turkey.html quoted in Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory

114 Twitter Transparency Report "Turkey" https://transparency.twitter.com/en/countries/tr.html accessed on 15 March 2018

115 Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory; also see Spary, S. (2016, April 8) "Facebook is Embroiled in a Row with Activists over 'Censorship'" Buzzfeed News https://www.buzzfeed.com/saraspary/facebook-in-dispute-with-pro-kurdish-activists-over-deleted?utm_term=.ahK5Z1mP4#.lmD7byEQB

116 Yeşil, B.; Sozeri, E.K.; Khazraee, E. (2017, February) "Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance" Internet Policy Observatory p.9

Date	Total Data Requests	Users / Accounts Requested	Percentage of Requests Where Some Data Produced	Content Restrictions
January-June 2013	96	170	47%	n/a
July-December 2013	129	353	56.59%	2.014
January-June 2014	153	249	60.78%	1.893
July-December 2014	165	278	70.91%	3.624
January-June 2015	368	475	87.50%	4.496
July-December 2015	443	503	84.20%	2.078
January-June 2016	993	1.200	80.67%	861
July-December 2016	459	522	49.46%	1.111
January-June 2017	1.041	1.367	71%	712

Table 5: Facebook Transparency Report[117]

Google's Transparency Reports provide a more detailed breakdown of data. Google notes that it complied with only around 1% of user information requests in 2013, 2014 and 2016 and refrained from doing so at other times. The compliance rate is much higher for removal requests, similar to the case of Twitter. Indeed, it was reported in 2012 that Google's service YouTube reopened in Turkey after a long lull only after acquiescing to the Turkish government's demands and giving more control to authorities over content on the website. User data disclosure requests have increased after 2014, and once again after 2016. When it comes to content removal requests, an interesting trend has been the steady rise of removal requests based on privacy/security and defamation reasons after 2014, perhaps linked to the 'tapes' that Turkish authorities linked to FETÖ. In turn, the rise of national security as a rationale since the second half of 2015 likely points to the increased terrorist attacks in the country. Overall, "national security" represents only 6.2% of total Turkish requests from Google to remove content since 2012.

Date	User data disclosure requests	Users/accounts requested	Total requests to remove content	Total items requested for removal	Overall removal percentage
January-June 2011	73	74	40	269	73%
July-December 2011	88	92	45	174	56%
January-June 2012	112	120	501	2.804	45%
July-December 2012	149	144	157	10.038	55%
January-June 2013	204	163	1673	12.162	17%
July-December 2013	133	182	895	1.803	17%
January-June 2014	224	905	487	2.284	32%
July-December 2014	344	1.498	370	1.249	38%
January-June 2015	425	503	433	1.440	27%
July-December 2015	333	398	745	2.926	32%
January-June 2016	390	595	880	3.611	32%
July-December 2016	431	899	901	4.286	40%
January-June 2017	906	1.117	871	2.896	15%

Table 6: Google Transparency Report[121]

117 Facebook Transparency Report "Turkey" https://transparency.facebook.com/country/Turkey/2017-H1/ accessed on 15 March 2018

118 Google Transparency Report "Requests for user information: Turkey" accessed on 15 March 2018 https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts,compliance;authority:TR&lu=user_data_produced&legal_process_breakdown=expanded:12&user_data_produced=authority:TR;series:compliance

119 Reuters (2012, October 2) "YouTube opens Turkish site, giving government more control" https://www.reuters.com/article/net-us-turkey-youtube/youtube-opens-turkish-site-giving-government-more-control-idUSBRE8910T420121002

120 The Washington Post (2014, March 21) "Why Turkey banned Twitter (and why banning Twitter isn't working)" https://www.washingtonpost.com/news/worldviews/wp/2014/03/21/why-turkey-banned-twitter-and-why-banning-twitter-isnt-working/?utm_term=.f002095690fb

