## Iran

Not Free  
15  
100  

<table>
<thead>
<tr>
<th>Category</th>
<th>Score</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Obstacles to Access</td>
<td>7</td>
<td>25</td>
</tr>
<tr>
<td>B Limits on Content</td>
<td>5</td>
<td>35</td>
</tr>
<tr>
<td>C Violations of User Rights</td>
<td>3</td>
<td>40</td>
</tr>
</tbody>
</table>

Last Year's Score & Status  
15 100 Not Free

### Overview

Internet freedom remained highly restricted in Iran during the coverage period, as authorities handed down harsh prison sentences to online journalists and other users, and continued to block access to independent news sites and a number of social media and communication platforms. While no internet shutdowns were observed during the coverage period, authorities maintain vigorous control over the internet infrastructure.

Iran holds elections regularly, but they fall short of democratic standards due in part
to the influence of the hard-line Guardian Council, an unelected body that disqualifies all candidates it deems insufficiently loyal to the clerical establishment. Ultimate power rests in the hands of the country’s supreme leader, Ayatollah Ali Khamenei, and the unelected institutions under his control. These institutions, including the security forces and the judiciary, play a major role in the suppression of dissent and other restrictions on civil liberties.

Key Developments

June 1, 2018 - May 31, 2019

- Unlike previous years, no internet shutdowns were reported during the coverage period. However, the state maintains significant control over the internet backbone, allowing the government to throttle foreign connection speeds at politically sensitive times (see A3).

- Several harsh prison sentences were handed down during the reporting period in retaliation for online activities. Mostafa Abdi, an editor of the news site Majzooban Noor, was sentenced to 26 years in prison and 74 lashes in August 2018. Five other journalists at the outlet received sentences ranging from 7 to 12 years (see C3).

- State-sponsored malware attacks have targeted a range of minority groups and activists located within and outside Iran, according to a May 2019 report from the Center for Human Rights in Iran (see C5).

A Obstacles to Access
Internet penetration rates have improved in recent years, and connectivity in rural areas has increased. The Supreme Council of the Cultural Revolution announced in May 2019 that the National Information Network (SHOMA), an initiative meant to improve access across the country, was over three-quarters finished. While no internet shutdowns were reported during the coverage period, the government maintains the capacity to throttle foreign connection speeds during politically sensitive periods.

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

Internet penetration, bandwidth, and speeds have increased markedly in recent years due to heavy government investment in information and communication technologies (ICTs). The International Telecommunication Union (ITU) estimated internet penetration at approximately 70 percent in 2018.\(^1\) A report published by the Communications Regulatory Authority (CRA) claimed that 89 percent of Iranians had internet access, including through mobile phones, at the end of June 2018.\(^2\)

According to the ICT minister, internet bandwidth increased from 724 Gbps to 4,000 Gbps during President Hassan Rouhani’s first term. The ICT Ministry had set a target of 12,000 Gbps by the end of 2017.\(^3\) According to a report published by the ICT Ministry in September 2018, Iran’s international internet bandwidth has reached 1,805 Gbps and the domestic data transition bandwidth is 22,191 Gbps.\(^4\) However, both Ayatollah Ali Khamenei and the parliament have warned authorities against increasing bandwidth before SHOMA’s completion.\(^5\)

In January 2019, the ICT minister attended the inauguration of a plan to implement SHOMA, known as the National Information Network, which is meant to increase the capacity of Iran’s internet protocol (IP) core network.\(^6\) The project demonstrates that, despite the deteriorating economy,\(^7\) authorities remain committed to developing SHOMA. SHOMA plans initiated in 2017 included the development of the national wireless network, featuring 4.5G service in 710 cities; expansion of IP backbone projects and fiber networks; expansion of the content delivery network (CDN); and an agreement with Nokia for research and delivery of 5G mobile service.\(^8\)
In May 2019, the Supreme Council of the Cultural Revolution announced that SHOMA was 80 percent complete. Saied Reza Ameli, the council’s secretary, asserted that the government allocated nearly 120 trillion rials ($285 million) to create a national cyber platform, while the private sector contributed 70 trillion rials ($166m).

Private and state-backed companies have sought foreign investment to improve the ICT infrastructure. In 2017, the South African telecommunications company MTN announced that it would bring fiber-optic networks to the cities of Tehran, Karaj, Qom, Tabriz, Shiraz, Isfahan, Ahvaz, and Mashhad. MTN would have controlled 49 percent of the Iranian Net Company, a consortium established in 2011 to deliver fiber-optic upgrades. However, in July 2018 the deal was scuttled due to MTN’s apparent failure to adequately fund the consortium. The deal’s failure was also attributed to expected sanctions from the United States.

As of December 2018, 70,000 kilometers of fiber-optic cables have been installed in 350 cities and villages across Iran, according to the Telecommunication Infrastructure Company (TIC), a state-owned enterprise controlled by the ICT Ministry.

