Turkey

Not Free
37
100

A Obstacles to Access  15 25
B Limits on Content  11 35
C Violations of User Rights  11 40

Last Year's Score & Status
34 100 Not Free

Overview
While disruptions to connectivity and convictions for online activities were not observed during the coverage period, internet freedom in Turkey remained highly restricted. Online content was frequently blocked, including news articles, and authorities continued to investigate or arrest users. Worryingly, regulations requiring online content providers to secure broadcasting licenses came into force after the coverage period, possibly leading to increased censorship and content regulation of local streaming and news websites.

President Recep Tayyip Erdoğan’s Justice and Development Party (AKP) has shown growing contempt for political rights and civil liberties, and its authoritarian nature has been fully consolidated since a 2016 coup attempt triggered a more dramatic crackdown on perceived opponents of the leadership. Constitutional changes adopted in 2017 concentrated power in the hands of the president, and worsening electoral conditions have made it increasingly difficult for opposition parties to challenge Erdoğan’s control.

Key Developments

June 1, 2018 – May 31, 2019

- While no disruptions to the internet were reported during the coverage period, Turkey’s internet backbone remains highly centralized (see A3).
- Over 3,000 URLs featuring news items were blocked in 2018. Widespread censorship has led users to obtain news and information via social media, particularly YouTube, in recent years (see B1 and B7).
- Numerous people were investigated or detained for their online activities, including for criticizing Erdoğan and commenting on the depreciation of the Turkish lira. However, no prison sentences for online expression were handed down during the coverage period (see C3).

A Obstacles to Access
There were no reported disruptions to network connectivity during the coverage period, and internet penetration rates continued to grow. However, the country’s internet backbone remained highly centralized and the cost of internet access continued to be relatively high.

A1 0-6 pts
Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

Infrastructural limitations do not directly restrict access to the internet or the speed and quality of internet connections. According to the International Telecommunication Union (ITU), the percentage of individuals using the internet stood at 71 percent in 2018, compared to 65 percent in 2017. According to the results of the Turkish Statistical Institute’s Household Usage of Information Technologies Survey, the share of households with internet access had risen to 83.8 percent in 2018. Turkey has one of the most concentrated mobile markets in Europe. There were 74.5 million broadband subscribers as of the last quarter of 2018. Regular mobile penetration reached 99 percent of the population, including machine to machine (M2M) communication.


A2 0-3 pts
Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?

Prices for internet access remain high in comparison with the minimum wage. In past years, connectivity in the southeastern region was negatively affected by poor telecommunications infrastructure and electricity blackouts. According to the 2019 Inclusive Internet Index report, 15 percent more men than women access the internet, though there is no apparent gender gap in mobile phone access.1


A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?

Restrictions on connectivity were less frequent during the coverage period than in previous years.

Past disruptions targeted the restive southeastern region, where ethnic Kurds comprise a majority of the population, and which has seen the implementation of a state of emergency and frequent security operations as part of a crackdown by Turkish security forces on the militant Kurdistan Workers' Party (PKK).1 In September 2016, landline, mobile phone, and internet services were shut down in 10 cities for six hours, affecting some 12 million residents; the shutdown came as 28 Kurdish mayors were being removed from their posts.2 A month later, the government suspended mobile and fixed-line internet service in 11 cities for several days, leaving six million citizens offline. Key public services, such as banks and payment mechanisms, were reportedly unavailable. That shutdown coincided with mass protests prompted by the detention of local Kurdish politicians, including the two comayors of Diyarbakır, and was apparently intended to delay or inhibit coverage of the police response. Reporters were forced to travel to nearby cities in order to upload and share footage of police beating protesters.3 Shutdowns have also been frequently imposed during military operations in the region.

There are at least four internet exchange points (IXPs) owned by private companies. Turkey's internet backbone is run by TTNET, a subsidiary of Türk Telekom that is
also the largest internet service provider (ISP) in the country. Türk Telekom, which is partly state owned, owns 282,000 kilometers out of 355,000 kilometers of Turkey’s total fiber-optic infrastructure. Other operators have a combined total of 73,000 kilometers of fiber.  


A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?