121 Ibid.

Date	Total requests to remove content	Defamation	Privacy / Security	National Security	Government Criticism	Obscenity / Nudity
January-June 2011	40	28% (11)	45% (18)	-	8% (3)	8% (3)
July-December 2011	45	22% (10)	11% (5)	-	11% (5)	16% (7)
January-June 2012	501	18% (88)	5% (24)	6% (32)	29% (144)	13% (67)
July-December 2012	157	42% (66)	5% (5)	5% (4)	11% (17)	8% (13)
January-June 2013	1673	8% (131)	2% (28)	1% (20)	5% (81)	70% (1177)
July-December 2013	895	19% (172)	3% (26)	2% (15)	9% (81)	53% (474)
January-June 2014	487	31% (153)	15% (74)	2% (10)	8% (40)	30% (146)
July-December 2014	370	56% (207)	19% (72)	5% (17)	5% (18)	8% (31)
January-June 2015	433	57% (248)	16% (71)	1% (3)	4% (19)	4% (17)
July-December 2015	745	46% (341)	28% (212)	16% (118)	1% (9)	3% (25)
January-June 2016	880	47% (413)	28% (244)	11% (98)	1% (8)	6% (55)
July-December 2016	901	41% (369)	30% (268)	15% (133)	1% (13)	7% (59)
January-June 2017	871	55% (477)	32% (280)	4% (39)	-	3% (27)

Table 7: Google Transparency Report – Reasons for removal requests[122]

On the other hand, Turkish authorities indeed face numerous challenges to national security and these challenges have extensions online. The conflict with the PKK, once again in full motion after 2015, has entered its fourth decade and now extends to Syria. Beyond the terrorism challenge and the military and security dimension, the conflict has major ramifications for the political, societal, and economic facets of the broader Kurdish issue, making spread of online misinformation and disinformation particularly disruptive. Against the successful operations of Turkish security forces to counter ISIL networks in the country over the last couple of years, ISIL likely maintains an operational presence – as exemplified by the recent foiling of an ISIL plot against the US embassy in Ankara.[123] Online radicalization that may lead to recruitment or inspire lone wolf attacks present a notable challenge given the long history of fundamentalist and extremist terrorist organizations in Turkey. Beyond the two organizations, a large number of terrorist organizations operate in Turkey. The most wanted or 'red list' of the Turkish National Police alone consists of 135 individuals from 11 different terrorist organizations.[124] This includes FETÖ, which Turkish authorities argue is not only behind coup attempt on July 2016, but also a series of disruptive acts over the years through the presence of the network in key public offices – including illegal surveillance.

As a result, the Institute for Economics and Peace's Global Peace Index[125] lists Turkey as the 146th least peaceful country, and the 9th most impacted by terrorism in its Global Terrorism Index[126] out of the 163 countries it assesses. By comparison, France, the United Kingdom and Germany, all of which have witnessed terrorist attacks over the past few years, are ranked 23rd, 35th and 38th most impacted in the Global Terrorism Index but are respectively the 51st, 41st and 16th most peaceful countries according to the Global Peace Index. The chronic manifestation of terrorism and conflict in Turkey and in its near neighborhood unsurprisingly creates a demand for some surveillance and censorship in Turkish authorities.

122 Google Transparency Report "Government requests to remove content: Turkey" https://transparencyreport.google.com/government-removals/by-country/TR accessed on 15 March 2018

123 Hurriyet Daily News (2018, March 5) "Police foil ISIL attack plot on US Embassy in Ankara" http://www.hurriyetdailynews.com/police-foil-isil-attack-plot-on-us-embassy-in-ankara-128237

124 Turkish National Police "Aranan Terörist: Kırmızı tam liste" (Wanted terrorists: Full red list) http://www.terorarananlar.pol.tr/detaylar/Sayfalar/kirmizitamliste.aspx accessed on 16 March 2018

125 Institute for Economics & Peace (2017) (Global Peace Index 2017) http://visionofhumanity.org/indexes/global-peace-index/

126 Institute for Economics & Peace (2017) (Global Terrorism Index 2017) http://visionofhumanity.org/indexes/terrorism-index/