2. “More than 3 million Iranians have high-speed Internet access,” Iran Intl, October 7, 2018, https://perma.cc/M3WC-27DE.
3. The Iran Project, “Minister: Iran Internet bandwidth to increase to 12,000 Gbit/s,” April 17, 2017, http://theiranproject.com/blog/2016/04/17/minister-iran-internet-bandwi....
7. Thomas Erdbrink, “Iran Faces Worst Economic Challenge in 40 Years,


14. “Thousands of kilometers of fiber were created in the country,” Mehr News, December 1, 2018, https://www.mehrnews.com/news/4490583/%D9%A7%D9%A0-%D9%87%D8%B2%D8%A7%D7%9C....

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? 13

The government’s investment in ICT infrastructure through SHOMA has increased internet connectivity in rural areas, lessening the urban-rural divide in access. The CRA has implemented measures to extend access to rural areas and decrease prices for users. According to a report by the ICT Ministry published in September 2018, 36,000 villages were connected to high-speed internet.1 Official figures claim that no rural villages were connected to high-speed internet before the Rouhani presidency.2 In February 2019, the CRA asserted that 80 percent of Iranian families would have broadband internet with speeds of at least 20 Mbps by 2021. However, some analysts are skeptical of this prediction, given the recent decline in broadband...
A3 0-6 pts

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

The development of SHOMA and the state’s control over the internet backbone provides the government with the ability to throttle foreign connection speeds during politically sensitive periods without crippling critical services. Moreover, a number of social media platforms and communication applications are blocked (see B1).

While no internet shutdowns were observed during the coverage period, in January 2019, authorities announced that security forces would hold a two-hour internet shutdown exercise later in the month, in which foreign-hosted data would be inaccessible. However, the exercise was ultimately cancelled, reportedly due to an online backlash.1

At the height of antigovernment protests across the country in January 2018, authorities slowed down internet connections and at times completely blocked access to servers and data outside Iran. The network monitor BGPmon noted in a tweet that international traffic temporarily dropped by nearly 50 percent on January 1.2 Small Media’s Filterwatch found that, “Although the incident only lasted for 12 minutes, the timing of the event does suggest that traffic was being intentionally throttled, and that the state has the capacity to limit international traffic as it chooses.”3 During the same timeframe, Iranian internet users reported major disruptions in access to servers hosted by the New York-based company DigitalOcean, which was apparently caused by internet service providers (ISPs) inside Iran.4
The Telecommunication Company of Iran (TCI) retains a monopoly on internet traffic flowing in and out of the country.\(^5\) In addition, TCI’s dominance of the ISP market provides an opportunity for the security apparatus to monitor online activities, since TCI’s majority shareholder is the Islamic Revolutionary Guard Corps (IRGC), a powerful branch of the security forces that also controls large portions of the economy (see A4).\(^6\)

Iranians often use virtual private networks (VPNs) and other circumvention tools to bypass censorship (see B1). However, the government regularly seeks to disrupt access to VPNs.

- 2. BGPmon.net, (@bgpmon,), “Close to 50% drop in announced BGP routes as well as a traffic drop from Iran between 13:23 UTC – 13:35 UTC,” Twitter post, January 1, 2018, [https://twitter.com/bgpmon/status/947871872619655170](https://twitter.com/bgpmon/status/947871872619655170).
- 4. Ibid.

A4 0-6 pts
Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?

The telecommunications industry is tightly controlled by the government. TCI owns the Data and Communication Company (DCC), the country’s main ISP. The Mobile Telecommunication Company of Iran (MCI), a subsidiary of TCI, is the largest mobile service provider.\(^1\)
In January 2018, the Supreme Leader ordered the IRGC and other security forces to reduce any economic activities that are not related to their core missions.\textsuperscript{2} and in October 2018, the corps announced that it was selling its stake in TCI.\textsuperscript{3} However, as of May 2019, there was no indication that the sale had taken place.

The second largest mobile service provider, MTN Irancell, is owned by MTN and Iran Electronics Industries, a state-owned subsidiary of the Ministry of Defense.\textsuperscript{4}

- \textsuperscript{1} “77 million mobile phones in hands of Iranian” Mehr News Agency, August, 31, 2016.
- \textsuperscript{2} “Khamenei Orders IRGC To Reduce Controversial Involvement In Economy,” Radio Farda, January 21, 2018, https://en.radiofarda.com/a/iran-khamenei-irgc-economic-role/28987830.h...
- \textsuperscript{3} “IRGC Gives Up Stake In Telecommunications Possibly To Avoid Sanctions,” Radio Farda, October 24, 2018, https://en.radiofarda.com/a/iran-irgc-gives-up-stake-in-telecommunicati...

A5 0-4 pts
Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?

The bodies that regulate the telecommunications sector lack independence. The Supreme Council of Cyberspace (SCC) sets most of the policies related to the internet. The council was established through a 2012 decree by the Supreme Leader and is comprised of 17 representatives from government institutions and 10 members appointed by Khamenei.\textsuperscript{1} It is intended to provide a centralized point for policymaking and the regulation of Iran’s virtual space, effectively minimizing the roles of the executive, legislative, and judicial branches and bringing internet policy under Khamenei’s direct control.