A number of regulatory and economic obstacles limit the diversity of service providers. Though all legal entities are allowed to operate an ISP, there are some requirements to apply for authorization, pertaining to issues such as the company’s legal status, scope of activity, and shareholders’ qualifications. Informal obstacles may also prevent newly founded companies without political ties or economic clout from entering the market. ISPs are required by law to submit an application for an activity certificate to the Information and Communication Technologies Authority (BTK) before they can offer services. Internet cafés are subject to regulation as well.
Those operating without an activity certificate from a local municipality may face fines of 3,000 to 15,000 Turkish lira ($500 to $2,500). Mobile service providers are subject to licensing through the BTK. Moreover, the BTK has the authority to request written notifications from ISPs. In 2016, for instance, the BTK asked all ISPs to submit weekly progress reports on the status of new restrictions on virtual private networks (VPNs).1

There were 448 operators providing information and communications technology (ICT) services in the Turkish market in the last quarter of 2018.2 TTNET, founded in 2006 by Türk Telekom, is the dominant player, with a market share of 52.6 percent of DSL (digital subscriber line) subscriptions at the end of 2018, a slight decline from the previous year.3 In recent years, regulators have sought to shut down inactive ISPs existing in name only.

Turkcell is the leading mobile service provider, with 42.1 percent of the market, followed by the British multinational company Vodafone and TT Mobil.4 An auction of 4G frequency bands was held in 2015, and by 2016, Turkcell and Vodafone, along with Avea, which is now known as TT Mobil, had started offering “4.5G” technology to mobile subscribers.5

Türk Telekom was created as a state-owned landline company in 1994 and launched broadband services in the early 2000s through its subsidiary, TTNNet. After its privatization in 2005, the company remained close to the government. Although the liberalization of the market is regulated, the implementation and enforcement of these regulations is weak, reducing the competitiveness of the market. As of May 2019, the former president of the BTK and current deputy transportation and infrastructure minister, Ömer Fatih Sayan, was the chairman of Türk Telekom.6

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?

The independence of the regulatory bodies that oversee service providers is sometimes compromised. Policymaking, regulation, and operations are separated under the basic laws of the telecommunications sector. The Ministry of Transportation, Maritime Affairs, and Communications is responsible for policymaking, while the BTK oversees regulation.1

However, though the BTK has its own dedicated budget, its board members are government appointees and its decision-making process is not transparent. Nonetheless, there have been no reported instances of certificates or licenses being improperly denied. After the 2016 coup attempt, the Telecommunication and Communication Presidency (TİB), which implemented the country’s website blocking law, was shut down under an emergency decree, and all of its responsibilities were transferred to the BTK.2 The TİB—described by President Erdoğan as “among the places that has all the dirt”—was closed due to suspicions that it was used by Gülenists as a “headquarters for illegal wiretapping.” (Authorities have declared the movement of exiled Islamic preacher Fethullah Gülen a terrorist organization, and have blamed it for the 2016 coup attempt.) 3

The Computer Center of Middle East Technical University has been responsible for managing domain names since 1991. The BTK oversees and establishes the domain-name operation policy and its bylaws. The BTK and the university signed a protocol, which was approved by the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA) in May 2019, to
transfer the management of domain names to the BTK within two years. Unlike in many other countries, individuals in Turkey are not permitted to register and own domain names ending with the country extension .tr, such as .com.tr and .org.tr, unless they own a trademark, company, or civil society organization with the same name as the requested domain.


**B Limits on Content**

*Self-censorship has persisted. While users have turned to social media, particularly YouTube, for news and information in recent years, websites continued to be blocked, including news articles. Journalists, scholars, and public figures who are critical of the government have faced coordinated harassment by progovernment trolls on Twitter. Regulations that came into force after the coverage period will require certain online content providers to obtain licenses.*

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?

Blocking of online content, particularly news and citizen journalism websites, has increased in recent years.

Engelli Web, a civil society initiative that lists blocked websites in Turkey, found that more than 240,000 websites were inaccessible as of December 2018, up from about 40,000 in 2013. The BTK was responsible for over 95 percent of the websites
Websites can be blocked for “obscenity,” which in the past has included any site with certain keywords relating to sex or sexuality in the domain name. Sites can also be blocked if they are deemed defamatory to Islam, including content that promotes atheism. However, the uptick in censored content in recent years is largely due to the blocking of news sites and articles that are critical of the government. According to Engelli Web, 3,306 URLs containing news items were blocked in 2018.

In October 2018, authorities blocked 10 articles at the request of the construction company Limak. The articles alleged the company’s involvement in embezzlement during the construction of an Istanbul airport. A number of other government-linked companies successfully appealed to authorities to block dozens of articles during the reporting period. Other news sites blocked are Ahval News (blocked in early 2018) and Haberdar (blocked in 2016), which remained inaccessible during the coverage period. A news site operated by prominent journalist Can Dündar, Özgürüz, was blocked in 2017, before it published its first article.

In 2017, Wikipedia was blocked in Turkey in order to prevent access to two articles that mentioned the Turkish government’s involvement in Syria. The ban remained in place throughout the reporting period. Additionally, the image-sharing site Imgur has been blocked since 2015. In 2016, the BTK ordered ISPs to ban more than 10 VPN services, as well as the circumvention tool Tor.