4.2. Bridging the Gap: Recommendations for Policy Makers

Whereas the demand from authorities to increase government presence online, at least on national security grounds, may be justifiable, this does not automatically justify the means of surveillance and censorship that authorities utilize and their severity. Indeed, the numbers provided above suggest that national security is not necessarily the main reason for the Turkish government's activity online. Still, surveillance and blocking decisions, such as the more recent Wikipedia block, do have ramifications beyond human rights and freedoms online, and affect how Turkish citizens benefit economically, socially, politically, and intellectually from the opportunities provided by the global common good that is the internet. Whereas the number of internet subscribers in Turkey increases steadily, as it does globally, surveillance and censorship policies may impact the "quality" of access, digital literacy, and content generation ability of the country's citizens, negatively contributing to the layers of the 'digital divide'[127] that exist both within the country and between Turkish internet users and the rest of the world.

As such, recognizing that neither individual rights and freedoms, nor government priorities that may limit them are absolute, this paper proposes five stepping stones for moving beyond the dichotomies of internet governance vs. non-governance, surveillance vs. privacy, and censorship vs. freedom of expression. These recommendations are by no means silver bullets to solve all issues at hand, and nor is there a perfect formula of online rights and freedoms and government presence that applies to all settings and countries. They are rather mutually reinforcing propositions to better the conditions of the debate and empower its stakeholders in Turkey, so that the country can take stronger steps to reach a healthier and more broadly acceptable balance.

4.2.1. Empowering the Public as a Stakeholder

One of the chronic problems of the debate in Turkey has been the increasing absence of the Turkish public from government decisions that come to affect their lives and online activities. According to Global Survey on Internet Security & Trust by Centre for International Governance Innovation and IPSOS, 54% of Turkish citizens are more concerned about their online privacy compared to a year ago. Whereas this rate was higher, at 63% when the same question was asked in 2014, this nonetheless suggests that concern among citizens are increasing although the pace is slowing down. Furthermore, 74% of Turkish citizens see their own government as a source of concern for their online privacy, with 47% arguing that their government is a major source of concern and 27% arguing that this is somewhat of a concern. In turn, Turkish citizens are less severely worried about foreign governments, with 38% suggesting that foreign governments are a major source of concern for their privacy and 32% seeing this as somewhat of a concern.[128]

As such, regardless of the benevolence or malignance of the intentions of Turkish government, there is a deficit in how the authorities communicate with the public and justify their decisions. Is blocking Wikipedia truly in the interest of the Turkish public? Or is government surveillance – at one point reaching at least half a million citizens – necessarily making them more secure? Regardless, the Turkish government should do more to communicate its decisions to the general public, convince the public on the economics of surveillance and censorship, and formulate the said decisions with input from the public in the first place. On a more practical level, increasing the digital literacy of the public stands as a key ingredient of making this possible. Further action to increase digital literacy and empower the public as a stakeholder in the debate would have positive ramifications for national security as well, such as through increasing awareness about cyber security. Indeed, education and raising awareness on safe practices online and cyber security could actually serve to be a sounder and more effective policy than blocking content.

4.2.2. Recognizing Political, Social and Economic Actors Beyond the Government as Stakeholders

Beyond the general public, the role of the political opposition parties and civil society has also been declining in decision-making surrounding the issue. Whereas Turkish authorities were interested in stakeholder engagement, as exemplified by initiatives in the aftermath of the Internet Law, neither the civil society, nor political opposition parties were taken into consideration when the amendments to the law were drafted and ratified in 2014.[129] In this scenario, the role of the opposition parties is reduced to providing

[127] For more on the digital divide, see IGI Global "What is Digital Divide" https://www.igi-global.com/dictionary/digital-divide/7600 accessed on 17 March 2018

[128] Centre for International Governance Innovation – IPSOS (2017) "CIGI-IPSOS Global Survey on Internet Security & Trust" https://www.cigionline.org/internet-survey

[129] Gürkaynak, G. et al. (2014, November) "New Era for Turkish Internet Law: Will Turkey Become Another China or Iran?" Journal of Business and Economics Volume 5, No. 11, pp. 1976-1982

caveats in legislation and parliamentary inquiries,[130] or pose parliamentary questions with little effect on actual policy making. The reducing transparency of implementers such as BTK further compounds the issue.