The CRA, which falls under the ICT Ministry, is responsible for telecommunications licensing. Its head is appointed by the ICT minister.\textsuperscript{2}

In 2015, Khamenei consolidated the SCC’s power over internet policy and made
some personnel changes to the council. In 2016, he dissolved the High Council of Informatics, the Supreme Council of Information, and the Supreme National Security Council of Information Exchange (AFTA), incorporating their responsibilities into the SCC.3

In the past, the SCC has been routinely criticized for being disorganized,4 not holding meetings frequently enough,5 and insufficiently encouraging Iranians to use the internet in a “clean” and Islamic fashion.6 However since Rouhani’s 2017 reelection and appointment of Mohammad-Javad Azari Jahromi as the ICT minister, SCC meetings have been held more frequently.7

The ICT Ministry and Islamic Republic of Iran Broadcasting (IRIB)—the state broadcaster whose head is appointed directly by the supreme leader—appear to be at odds on the right to license internet protocol television (IPTV) services. The ministry has sought to capitalize on expanded bandwidth by promoting IPTV as a new avenue for media diversity. However, in 2016, the IRIB notified all private IPTV providers that licenses issued to them by the ICT Ministry were invalid, insisting that only the IRIB has the power to issue licenses.8 The broadcaster began issuing its own licenses in 2017.9 The conflict had yet to be resolved as of May 2019.10

B Limits on Content

Significant restrictions on content have been in place since 2009. Major international platforms like Facebook and Twitter remained blocked during the coverage period, as was Telegram. Censorship decisions remained highly politicized, with both conservative and reformist news sites facing censorship for failure to adhere to strict guidelines on coverage of sensitive political, social, and international issues. Self-censorship is pervasive, and overt digital activism is fairly limited.

B1 0-6 pts

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

 Authorities restrict access to tens of thousands of websites, particularly those of international news services, the political opposition, ethnic and religious minority groups, and human rights organizations. Websites are also blocked if they contradict state doctrine regarding Islam, as well as the government narrative on domestic or international politics. News stories that cover friction between political institutions are also frequently censored.

Twitter, Facebook, and YouTube, are all blocked, in addition to major blog-hosting platforms like WordPress, Blogspot, and Blogger. Conservative leaders have repeatedly exerted pressure on the Committee to Determine Instances of Criminal Content (CDICC)—a government body headed by the prosecutor general that consists of representatives from 12 state institutions—to block other prominent social media platforms, while President Rouhani has used his administration’s six seats and two parliament representatives on the committee to push back in some
Apps and websites have been blocked over links to foreign countries, particularly the United States and Israel. For example, the navigation app Waze and messaging app Viber, which were developed in Israel, were first blocked in 2017 and 2014, respectively. After authorities blocked Viber, Telegram became the most widely used messaging app in the country, with an estimated 40 million monthly users in 2017.

However the government soon pushed back against the platform, blocking Telegram’s encrypted voice calling feature in 2017 before blocking the entire service, along with Instagram, for several days in late 2017 and early 2018 in response to antigovernment protests. In April 2018, a prosecutor in the Media Court issued an order to filter Telegram, which led to all normal access to the platform being obstructed by ISPs and mobile service providers. Since the ban, authorities have provided financial support for and promoted domestic messaging apps as an alternative to Telegram (see C6).

According to BGPStream, for one hour in July 2018, TCI rerouted IPs associated with Telegram, making the messaging app temporarily inaccessible even with the use of circumvention tools such as VPNs. This violated the Computer Crimes Law and, in response to the hijacking, Jahromi tweeted that the CRA would investigate the incident and impose a large fine on TCI.

Despite the ban on Telegram, two of its “client apps,” Talaeii and Hotgram, were still accessible to Iranians during the coverage period, though they were later shut down (see C6). The two versions, which were allegedly created in part by a national security agency, blocked channels the authorities disapproved of, such as BBC Persian and the Center for Human Rights in Iran.

In January 2018, the government reportedly lifted a long-standing ban on the Chinese messaging app WeChat, restoring access to the platform.

Internet censorship is highly politicized, often reflecting tensions between conservatives and reformists. Instagram’s live video feature was temporarily blocked in 2017. Pro-Rouhani and reformist figures had been using the platform to broadcast nightly debates and cover campaign rallies in support of Rouhani’s reelection the following month. No government body took responsibility for the blocking order.

Domestic news sites are frequently blocked for criticizing the government. Anar
Press and Aban Press, for example, were blocked after the editor-in-chief of both sites was arrested in April 2019. In 2016, Memari News was blocked on the order of the public prosecutor of Tehran after it published a letter from a judicial body to the Tehran municipality that exposed corruption. Borna News, Moj News, and Nasim News were similarly blocked in 2016 though the latter two appeared to be accessible as of May 2019.