ISPs offer “child” and “family” filtering options under rules established by the BTK in 2011, though the filtering criteria have been criticized as arbitrary and discriminatory. The child filter obstructs access to Facebook, YouTube, Yasam Radyo (Life Radio), the Armenian minority newspaper Agos, and several websites advocating the theory of evolution. Internet access is filtered at primary education institutions and public bodies, resulting in the blocking of a number of news sites.

• 4. “New Internet Filtering System Condemned as Backdoor Censorship,”
Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?

In addition to widespread filtering, state authorities are proactive in requesting the deletion or removal of content. Social media platforms comply with administrative decisions and court orders promptly in order to avoid blocking and, more recently, throttling. Like international social media platforms, popular Turkish websites are subject to content removal orders. Online news outlets have also removed content that was blocked. The Gülen-linked newspapers Zaman and Today’s Zaman, as well as the Cihan News Agency, were seized by the government in 2017. The online archives of each paper were deleted, as was Zaman’s previous Twitter activity. Zaman was one of approximately 130 news outlets that were shut down in July 2016, after the government arrested 89 media workers for alleged ties to the Gülen movement.

Several well-known Twitter accounts have been removed at the request of the authorities. Turkey has consistently ranked among the countries with the highest number of removal requests sent to Twitter. According to Twitter’s latest transparency report, between July and December 2018, the Turkish government made over 5,000 removal requests, and Twitter complied with 4 percent of them. In the first half of 2018, the government made nearly 9,000 removal requests, and Twitter complied with 18 percent of them. Most of the accounts that Twitter has withheld at the request of the government are connected to pro-Kurdish movements or the Gülen movement, and have been shut down on antiterrorism grounds.

Facebook and Instagram also received a large number of content restriction requests from Turkey. According to Facebook’s transparency report covering July to...
December 2018, 747 pieces of content were restricted by Facebook, 400 at the request of the government, and 347 in response to privately lodged accusations of defamation. Between January and June 2018, 1,634 pieces of content were restricted, 1,106 at the request of the government, and 528 in response to private reports of defamation. Some analysts believe the declining number of requests can be attributed to the government’s shift to blocking content through technical means.

2. Zaman’s Twitter account has been renamed “@AnalizMerkez.” See Efe Kerem Sozeri’s statement: https://twitter.com/efekerem/status/706282702861942784?lang=en, March 5, 2016, and https://web.archive.org/web/20160306005700/https:/twitter.com/analizmer...

B3 0-4 pts
Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?

Many of the restrictions on the internet and digital content lack proportionality and transparency. The blocking and removal of online content (see B1 and B2) is regulated under Law No. 5651. The law was initially enacted in 2007 to protect children and prevent access to illegal and harmful content, including child sexual abuse, drug use, the provision of dangerous substances, prostitution, obscenity, gambling, suicide promotion, and crimes against Mustafa Kemal Atatürk. The responsibilities of content providers, hosting companies, public access providers, and ISPs are delineated in this law. Domestically hosted websites with proscribed content can be taken down, while websites based abroad can be blocked and filtered through ISPs. The law has been amended in recent years to broaden the
circumstances in which censorship is legally permissible.

ISPs must join an association for access providers in order to obtain an “activity certificate” to legally operate in the country. ISPs must also comply with blocking orders from the BTK within four hours or face a fine of up to 300,000 Turkish lira ($50,000). Failure to take measures to block all alternative means of accessing the targeted site, such as proxy sites, may result in a fine of up to 50,000 Turkish lira ($8,400).

The vast majority of blocking orders are issued by the BTK, rather than by the courts. The procedures surrounding blocking decisions are opaque, creating significant challenges for those seeking to appeal. Judges can issue blocking orders during preliminary investigations as well as during trials. The reasoning behind court decisions is not provided in blocking notices, and the relevant rulings are not easily accessible. As a result, it is often difficult for site owners to determine why their site has been blocked and which court has issued the order. The BTK’s mandate includes executing judicial blocking orders, but it can also issue administrative orders for foreign websites, content involving sexual abuse of children, and obscenity. Moreover, in some cases it successfully asks content and hosting providers to remove offending items from their servers, in order to avoid issuing a blocking order that would affect an entire website. This occurs despite the fact that intermediaries are not responsible for third-party content on their sites.

A bylaw approved after the coverage period allowing the Radio and Television Supreme Council (RTÜK) to regulate content, including streaming services, may lead to the council demanding the removal of content or the restriction of access to the platforms under its purview (see B6).