The private sector is another part of the equation. Although there are initiatives shaped around service provision, innovation, and cyber security, there is yet to be a sustainable public-private partnership model on internet governance in Turkey. The relationship appears to be a hierarchical one, for example with BTK acting as the decision maker and the private sector that own the internet infrastructure and online platforms merely abiding by BTK's directives. For the internet governance ecosystem, that affects all Turkish citizens, to be better calibrated and sustainable, it should be based on a more pluralistic foundation. The Turkish public should have a say in the process, so that the government can uphold the rights of its citizens vis-à-vis the private sector and balance its own policies, civil society and political opposition should act as counterbalances so that legislative and executive acts better reflect the viewpoints and interests of the society and its various interest groups, whereas the private sector should engage with the public and the civil society to create demand for its services and shield its interests from over-regulation.

4.2.3. Acknowledging Security as One of the Priorities and Not the Ultimate One

When it comes to national security, Turkish authorities are dealing with challenges which may necessitate surveillance and even censorship capabilities. However, the over-prioritization of security, especially in the absence of proper checks and balances, may create further problems than it solves. For one, steps taken to uphold national security can in and of themselves be counterproductive. For example, a critical part of crisis management depends on establishing an official channel of information that would satisfy the concerns and curiosity of the public and media.[131] Blocking social media and imposing broadcast bans with the intention of preventing propaganda, misinformation, and disinformation, especially without a very successful public communication strategy may further heighten public anxiety and fear rather than remedying it.

Yet even more importantly, legislative steps that protect the rights of citizens online have lagged behind those that grant official agencies, as well as the private organizations they entrust implementation with, significant control over the internet. For example, Law No. 6698 on the Protection of Personal Data was ratified on March 2016, even though initial plans suggested that the law would be prepared by the end of 2006, and the first draft of the law was submitted to the Parliament on 2008.[132] Even then, the major impetus towards the ratification of the law was a deal between the European Union and Turkey and the law failed to address some key deficiencies.[133] Similarly, whereas citizens may be exposed to extrajudicial surveillance, recent cases have displayed that it may take years before legal remedies are found.[134] Echoing a recommendation that has been made numerous times over the past decade, this paper recommends a redefinition of official priorities online, with a multi-stakeholder approach, as well as increasing the digital literacy of policy-makers, implementers, and perhaps more importantly, of the judiciary (perhaps even forming specialized courts)[135] to prevent any future victimization.

4.2.4. Improving the Standards of Judicial Practices and Legislation

The European Convention on Human Rights remains

[130] See for example Türkiye Büyük Millet Meclisi (2013, June) "Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması Komisyon Raporu" (The Report of the Parliamentary Research Commission on Determining and Taking Preventative Measures for Violations to the Freedom of Communication and Privacy) available at: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss489.pdf

[131] Ergun, D.; Çelikpala, M.; Kasapoğlu, C. (2016) "Preventing the Worst Case: Accident and Consequence Management for Nuclear Power Plants and the Case of Akkuyu" at "Managing the Risks of Nuclear Energy: The Turkish Case" ed. Ülgen, S. http://edam.org.tr/wp-content/uploads/2016/01/edam_managing_nuclear_risks_report.pdf

[132] Bıçakcı, S.; Ergun, D.; Çelikpala, M. (2015) "The Cyber Security Scene in Turkey" at "A Primer on Cyber Security in Turkey and the Case for Nuclear Power" ed. Ülgen, S. http://edam.org.tr/wp-content/uploads/2016/03/edam_cyber_security_report.pdf

[133] See Ünver, A; Kim, G. (2016, February) "Data Privacy and Surveillance in Turkey: An Assessment of the Draft Law on the Protection of Personal Data" http://edam.org.tr/wp-content/uploads/2016/02/EDAMTurkeyDataPrivacy_format.pdf

[134] See for example Hurriyet (2015, December 15) "Telekulağa 2. Tazminat" (The second compensation to wiretapping) http://www.hurriyet.com.tr/gundem/telekulaga-2-tazminat-40027516