In recent years, authorities have even targeted commercial websites for filtering and blocking. In February 2019, the head of the Iranian Cyber Police (FATA) in Tehran revealed that it had requested the leading website for classified advertisements, Divar, be filtered. However, the request had not yet been fulfilled at the end of the coverage period. From June to September 2018, nearly 180 commercial tourism websites were blocked based on an investigation into unauthorized activities. In July 2018, during the economic crisis, a number of online trading outlets selling bitcoin were blocked.

Circumvention tools are frequently used in Iran to access blocked web content. In a May 2019 interview with BBC Persian, Michael Hull, the head of the circumvention tool Psiphon, claimed that between one and two million people in Iran use Psiphon daily.

Authorities employ a centralized filtering system that can effectively block a website within a few hours across the entire network. Private ISPs are forced to either use the bandwidth provided by the government or route traffic containing site-visit requests through government-issued filtering boxes developed by software companies within Iran. The filtering boxes inspect URL requests submitted by users for banned text strings—either keywords or domain names—and block access accordingly. This method only limits access to content retrieved through unencrypted Hypertext Transfer Protocol (HTTP) connections. Individual pages remain available over an encrypted connection (HTTPS), which disguises the banned text, requiring censors to block the entire site in order to restrict access to specific content.

15. “Iran arrests editor Abdollahi, fails to disclose charge or his location,” CPJ, May 3, 2019, https://cpj.org/2019/05/iran-arrests-editor-abdollahi-fails-to-disclose...
Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?

Authorities frequently employ administrative measures to force the removal of legitimate online content. Content removals were common during the 2017 presidential election period. According to the Center for Human Rights in Iran, hours after the Rouhani campaign published a video in which reformist former president Mohammad Khatami declared his support for Rouhani’s reelection bid, campaign officials were told by the judiciary to delete the video from social media or face arrest.1

In March 2019, the Iranian Android app store Myket reported that the CDICC had ordered it to remove 12 apps, including Wizz, WeChat, Tango, and IMO. Myket complied with the order.2

The IRGC routinely arrested Telegram group administrators in order to coerce them to remove content or delete their channels from the platform (see C3). This was prevalent in the months prior to the 2017 presidential election, when the reformist-aligned Telegram channels operated by Eslahtalaban News, Eslahat News, Majmeye Eslahtalaban, and Haamiyan Dolat were either deleted or stopped publishing due to
the arrests of their administrators. The prosecutor general stated in 2017 that the judiciary issued orders to block tens of thousands of Telegram channels every week, but company representatives denied accusations that they complied with censorship beyond the removal of terrorist content and pornography.


**B3 0-4 pts**

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

Censorship decisions are made by the CDICC, and they are often arbitrary and lack transparency. Such decisions are ostensibly made based on the 2009 Computer Crimes Law (CCL), which outlines a broad range of banned content, from insulting religious figures and government officials to distributing pornographic content and using illegal circumvention tools. In practice, little information is available about the inner workings of the committee.

Former ICT minister Mahmoud Vaezi suggested that the country may transfer more censorship authority to ISPs during the next phase of SHOMA development. Empowering ISPs to censor content may result in more repressive policies, since the...
IRGC is a dominant player in the ISP market, and reformists would be unable to counter such decisions. SHOMA also aims to move much of the content and websites visited by users to domestic servers, where traffic can be closely monitored and censored by the authorities.

The prosecutor general leads the CDICC and is responsible for convening the body’s meetings. In January 2019, two members of parliament who sit on the CDICC wrote to the parliamentary speaker complaining about the lack of regular meetings and questioning the legality of attempts to hold online votes on filtering websites. The prosecutor general’s reluctance to call a meeting may stem from the fact that the ICT Ministry and its allies likely have enough votes to reject attempts to block certain sites.

Website owners must register their sites with the Ministry of Culture and are then subject to requests to remove posts deemed unacceptable by the government. The 2009 CCL makes hosts such as blogging platforms responsible for any content that appears on their sites. This has led to the suspension of blogs and shuttering of news sites hosted on platforms inside Iran, under orders from government officials.

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

Self-censorship among journalists and ordinary users is extensive, particularly in regard to political issues. The arrests and imprisonment of journalists, activists, and ordinary citizens in retaliation for their online activities, as well as perceptions of pervasive surveillance, contribute to self-censorship. Many journalists and bloggers abandoned their online activities or used pseudonyms after the crackdown on 2009 protests linked to that year’s disputed presidential election, resulting in a palpable reduction in the amount of original content produced by users. The situation slightly improved after Rouhani assumed the presidency in 2013, especially among reformist journalists. Nevertheless, tight restrictions on journalism and online speech remain in place, and journalists continue to be prosecuted (see C3). In addition, the intimidation of content producers, particularly on Instagram, has caused a rise in self-censorship on social media platforms (see C7).