Regarding appeals to content restriction decisions, in May 2019 the Wikimedia Foundation petitioned the European Court of Human Rights against the blocking of Wikipedia in Turkey. In 2017, Twitter noted that, “Whenever possible under Turkish law, Twitter filed legal objections in response to all court orders involving journalists and news outlets...disappointingly, none of our objections prevailed” (see B2).

- Law No. 5651 was published in the Official Gazette on May 23, 2007, in issue No. 26030. A copy of the law can be found (in Turkish) at World Intellectual Property Organization, “Law No. 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet


6. According to TİB statistics from May 2009, the last date these were available, the courts are responsible for 21 percent of blocked websites, while 79 percent are blocked administratively by the TİB. “Telecom Authority Accused of Concealing Blocked Website Figures,” Reporters Without Borders, May 19, 2010,[http://en.rsf.org/turkey-telecom-authority-accused-of-19-05-2010.37511...](http://en.rsf.org/turkey-telecom-authority-accused-of-19-05-2010.37511...).


Do online journalists, commentators, and ordinary users practice self-censorship?

Digital media outlets are inhibited by heightened self-censorship. A steep rise in prosecutions for defaming the president has also had a chilling effect on social media users in recent years (see C3). Self-censorship online has been exacerbated by decrees passed under the state of emergency that have expanded surveillance.

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?

Government manipulation on social media has adversely impacted the online information landscape.

Numerous reports have revealed that an “army of trolls” numbering around 6,000 individuals has been enlisted by the ruling AKP to manipulate online discussions, drive particular agendas, and combat government critics on social media. Emails leaked in 2016 provided insight into a coordinated campaign by President Erdoğan’s inner circle to counter critical narratives and weaken protest movements on social media. Messages sent to then minister of energy and natural resources Berat Albayrak, who is also the son-in-law of the president, discussed the establishment of “a team of professional graphic designers, coders, and former army officials who received training in psychological warfare,” according to a report by the Daily Dot. One email proposed exposing the drug habits of celebrities who had supported the 2013 Occupy Gezi movement, which resulted in police raids on the homes of 55 actors, directors, and other celebrities two months later. The images of the celebrities during the raids were widely shared by progovernment outlets on social media.

According to a study published in December 2018 by the Heinrich Böll Stiftung Foundation and the Turkish Social Economic Political Research Foundation (TÜSES), “The use of social media by young people shows supporters of the AKP are more effective than those of other parties in disseminating political messaging. AKP activists worked in a more extensive and systematic way, coordinating with the party’s media wing on social media strategy. They also had financial support and
access to expert advice during election periods.”

Journalists, scholars, and civil society leaders who are critical of the government have faced orchestrated harassment on Twitter, often by dozens or even hundreds of users working to discredit them (see C7). For example, in May 2019, ahead of Istanbul’s second mayoral election, which was held after the first results were annulled, numerous progovernment social media accounts spread a misleading video of the opposition candidate Ekrem İmamoğlu. The video was altered to show İmamoğlu saying he would have terrorist groups run the country. Shortly before the November 2015 elections, progovernment trolls circulated allegations that Oy ve Ötesi (Vote and Beyond), the first civic election-monitoring initiative in Turkey, was committing fraud and aiding terrorist organizations.

Fake news is a problem in Turkey, as well. According to the Reuters Institute for the Study of Journalism’s Digital News Report 2018, 49 percent of Turks were “exposed to completely made-up news in the last week,” making it the country most saturated with fake news in the report.

Media coverage regarding the Kurdish-populated southeastern region is heavily influenced by the government. In 2016, for example, new progovernment editorial administrative boards for Gülen-affiliated news outlets were established by court order (see B2).

- 7. Efe Kerem Sozeri, “How pro-government trolls are using a sexy Twitter bot
Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?

Some economic constraints can negatively affect users’ ability to publish content online.

Advertising is frequently used as a tool to control the media. The government financially supports AKP-friendly media outlets, including online outlets, through advertising, and withholds such support from critical publications, leaving independent online media at a disadvantage. Net neutrality is not explicitly protected by Turkish laws.

In March 2018, the parliament approved a bill granting the Radio and Television Supreme Council (RTÜK) authority to regulate online content, including but not limited to commercial streaming services such as Netflix, as well as foreign-based online media platforms such as Arti TV and Deutsche Welle (DW), both of which are based in Germany. The RTÜK prepared draft bylaws in September 2018, which came into force after the coverage period, in August 2019. Under the new rules, online content providers must secure a license from the RTÜK, which will also be able to issue fines or revoke licenses. Analysts fear that this new regulatory framework will further threaten the ability to publish online.

4. Arzu Geybullayeva, “How Turkey's broadcast regulator is taking over the supervision of online content,” Global Voices Advox, September 6, 2019, https://advox.globalvoices.org/2019/09/06/how-turkeys-broadcast-regulat...
Shutdowns of independent outlets, the preponderance of progovernment media, and self-censorship have negatively affected the diversity of online content.