[135] For example the Kartepe Summit discussed above https://web.archive.org/web/20100430151220/http://5651calistay.org/ Türkiye Büyük Millet Meclisi (2013, June) "Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması Komisyon Raporu" (The Report of the Parliamentary Research Commission on Determining and Taking Preventative Measures for Violations to the Freedom of Communication and Privacy) available at: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss489.pdf

the legal compass for Turkey since its ratification of the Convention in 1954. However, as discussed in depth by Deniz,[136] Turkey remains one of the most convicted parties by the European Court of Human Rights since 1959, along with Russia. Roughly 17 percent of Turkish convictions in 2017 emanated from violations of freedom of expression and the right to privacy. With regards to the extension of these rights to the cyber realm, Turkey has been convicted of violating the freedom of expression in the Yıldırım v. Turkey, and Cengiz & others v. Turkey cases over the blocking of Google Sites and YouTube respectively. The ECtHR ruled that the decision of Turkish courts to block entire websites over webpages and content deemed illegal was disproportionate, and that the courts failed to take the principles of the Convention into account before making their decision. The judicial review processes and domestic law were also criticized for failing to take proportionality and necessity principles into account when taking blocking decisions.[137]

On the one hand, as noted by the ECtHR rulings and the Venice Commission,[138] Turkish authorities should improve both the existing legislation and legal procedures so that less intrusive measures are available to balance national security concerns with freedom of expression concerns. In addition to aligning more closely with the Convention standards on legality, legitimacy, and necessity and proportionality, Turkish authorities should also better inform citizens about how the existing legislation applies to the individuals' use of the internet – such as the limitations of their freedom of expression and privacy rights – and redress mechanisms available to them in case of an infraction of their rights. Furthermore, Turkish authorities should improve the mechanisms for informing content providers, users, hosting providers and other affected persons about blocking decisions and allowing affected persons the means to challenge the decisions to avoid any prolonged and undue harm to individual rights and freedoms online.[139] In essence, beyond improving the capacity of the judiciary to take more sound decisions about online activity, the existing legislations, regulations and judicial processes themselves have to be re-examined under a human rights lens to prevent future breaches of individual rights and freedoms online unless absolutely necessary for national security concerns.

4.2.5. Establishment of Effective and Independent Checks and Balances

Beyond improving legislation and judicial standards, empowering the judiciary through increasing the digital literacy of prosecutors and judges, increasing the pool of expert witnesses, and establishing dedicated courts, the legislative branch should also be capacitated to play a role in ensuring the accountability and transparency of surveillance and censorship decisions. The Parliamentary Research Commission Report on Violations to the Freedom of Communication and Privacy dated 2013, notes that "it has been determined that the organizations that are legally entitled to surveil did not conduct surveillance activities according to the law, digital documents have been tempered with from the outside, documents that should have been destroyed were stored and used later or were served to other persons and institutions, and the Ministry Chief Inspectors did not carry out their duties regarding the destruction of documents".[140]

These remarks would be echoed through the illegal surveillance investigation and a series of disruptive activities later tied to FETÖ. Had there been a permanent Parliamentary commission or any other independent legislative mechanism that would oversee the decisions taken by BTK, TİB, and others, perhaps the impact of such extrajudicial surveillance activities could have been minimized. Hence this report recommends the establishment of an independent oversight mechanism to monitor the surveillance and censorship architecture in the country, ideally through the equal representation of all political parties in the parliament, and with the ad hoc participation of external experts, such as academics, practitioners, and civil society. Such a move would serve to boost transparency and accountability, as well as serving as a preventative mechanism for any future wrongdoing. To bolster the latter point, legal, and financial penalties for potential violations should also be strengthened to serve as deterrents.