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

The state counters online criticism through an extensive digital propaganda apparatus. The regime has backed numerous initiatives to promote blogging among its supporters and members of the Basij paramilitary group. For example, an Iranian cultural center has sponsored the annual National Cyber Jihad Festival for bloggers to promote conservative religious values online. Authorities also actively support the creation of social networks and mobile apps by offering free bandwidth and hosting to local developers. There have been reports of automated accounts spreading military propaganda on Twitter aimed at foreign audiences.

Telegram played a significant role in the 2017 presidential election, with both major campaigns deploying sophisticated tools including chat bots that were set up to disseminate political messages and push back against the other side’s rhetorical attacks. In addition to videos of campaign events, both campaigns shared short audio clips of key passages in the candidates’ speeches. The campaigns were also professionally integrated across platforms, using Telegram to direct followers to
relevant content on Instagram and other services.5

News sites are consistently warned against covering sensitive political or social topics, such as controversial former presidents like Khatami, in a manner the government disapproves of.6

In January 2019, Facebook announced that it had removed 783 pages, groups, and accounts, including some on Instagram, “for engaging in coordinated inauthentic behavior tied to Iran.” The accounts targeted users in various countries, particularly non-Persian speakers. The posts, some originating as far back as 2010, largely consisted of news reports.7

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?

There are a number of regulatory and economic constraints that impact the ability of users to publish online. Only apolitical and progovernment websites receive online advertising revenue. Google does not allow advertising campaigns to target Iran,1 disadvantaging domestic outlets as well as those in the diaspora seeking to cultivate an audience inside Iran.

Since the United States has increased diplomatic pressure on Iran under President Donald Trump, many companies such as the software development platform GitHub no longer offer services to Iranians, forcing them to use domestic alternatives.2

A move to prioritize local content through differential pricing threatens net neutrality, the principle that providers should not discriminate against certain types of content or services. In 2017, the ICT Ministry implemented an information network tariff, which provided a 50 percent discount to users on data for all domestic websites.3

Since the rollout of the 50 percent discount, users have received even larger discounts for a number of domestic services, such as streaming websites and domestic messaging apps, and in some cases, have had the tariff eliminated by ISPs, a move supported by authorities.5

• 1. “Google Traffic is here but what does it mean for Iran?” Techrasa, December 26, 2015, http://techrasa.com/2015/12/26/google-traffic-mean-iran/;
Does the online information landscape lack diversity?  

By splitting domestic and international traffic and creating price incentives for users to browse domestic content, Iran has created barriers to media diversity and innovation (see B6). In 2017, MTN Irancell announced that consumers using VPNs would not receive the 50 percent discount when accessing domestic content, further discouraging the use of circumvention tools to access restricted content.

While Instagram is often used as a news source and a platform to discuss politics, Aparat, an Iranian website similar to YouTube that enjoys less expensive tariff rates, is the second most visited website in Iran. Content on Aparat is governed in accordance with Iranian law, making it difficult for users to access socially or politically sensitive views.


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

Despite formal blocks on Facebook, Twitter, and Telegram, social media plays an important role for dissidents in pursuing online campaigns and sharing information. Instagram and Telegram in particular are popular communication tools for activists. After November 2018 protests in which labor activist Esmail Bakhshi was detained, fellow workers at the Haft Tapeh sugar cane company used their Telegram channel to regularly publish statements about his arrest and mistreatment. In January 2019, Bakhshi used Instagram to post a letter detailing the torture he faced in
prison; he was subsequently rearrested.2

Social media is also used to engage in political debates. In the run-up to the 2017 presidential election, all of the main candidates used social media platforms and messaging apps, particularly Instagram and Telegram, as campaign tools. Even conservative candidates who had once railed against social media used such platforms during the campaign, a demonstration of their political importance in Iran.3

In late 2017, a series of antigovernment protests erupted, which focused on a variety of issues, including the compulsory hijab, corruption, and economic hardship. Social media was used to expand the protests to cities across the country through the first week of January 2018, despite violent clashes with security forces. Additional demonstrations occurred later in the year.4

In the spring of 2019, when parts of the country faced major flooding, Iranians took to Twitter to highlight how the blocking of social media platforms, particularly Telegram and Twitter (which necessitates the use of VPNs), hindered emergency relief efforts. Many called for the bans to be lifted.5


*5.* “Government official says the ban on messaging apps is slowing flood relief in Iran,” Global Voices, April 3, 2019, https://advox.globalvoices.org/2019/04/03/government-official-says-the-....

C Violations of User Rights

There have been no changes to legal restrictions on internet freedom, and several harsh prison sentences were handed down during the coverage period in retaliation for online activities, including a 26-year sentence. State-sponsored malware attacks have targeted a range of minority groups and activists located within and outside
C1 0-6 pts
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 legal framework do not protect freedom of expression and press freedom online. The judiciary lacks independence. The head of the judiciary is appointed by the Supreme Leader. In March 2019, Khamenei appointed Ebrahim Raisi to lead the judiciary. Raisi’s role as a member of the four-person committee responsible for the executions of thousands of political prisoners in 1988 stoked strong opposition from human rights groups.1

The constitution provides for limited freedom of opinion and expression, but a variety of haphazardly enforced statutes limit these rights in practice. In 2016, President Rouhani launched the Citizens’ Rights Charter, a nonbinding document2 that includes commitments to freedom of speech and expression “within the limits prescribed by the law.”3


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

Numerous laws tightly restrict online speech and allow harsh punishments for those who deliberately flout these constraints or inadvertently draw the ire of authorities. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights, none of which are clearly
defined. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize criticism of the government, including online.