Turkish users rely on online publications for news, despite the country’s restrictive legal environment and self-censorship. There are a wide range of blogs and websites through which citizens question and criticize Turkish politics and leaders, though many such platforms have been blocked since the attempted coup and the flare-up in hostilities between government forces and Kurdish separatists. The 2016 blocking of Tor and popular VPN services made it more difficult for users to reach blocked websites (see B1).

As of mid-2019, the progovernment En Son Haber was the most visited news site in the country, followed by the websites of the newspapers Hurriyet and Aksam, also progovernment outlets, and the website of the opposition newspaper Sozcu. Platforms for citizen journalism and volunteer reporting have gained traction in recent years, including 140journos, dokuz8Haber, and Ötekilerin Postası. Fact-checking initiatives (see B8) also act as information sources. Censorship of prominent local news sites, as well as government influence in coverage, make information-gathering even more difficult in the Kurdish-majority southeastern region.
Social media platforms also provide an important source of independent news. The Reuters Institute for the Study of Journalism’s *Digital News Report 2019* found that slightly fewer people are getting their news through Facebook and Twitter. However, people are increasingly consuming news via YouTube, WhatsApp, Instagram, and Facebook Messenger. According to the report, “Social and digital media are an important outlet for alternative and critical perspectives.” With most Turkish media outlets controlled by the government, the opposition has been forced to find new ways to inform the public via social media. YouTube has increasingly become popular for news, including through the channels of journalists Emin Çapa and DW Türkçe. Along with DW, the BBC, France 24, and Voice of America (VoA) have launched YouTube channels in Turkish, expanding access to independent sources of information.

Retaliation against journalists who give a platform to opposition voices also limits the diversity of online content. In July 2019, after the coverage period, former prime minister and AKP leader Ahmet Davutoğlu, who has since criticized Erdoğan, was interviewed by radio host Yavuz Oğhan and two other journalists. After the interview was posted on YouTube, Radyo Sputnik canceled Oğhan’s program.

- **4.** “Sputnik cancels Turkish radio program after host interviews former PM Davutoğlu,” Turkish Minute, July 19, 2019, [https://www.turkishminute.com/2019/07/19/sputnik-cancels-turkish-radio-....](https://www.turkishminute.com/2019/07/19/sputnik-cancels-turkish-radio-....)

B8 0-6 pts

Do conditions impede users’ ability to mobilize, form communities, and campaign, particularly on political and social issues?

Digital activism has played a significant role in the country since the 2013 Occupy Gezi protests, although it has waned somewhat in recent years as a result of the
repressive climate after the 2016 coup attempt and growing self-censorship.

A number of websites and apps are used to organize both online and offline. Turkey Blocks, an organization that tracks censorship in real time, was granted the Index on Censorship’s 2017 award for digital activism.1 The organization Vote and Beyond monitored the June 2018 elections through a mobile app that enables volunteers to report voting data, which is then compared with preliminary results announced by the Supreme Electoral Council.2 Share of Truth is a political fact-checking website, and a popular source for information.3 Teyit is another fact-checking initiative that focuses on verifying news reports and debunking disinformation and urban legends.

Social media is seen as a platform to advocate for justice, and has been utilized to bring attention to criminal cases that may be ignored in the mainstream media. The death of an 11-year-old girl, Rabia Naz Vatan, in 2018 in Giresun, which authorities initially ruled a suicide but her family claimed was a hit-and-run accident perpetrated by an individual with connections to the local government, led to a campaign on Twitter that brought renewed attention to the case and ultimately led to the investigation being reopened.4


C Violations of User Rights

*Turkish citizens faced investigations and arrests for their online activities, though no prison sentences were handed down during the coverage period. Social media users were targeted for criticizing the president and commenting on the Turkish lira’s depreciation. Surveillance remained a concern.*
Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?

The constitution and laws of Turkey fail to protect freedom of expression and press freedom online. The constitution includes broad protections for freedom of expression. Article 26 states that “everyone has the right to express and disseminate his thought and opinion by speech, in writing, or in pictures, or through other media, individually or collectively.” Turkish legislation and court judgments are subject to the European Convention on Human Rights and bound by the decisions of the European Court of Human Rights. Despite these guarantees, online journalists and ordinary users frequently face civil and criminal penalties for legitimate expression. The constitution also guarantees the right to privacy, though there are legal limitations on the use of encryption devices (see C4), and surveillance of online activity by security agencies is believed to be widespread (see C5).