136 Deniz, Y. (2018) "Online Freedoms and the European Court of Human Rights: A Path Forward for Turkey?" Centre for Economics and Foreign Policy Studies

137 European Commission for Democracy Through Law (2016, June 15) "Turkey: Opinion on Law No. 5651" Opinion No. 805 / 2015 Adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)

138 Ibid.

139 See Deniz, Y. (2018) "Online Freedoms and the European Court of Human Rights: A Path Forward for Turkey" Centre for Economics and Foreign Policy Studies

140 Türkiye Büyük Millet Meclisi (2013, June) "Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması Komisyon Raporu" (The Report of the Parliamentary Research Commission on Determining and Taking Preventative Measures for Violations to the Freedom of Communication and Privacy) pp.277-278 available at: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss489.pdf

5. In Conclusion

Finding the right mixture of judicial and legislative action to ensure national security while upholding individual rights and freedoms online remains a challenging task for democracies. Whereas the maximum amount of security is of course needed for a peaceful society, this should come at the expense of the minimum infringement of human rights.

In this regard, the cyber scene in Turkey has been problematic for both the Turkish government and institutions aiming to maximize national security and for the Turkish citizens, academia, NGOs and political opposition concerned about human rights online. This paper observes that whereas the Turkish government was mainly concerned about the 'safety' aspect in regulating the internet initially, from grave concerns surrounding child abuse, to more broader issues such as obscenity, national security increased as a priority parallel to political and security related developments after 2013. In time, Turkish authorities accumulated significant means of blocking content and surveilling user activity online, from a variety of blocking techniques and tools, to preventing circumvention by VPN banning, from limiting access without a legal blocking decision such as broadband throttling and DNS poisoning, to compelling social media networks, access, hosting and service providers to collaborate closely with the government, and to obtaining tools and developing an institutional capacity to surveil user activity. Financial and legal deterrents have been expanded to ensure compliance and penalize user behavior.

However, these have not been complemented with policies and legislative action to prevent any wrongdoing by authorities or allow individuals to easily challenge official decisions and seek remedies. In fact, the transparency and accountability of decision-making has declined in time, with more legal power resting in an administrative body, BTK (and TIB before that), with authorities failing to disclose sufficient data even to the Venice Commission[141] and to the Turkish Parliamentary Research Commission[142] and with the judiciary criticized by the European Parliament for not deliberating enough on human rights dimensions of their decisions and not taking into account the principles of the European Convention on Human Rights. As a result, Turkey's ranking in international internet freedom indexes have declined sharply, and more Turkish citizens are concerned about their privacy and the role of their government in violating their privacy online.

Regardless of the benevolence or malignance of the intentions of the Turkish government and Turkish officials, there is significant room and need for improving the unbalanced rights/security axis in the country. As FETÖ's disruptive activities have highlighted, in the absence of transparency, accountability, independent oversight capacity, and appropriate checks and balances, the existing system is vulnerable to abuse or misuse. This paper thus recommends an all-stakeholder approach to policy and legislation formulation in this critical issue that concerns all Turkish citizens, more pluralistic and independent oversight mechanisms for surveillance and blocking decisions, the empowerment of the public to become a stakeholder in the debate, the empowerment of decision-makers and judiciary to make more informed decisions through a more holistic understanding of the security and rights nexus, and developing non-securitized and less intrusive measures to deal with national security challenges online where possible, such as educating citizens on safe behavior online, and allowing room for notice and takedown, self-regulation, and content specific blocking decisions to work before taking down entire websites. In essence, Turkish authorities should shift their focus from a security-first stance into a position that balances human rights and national security priorities online - which may restore the trust of the Turkish public and may actually provide more security than the current scenario. The European Convention on Human Rights standards and the European Court of Human Rights decisions present valuable compasses to move in this direction.

141 European Commission for Democracy Through Law (2016, June 15) "Turkey: Opinion on Law No. 5651" Opinion No. 805 / 2015 Adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)

142 Türkiye Büyük Millet Meclisi (2013, June) "Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması Komisyon Raporu" (The Report of the Parliamentary Research Commission on Determining and Taking Preventative Measures for Violations to the Freedom of Communication and Privacy) pp.277-278 available at: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss489.pdf

Centre for Economics and Foreign Policy Studies

Cyber Governance and Digital Democracy 2018/1

April 2018

National Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy

Doruk Ergun | Research Fellow, EDAM