The 2009 CCL outlines punishments for spying, hacking, piracy, phishing, libel, and publishing materials deemed to damage “public morality” or result in the “dissemination of lies.” Punishments are severe and include the death penalty for offenses against public morality and chastity, as well as long prison sentences, draconian fines, and other penalties for service providers that fail to enforce government content restrictions. The repressive penal code also applies to online activities.

In February 2018, ICT Minister Jahromi published drafts of five bills meant to codify the legal regime governing ICT policy in Iran, though only one had moved forward to the cabinet at the end of the coverage period. The five bills address e-government, electronic identification, the responsibilities of service providers, electronic financial transactions, and data protection (see C5). Despite their broad reach, none of the proposed bills deal with the restrictions on internet users’ human rights imposed by the CCL.

- **1.** Sources vary on whether the CCL was adopted in 2009 or 2010.
- **5.** Ibid.

C3 0-6 pts
Are individuals penalized for online activities? 06

Authorities arrested and prosecuted numerous individuals for their online activities during the coverage period. In October 2018, the head of FATA announced that nearly 75,000 people had been arrested for online activities in the previous eight years. While some of those arrests may have been justified, many were for legitimate online activities, including criticism of the government.
In August 2018, a revolutionary court in Tehran handed down heavy prison sentences and lashes in absentia to six writers and editors of Majzooban Noor, a news site for Gonabadi dervishes, after they were convicted on charges that included “disturbing public order,” “propaganda against the state,” and “reporting information about the dervish minority to opposition media.” In March 2019, an appeals court upheld the sentences of editors Saleholldin Moradi and Reza Entesari, as well as citizen journalist Sina Entesari, who each received seven-year sentences. Citizen journalist Mohammad Sharifi Moghadam and editor Kasra Nouri were each sentenced to 12 years in prison. Another editor, Mostafa Abdi, was sentenced to 26 years and three months. In addition, each of those convicted received 74 lashes and, upon release, a two-year internal exile concurrent with a ban on participating in civil society and journalism. Three other citizen journalists from the website were handed five-year sentences in July 2018 after being convicted of “meeting and plotting against national security.”

Journalist and activist Hengameh Shahidi received a prison sentence of 12 years and 9 months in December 2018, after she was convicted of spreading false information, insult, and propaganda against the regime for her social media posts criticizing the head of the judiciary. Her appeal was denied by a revolutionary court in May 2019, though the court reduced her sentence to seven-and-a-half years.

In April 2019, Mohammad Reza Nassab Abdollahi, the editor of Anar Press and Aban Press, was arrested by security forces, who also raided his and his mother’s homes and took items including his computer, phone, and hard drive. The reason for Abdollahi’s arrest was unclear, but he had previously been arrested for an article critical of the regime. In November 2018, authorities raided the home of journalist Masoud Kazemi and seized his computers after he tweeted about corruption. Kazemi was initially charged with propaganda against the state, but at his trial in May 2019, he was also charged with acting and colluding against national security.

As Telegram grew in prominence in Iran, security forces turned their attention toward the administrators of the platform’s various channels. In December 2018 and January 2019, three journalists for Gam, a news channel on Telegram that covers politics, were arrested and charged with “assembly and collusion against national security,” “forming groups with the intention to disturb national security,” and “contacts with antistate organizations.” A trial had yet to be scheduled as of
May 2019. In July 2018, a revolutionary court in the city of Isfahan sentenced Mohammad Hossein Maleki, the administrator of the Asre-Javan website and Telegram channel, to death. The death sentence was later overturned by the Supreme Court in May 2019. Asre-Javan sold equipment enabling access to pornographic content on satellite television. Maleki was convicted of “corruption on earth through organized activities regarding the sale of CCcam and several satellite accounts.”

In January 2019, the prosecutor of Omidiyeh, a city in Khuzestan province, issued an arrest warrant for an unspecified number of administrators of a Telegram channel who allegedly published confidential documents that “disturbed public opinion.” The administrators were reportedly in hiding at the time the warrant was issued, and no further updates had been provided on the case as of May.

In September 2018, Mehdi Hajati, a member of Shiraz’s city council, was detained and charged with “propaganda against the state” after tweeting and publicly advocating on behalf of two members of the Baha’i faith. In June 2019, after the coverage period, he began a one-year prison sentence, to be followed by two years in exile, because of the charge.

Amid domestic political tensions between reformists and conservatives, hard-liners within the judiciary and IRGC have conducted a campaign against the perceived “infiltration” of western ideas, individuals, and companies. Numerous foreigners or Iranians with dual nationality who were active in journalism, human rights work, or ICT development have been imprisoned by the authorities, often with little explanation.