The state of emergency enacted in the wake of the 2016 coup attempt and in effect until July 2018 allowed President Erdoğan to issue decrees without judicial oversight, including decrees that threatened freedom of expression online, which were used to block websites, shut down communication networks, and close civil society organizations and news outlets. Decree No. 671, published in 2016, amended the Law on Digital Communications to authorize the government to take “any necessary measure” on the grounds of “national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms” guaranteed under Article 22 of the constitution. The decree also obliges telecommunications providers to enforce government orders within two hours of receiving them. Despite the fact that the state of the emergency is no longer in effect, the decree remains on the books.
Turkish laws are enforced by a judiciary whose independence has been compromised, particularly since the coup attempt. Judges still occasionally rule against the government, but the appointment of thousands of new, loyalist judges in recent years, the potential professional costs of ruling against the executive in a major case, and the effects of an ongoing purge of judges suspected of supporting the coup attempt have all severely weakened judicial independence in Turkey.


C2 0-4 pts
Are there laws that assign criminal penalties or civil liability for online activities?

There are no laws that specifically criminalize online activities like posting one’s opinions, downloading information, sending emails, or transmitting text messages. Instead, many provisions of the Criminal Code and other laws, such as the Anti-Terrorism Law, are applied to both online and offline activity.

According to Article 7 of the Anti-Terrorism Law, “Those who make propaganda of a terrorist organization by legitimizing, glorifying, or inciting violent methods or
threats” can face prison terms of one to five years. The law has been widely criticized for its broad definition of terrorism, which has been exploited by courts to prosecute journalists and academics who criticize the government, with no link to terrorism.  

Defamation is a criminal offense punishable by a fine and up to two years in prison. Defamation charges have frequently been used to prosecute government critics. Defaming a public official carries a minimum sentence of one year in prison, while insulting the president is punishable by between one and four years in prison, according to Article 299 of the Criminal Code. Several courts deemed Article 299 unconstitutional in the first half of 2016, but the Constitutional Court upheld the provision in December 2016.


C3 0-6 pts
Are individuals penalized for online activities? 26

Prosecutions and detentions of Turkish citizens for their online activities continued during the coverage period. Many journalists, activists, and ordinary citizens faced arrest in retaliation for criticism of the war in Syria and other government policies, as well as expressions of Kurdish identity. According to the Committee to Protect Journalists (CPJ), a total of 68 journalists were imprisoned in Turkey as of 2018.

The Turkish government has also sought the extradition of online critics living abroad. In May 2019, the Turkish government attempted to secure the extradition of Özcan Keleş, a critic of Erdoğan of Turkish descent who lives in the United Kingdom, on the grounds that he allegedly spread terrorist propaganda via Twitter and had an association with a group that Turkey claims is associated with Gülen.
In August 2018, during Turkey’s currency crisis, the Ministry of the Interior announced that an investigation had been launched into 346 social media accounts posting provocative content on the Turkish lira. While the results of this investigation are unclear, in June 2019, after the coverage period, two Bloomberg journalists who had written about the depreciation of the lira in August 2018 were indicted, as were 36 people who had commented on the article or criticized the economy on social media.

Prosecutions for insulting the president online have increased in recent years, although they have rarely resulted in convictions. However, some defendants have been jailed while awaiting trial. Insulting the president online is an offense punishable by up to four years in prison. After the failed military coup in 2016, Erdoğan dropped around 2,000 of the cases (some had been filed against teenagers) as a good faith gesture and to promote national solidarity. However, arrests and detentions have continued for insulting Erdoğan on social media. The government frequently claims such arrests are meant to root out people with links to the PKK or the Islamic State. In May 2019, opposition Republican People’s Party (CHP) Istanbul official Canan Kaftancıoğlu was indicted for tweets posted between 2012 and 2017 that allegedly insulted the Turkish government, President Erdoğan and public servants; incited “hatred and enmity;” and spread “propaganda for a terrorist organization.” If convicted, Kaftancıoğlu faces up to 17 years in prison.

Social media influencer Pınar Karagöz, who is known as “Pucca,” was detained in October 2018 for social media posts that referenced drug trafficking while discussing the popular television show Narcos, which prosecutors claimed encouraged drug use. In July 2019, after the coverage period, Pucca was sentenced to five years and ten months in prison for the posts. The conviction was subsequently appealed.

In January 2018, a number of journalists were arrested for online critiques of Operation Olive Branch, a Turkish military operation in Afrin, Syria. The Turkish police force has associated criticism of the operation with terrorism, linking it with the militant PKK. Furthermore, Turkey has asked social media sites including Facebook and Twitter to take down posts that criticize Operation Olive Branch (see B2). As part of the crackdown, journalists Hayri Demir and Sibel Hürtaş were detained for comments on social media that critiqued Turkey’s military role in Afrin and contradicted the Turkish government’s assertions about the conflict. They
were detained for “inciting the people to violence” and convicted of “terrorist propaganda via media.”