For example, Nazanin Zaghari-Ratcliffe, an Iranian-British dual citizen, remained in prison at the end of the coverage period. She was sentenced to five years in prison in 2016 for supposedly spying and designing websites that support sedition.

Iran orders at least 7 journalists jailed and flogged over Dervish protest coverage,” CPJ, August 31, 2018, https://cpj.org/2018/08/iran-orders-at-least-7-journalists-jailed-and-flogg-


5. “Iran arrests editor Abdollahi, fails to disclose charge or his location,” CPJ, May 3, 2019, https://cpj.org/2019/05/iran-arrests-editor-abdollahi-fails-to-disclose-


7. “Iran charges Telegram news channel Gam reporters over labor coverage,” CPJ, June 13, 2019, https://cpj.org/2019/06/iran-charges-telegram-news-channel-gam-reporter-


C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?

The legal status of encryption in Iran is somewhat murky. Article 10, Chapter 2 of the CCL prohibits “concealing data, changing passwords, and/or encoding data that could deny access of authorized individuals to data, computer, and telecommunication systems.” This could be understood to prohibit encryption, but enforcement is not common. Nonetheless, authorities have periodically blocked encrypted traffic from entering the country through international gateways, particularly during contentious moments such as elections.

The government has continued its efforts to curtail the use of circumvention tools, which also have a relatively opaque legal status. The use of VPNs does not appear to be criminalized, unlike the sale or promotion of VPN services.

In January 2018, the ICT Ministry launched its mobile registry scheme. The program makes it illegal for service providers to connect unregistered mobile phones to the internet and was implemented to crack down on the smuggling of mobile phones into the country. In August 2018, the ICT minister announced a smuggling rate of zero. The program has led to concerns about users’ privacy.

Does state surveillance of internet activities infringe on users’ right to privacy? 16

The online sphere is heavily monitored by the state, though Article 37 of the nonbinding Citizens’ Rights Charter states that online privacy should be respected.1 Moreover, in April 2018, Supreme Leader Khamenei issued a fatwa related to users’ privacy on social media and online messaging, saying, “The officials must safeguard the people’s and the country’s security and privacy. Invading the privacy and security of the people is religiously forbidden, and against the Islamic law and must not be undertaken.”2 However, the fatwa has not been enshrined into law.

A draft bill on data protection and privacy (see C2) was presented to the cabinet in July 2018. However, as of May 2019, for reasons unknown, the bill had yet to be approved by the cabinet or the president, nor proposed to the parliament.3 The rights group Article 19 has raised concerns about the content of the proposed bill, citing the lack of independence of the body that would implement the legislation, “as well as the lack of adequate remedies for individuals to counter violations of their rights, and to seek compensation for any damage suffered.”4 A report published by Small Media’s Filterwatch in April 2019 raised concerns that if implemented, the draft data protection bill, along with four other draft bills (see C2) would lead to even greater control and surveillance of internet users.5

In 2015, amid preparation for elections to the parliament and the Assembly of Experts (a body of clerics that appoints the Supreme Leader), the deputy interior minister for security announced that a new “elections security headquarters” would be established “to monitor cyberspace.”6 Similarly, the IRGC launched a military exercise named “Eghtedare Sarallah” in 2015, which included the monitoring of social media activities.7 Also in 2015, the FATA created a new unit for monitoring computer games.8

State agencies such as the IRGC have pressured or coerced detained activists into handing over log-in details for their social media accounts, which the authorities have then used for surveillance and phishing attacks. This seems to be part of a broader pattern, as a number of activists have reported phishing attempts that were apparently sponsored by the government.9 According to a report published by the Center for Human Rights in Iran in May 2019, the government still employs malware to target minority groups both within and outside the country in order to gather private information. Victims of malware attacks include Gonabadi dervishes,
Azeri dissidents, women’s rights activists, and student activists.\textsuperscript{10}

- \textsuperscript{1.} The Islamic Republic of Iran, Charter on Citizens’ Rights, December 2016, \url{http://epub.citizensrights.ir/CitizensRightsEN.pdf}.
- \textsuperscript{2.} "Imam Khamenei’s fatwa: ‘Invading users’ privacy on social media is religiously forbidden’,” Khamenei, April 10, 2018, \url{http://english.khamenei.ir/news/5590/Imam-Khamenei-s-fatwa-Invading-use-...}.
- \textsuperscript{3.} “Iran’s Draft Data Protection Act: Too little but not too late,” Article 19, June 27, 2019, \url{https://www.article19.org/resources/irans-draft-data-protection-act-too-...}.
- \textsuperscript{6.} “A New Round of Intimidation, Arrests, and Prosecution of Social Media Users in Iran,” International Campaign for Human Rights in Iran, June 14, 2015, \url{https://www.iranhumanrights.org/2015/06/intimidation-arrests-social-med...}.
- \textsuperscript{7.} “Cyber army exercises held,” [In Farsi,] Itmen, \url{http://www.fanavarandaily.ir/index.aspx?pid=99&articleid=82120}.
- \textsuperscript{8.} “Cyber Police launches gaming unit,” [In Farsi,] Mehr News, \url{https://perma.cc/8M4H-PTD6}.
- \textsuperscript{9.} Lorenzo Franceschi-Bicchierai, “The Iranian Hacking Campaign to Break into Activists’ Gmail Accounts,” Motherboard, August 27, 2015, \url{http://motherboard.vice.com/read/inside-the-iranian-hackers-campaign-to...}.
- \textsuperscript{10.} “Iranian State Malware Continues to Hack Online Accounts of Religious Minority Groups,” Center for Human Rights in Iran, May 20, 2019, \url{https://iranhumanrights.org/2019/05/iranian-state-malware-continues-to-...}.