Although they were released on bail after four days, Demir, Hürtaş and 10 other defendants faced up to 10 years and 6 months in prison for their criticism of the operation on social media.

Following a number of delays, the next trial date has been set for December 2019. In May 2018, Demir was handed a separate suspended sentence of one year, six months, and 22 days for spreading terrorist propaganda online.

According to the Ministry of the Interior’s yearly report for 2018, over 42,000 social media accounts were investigated for propaganda for terrorist organizations, praising these organizations, publicly declaring that they are involved in terrorist organizations, encouraging hatred and enmity, and insulting government officials, among other offenses. More than 18,000 people faced legal action as a result of these investigations.

However, it is unclear how many of these cases were legitimate.

These arrests and others have led to increasing self-censorship online by many users, who fear that if they speak out against the government they too may face prosecution (see B4).


17. “Journalists Sibel Hürtaş and Hayri Demir’s trial dragged by the Ministry,”
Does the government place restrictions on anonymous communication or encryption?

Limitations on encryption and anonymity are concerns in Turkey. The anonymous purchase of mobile phones is not allowed; buyers must provide official identification. According to a presidential decree issued in May 2019, Turkish citizens may only import one mobile phone every three years. Import devices can be registered at mobile service providers’ subscription centers and an e-government website for a fee of 1,500 Turkish lira ($250). Devices that are not registered within 120 days are blocked from telecommunications networks, excluding emergency services.

In 2011, the BTK imposed regulations on the use of encryption hardware and software. Suppliers are required to provide encryption keys to state authorities before they can offer their products or services to individuals or companies within Turkey. Failure to comply can result in administrative fines and, in cases related to national security, prison sentences.

- **1.** Citizens could previously import up to two mobile devices. “Yurtdışından getirilen cep telefonuna kısıtlama, kitap hariç eşyaya vergi,”[in Turkish], Medyascope, May 15, 2019, [https://medyascope.tv/2019/05/15/yurt-disinda-getirilen-cep-telefonuna-...](https://medyascope.tv/2019/05/15/yurt-disinda-getirilen-cep-telefonuna-...)

C5 0-6 pts
Does state surveillance of internet activities infringe on users’ right to privacy? 16

Government surveillance and the bulk retention of user data have violated privacy rights. Leaked emails revealed a contract between the Italian surveillance software company Hacking Team and the General Directorate of Security (GDS), a civilian police force, for the use of Hacking Team’s Remote Control System (RCS)” from 2011 to 2014.1 Under Turkish law, the interception of electronic communications had fallen under the purview of the TİB (now the BTK), and questions remain over the legality of the GDS using software that can infiltrate targets’ computers.

The prominence of alleged Gülenists in the police and judiciary had been a major point of discussion in the country in recent years, particularly after Gülenists were widely blamed for leaked wiretaps that led to various government corruption scandals in 2013 and 2014. Further scandals prompted high-level dismissals and reshuffling within the police and judiciary, apparently aimed at removing suspected Gülenist officials.2 The 2016 coup attempt prompted a new wave of surveillance as part of the broader purge of individuals with alleged links to banned groups.3

According to Article 22 of the constitution, “Everyone has the right to freedom of communication, and secrecy of communication is fundamental.” This right can only be limited by a court order in cases affecting “national security, public order, prevention of the commission of crimes, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law in cases where delay is prejudicial.”4 For the most part, any action that could interfere with freedom of communication or the right to privacy must be authorized by the judiciary. For example, judicial permission is required for technical surveillance under the Penal Procedural Law. Before the passage of the Homeland Security Act in 2015, the law allowed Turkish security forces to conduct wiretapping for 24 hours without a judge’s permission in urgent situations. However, under the new law, the time limit was increased to 48 hours, with a new requirement that officials who conduct wiretapping notify their superiors. In addition, only the Ankara High Criminal Court is authorized to decide whether a wiretapping request is legitimate. Despite constitutional guarantees, most forms of telecommunication continue to be tapped and intercepted.5

Furthermore, the powers of the National Intelligence Organization (MİT) to conduct surveillance were expanded under Law No. 6532 on Amending the Law on State Intelligence Services and the National Intelligence Organization, which was passed
in 2014 and grants intelligence agents unfettered access to communications data without a court order (see C6).

In a clause under Law No. 6532 (see C6) related to the MİT’s ability to intercept and store private data on “external intelligence, national defense, terrorism, international crimes, and cybersecurity passing through telecommunication channels,” no requirement to procure a court order is mentioned.6 The law also limits MİT agents’ accountability for wrongdoing. Courts must obtain the permission of the head of the agency in order to investigate agents, and journalists or editors who publish leaks on MİT activities may be imprisoned for three to nine years. The law has facilitated a crackdown on government opponents such as the Gülenists.7

In a largely positive development, the Data Protection Law entered into force in 2016, aligning the country’s legislation with EU standards.8 In April 2019, the Personal Data Protection Authority fined Facebook 1.65 million Turkish lira ($280,000) due to an application programming interface (API) bug that allowed third-party applications to access the photos of users, including from Turkey.9

3. As of January 2017, almost 70,000 social media accounts had been put under surveillance since July 2016 (“Over 68K social media accounts under police surveillance in Turkey,” Birgun, January 17, 2017, http://www.birgun.net/haber-detay/over-68k-social-media-accounts-under-...
Are service providers and other technology companies required to aid the government in monitoring the communications of their users?

Law No. 6532 (see C5) forces public and private bodies—including but not limited to banks, archives, private companies, and professional organizations such as bar associations—to provide the MİT with any requested data, documents, or information regarding certain crimes related to national security, state secrets, and espionage. Failure to comply can be punished with imprisonment.

Under Law No. 5651, hosting and access providers must retain all traffic information for one year and maintain the accuracy, integrity, and confidentiality of such data. In addition, access providers must file the data together with a time stamp and provide assistance and support to the TİB (now the BTK) in monitoring internet traffic. In 2015, the Constitutional Court nullified a set of amendments passed in 2014, including a requirement that hosting providers must store data for up to two years.1

Public-use internet providers have different responsibilities for retaining data, depending on whether they hold commercial or noncommercial status. Commercial providers are defined as entities such as internet cafés that provide internet service for a payment. Noncommercial public-use internet providers are defined as entities that provide internet service at a certain venue for a specific period of time, such as hotels and restaurants. While all public-use internet providers are expected to take measures to prevent access to illegal content and store internal IP distribution logs, commercial providers must also receive permission from the local authorities, use a
content-filtering service approved by the BTK, and keep accurate daily records of internal IP distribution logs using software supplied by the BTK, which must be stored for a period of one year. In addition, these commercial providers are required to install a video surveillance system to identify users, and retain such records for seven days. All data must be made available to the BTK upon request, and a court order is not required. Those who do not comply can face fines between 10,000 ($1,700) and 100,000 Turkish lira ($16,800).


C7 0-5 pts
Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?

Harassment of journalists on social media is a problem in Turkey. Since 2016, the International Press Institute (IPI) has collected at least 950 instances of abusive behavior against journalists online and 176 threats of violence.1 A Twitter account (@ustakiloyunlari) with over 100,000 followers has regularly smeared journalists and threatened to release personal information about them. Online speech on Islam or the prophet Muhammad, the Kurdish situation, and even mild criticism of the president, government, or ruling party can result in death threats and legal battles. Citizen journalists and reporters for online news outlets risk assault in retaliation for their reporting.2


2. Erkan Saka, “Social Media in Turkey as a Space for Political Battles: AKTrolls and other Politically motivated trolling,” Middle East Critique 2018, https://www.academia.edu/36018785/Social_Media_in_Turkey_as_a_Space_for...
Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?

News sites have frequently come under technical attack at politically sensitive moments or after publishing controversial information. In July 2019, after the coverage period, the blog and news site of journalist Fehmi Koru were inaccessible for around two days due to a cyberattack. Koru had published a blog post alleging that the head of the Nationalist Movement Party (MHP), Devlet Bahçeli, had gained more authority by forming an alliance with the AKP. He was later criticized for the post by Bahçeli, who referenced Koru’s ties to Gülenists. The arts and culture news site Sanatatak suffered technical attacks after publishing a letter supporting Turkish actress Füsun Demirel, who had declared that she had “wanted to be to be a [Kurdish] guerrilla” in her youth. The website was inaccessible for about 48 hours in 2016 due to distributed denial-of-service (DDoS) attacks.

While opposition news sites and Twitter accounts are frequently targeted by progovernment hackers, government ministers have also been affected. The 2016 penetration of the personal email account of Berat Albayrak by RedHack, a Turkish hacking group, yielded more than 57,000 messages from 2000 to 2016, including many that covered state affairs. The material was uploaded to Dropbox, OneDrive, GitHub, and Google Drive. In 2017, the BTK announced that the government would set up an army of “white-hat hackers” to defend Turkey in cyberspace.

Country Facts

- Freedom in the World Status
  Not Free
- Networks Restricted
  No
- Social Media Blocked
  No
- Websites Blocked
  Yes
- Pro-government Commentators
  Yes
- Users Arrested
  Yes

Previous Reports
• 2018 Report