\textbf{C6 0-6 pts}

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?

In 2017, the SCC released new regulations entitled Policies and Actions Regarding the Organization of Social Media Messaging Applications. The regulations outline the legal framework for messaging apps operating in Iran and formalize previous demands that foreign messaging apps work with Iranian authorities to obtain
licenses and move their data centers inside Iran. The new rules also task the ICT Ministry with forming a committee to suggest a licensing process for domestic and foreign messaging apps.1

It remains unclear how thoroughly the authorities can monitor the content of messages on foreign social networks, given that some apps encrypt their messages. However, all platforms and content hosted in Iran are subject to arbitrary requests by various authorities to provide more information on their users. Local platforms do not guarantee the kind of user protection offered by some of their international counterparts, which may explain their lack of popularity.

However, since the ban on Telegram, the government has promoted domestic messaging apps such as Soroush and Bale, including through financial and technological support. There are plans to incorporate these apps into e-government schemes, which would provide government and banking services exclusively through domestic messaging apps. The potential rise of these apps, which work closely with the authorities, could further jeopardize the privacy rights of users.2

In November 2018, researchers at the Cisco Talos Intelligence Group warned people against using the Iranian versions of Telegram, including Telegram Talaeii and Hotgram, which became popular after the platform’s ban (see B1). According to Cisco Talos, the apps gain access to all the information on a user’s phone, which could potentially lead to government surveillance.3,4 Google removed Hotgram and Talaeii from its app store and users’ phones in April 2019, citing security and privacy concerns.5 The two apps shut down in June 2019, after the coverage period.6

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?

Extralegal intimidation and violence by state authorities is common in Iran.

In January 2019, a number of Iranian Instagram influencers announced that they would wear a more conservative hijab in their posts and deleted older pictures with less conservative hijabs or no hijab at all. FATA reportedly threatened to suspend the influencers’ profiles if this content was not removed within a week. While the extent of this intimidation and whether it was applied to other content producers is unclear, it signals increased efforts to intimidate nonpolitical actors and a new wave of self-censorship.

A survey of LGBT+ Iranians conducted by Small Media in early 2018 found that half had experienced online harassment, while one in five reported being entrapped by state or nonstate actors on dating apps. This is part of a long-term campaign of harassment against LGBT+ people. Article 19 also identified numerous cases of online harassment against LGBT+ people in a February 2018 report.

In July 2018, lawyer Payam Derafshan claimed that 10 of his clients in Isfahan were summoned to court and asked to move their Telegram channels to the domestic messaging app Soroush. The administrators had reportedly received text messages from a security agency noting that their activities on Telegram were illegal.

- **6.** “Iranian versions of Telegram were closed,” Radio Farda, July 1, 2019, [https://www.radiofarda.com/a/30014027.html](https://www.radiofarda.com/a/30014027.html).
Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?

State hackers often launch cyberattacks against activists and campaigners, including those in the diaspora. Due to growing tensions between Iran, neighboring countries, and the United States, there has been a notable rise in reported hacking campaigns and cyberattacks. Iran has also reportedly perpetrated attacks abroad.\(^1\) In November 2018, ICT Minister Jahromi claimed that the Israeli firm Internet Gold Golden Lines launched a series of cyberattacks on Iran’s network infrastructure that was neutralized by Iranian agencies.\(^2\)

According to a report published by the Center for Human Rights in Iran in May 2019, the Gonabadi dervish website Majzooban suffered state-sponsored distributed denial-of-service (DDoS) attacks in May 2019, which made it inaccessible for hours.\(^3\)

SHOMA is meant to protect against foreign cyberattacks. It was defined in a 2011–16 development plan as “an IP-based internet supported by data centers that are completely undetectable and impenetrable by foreign sources and allow the creation of private, secure intranet networks.”\(^4\)

---


Country Facts

- **Freedom in the World Status**
  - Not Free

- **Networks Restricted**
  - No

- **Social Media Blocked**
  - Yes

- **Websites Blocked**
  - Yes

- **Pro-government Commentators**
  - Yes

- **Users Arrested**
  -
Yes

Previous Reports

• 2018 Report