Freedom House

FREEDOM ON THE NET 2024

# France

FREE

**76** /100

| | |
|---|---|
| A. Obstacles to Access | 22 /25 |
| B. Limits on Content | 29 /35 |
| C. Violations of User Rights | 25 /40 |

LAST YEAR'S SCORE & STATUS

76 /100 **Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

# Key Developments, June 1, 2023 – May 31, 2024

Internet freedom remained robust in France, despite a two-week block on the social media platform TikTok in the Pacific territory of New Caledonia during a state of emergency there. Laws adopted in recent years have expanded censorship of online content or increased online surveillance, but the rights of users remained largely protected.

- In May 2024, after declaring a state of emergency in New Caledonia due to civil unrest linked to protests against proposed voting reforms, the French government blocked TikTok for two weeks and accused the Azerbaijani government of using the application to spread misleading information in support of a separatist movement (see A3 and B5).
- Also in May, French legislators enacted the Law to Secure and Regulate the Digital Space (SREN), which introduced several provisions aimed at protecting users from harmful content, including by allowing state regulators to order the blocking of websites and online platforms that host financial scams or that fail to comply with age verification requirements to prevent minors from accessing pornographic content (see B1 and B3).
- The SREN law allows the media regulator to order social media platforms to institute temporary account bans on individuals who have been convicted of spreading hate speech online (see B2 and B3).
- Viginum, a government agency tasked with combating disinformation, identified several influence operations that sought to manipulate public debate in France ahead of the June 2024 European Parliament elections, with networks of news portal websites and accounts on the social media platform X spreading negative Moscow-backed propaganda about the 2024 Paris Olympics and French support for Ukraine (see B5).
- In November 2023, the president promulgated a new surveillance law that authorizes the remote activation of devices in order to geolocate individuals who are under investigation for crimes punishable by five or more years in prison (see C5).

# Political Overview

The French political system features vibrant democratic processes and generally strong safeguards for civil liberties and political rights. However, successive governments have responded to terrorist attacks, the COVID-19 pandemic, and other challenges by curtailing constitutional protections and empowering law enforcement agencies to infringe on personal freedoms.

# A. Obstacles to Access

**A1** 0-6 pts

| | |
|---|---|
| **Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?** | **6** / 6 |

Infrastructural limitations generally do not restrict access to the internet in France.

As of February 2024, DataReportal estimated the country's internet penetration rate to be 93.8 percent. [1] According to Organisation for Economic Co-operation and Development (OECD) data from June 2023, there were 103 mobile broadband subscriptions per 100 inhabitants. [2]

In 2018, the government and the Electronic Communications, Postal, and Print Media Distribution Regulatory Authority (ARCEP) initiated a Mobile New Deal plan to develop fourth-generation (4G) mobile networks. In the third quarter of 2023, the areas of the country with full 4G coverage had risen to 88 percent, while "white zones" (areas without any 4G reception) fell to 1.9 percent. [3] The 4G networks of the country's four main mobile service providers cover a vast majority (99 percent) of the metropolitan French population. [4] As of June 2023, 13 to 16 percent of all 4G sites in rural areas were attributed to the Mobile New Deal and its "targeted coverage system." [5]

Providers have been piloting fifth-generation (5G) technology across France since 2020. The rollout is concentrated in the largest cities, including Paris, Lyon, Nice, Marseille, Montpellier, and Bordeaux. [6]

According to April 2024 data from Ookla, France had median mobile download and upload speeds of 96.62 Mbps (megabits per second) and 8.20 Mbps, respectively; median fixed-line broadband download and upload speeds increased to 243.47 Mbps and 177.59 Mbps, respectively. [7]

The France High-Speed Broadband Plan aims to provide coverage to the entire country by the end of 2025, with connection speeds of at least 30 Mbps. There were 24.22 million fiber-optic internet subscribers in the fourth quarter of 2023. [8] The plan also aims to deploy very high-speed digital subscriber line (VDSL), terrestrial, and satellite networks throughout the country. [9] In 2023, very high-speed broadband coverage accounted for 75 percent of all high-speed broadband connections, according to ARCEP. [10]

In the aftermath of September 2022 explosions that damaged the Nord Stream gas pipeline in the Baltic Sea, authorities in France and other European countries faced concerns about potential attacks on subsea cables that could limit the region's internet access. The government responded by investing in security capabilities to protect critical internet infrastructure. [11]

In April 2023, environmental activists claimed credit for instances of sabotage affecting electrical infrastructure, which caused brief outages for some 7,000 people and affected internet connectivity. [12]

**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?** | **3**/3 |
|---|---|

Internet connections are relatively affordable. According to Cable, the average price of 1 gigabyte (GB) of mobile data was the equivalent of $0.20 as of July 2023, while the average monthly cost of broadband was €30.99 ($33.87) as of June 2023. [13]

In 2020, a provision was added to France's post and electronic communications code to ensure a "universal electronic communications service" at a reasonable price. [14] There are some 20 internet exchange points (IXPs) located throughout the country, [15] contributing to improved access and lower consumer prices. [16]

The government provides support to the lowest-income households for installation of broadband service. In January 2024, the maximum amount of assistance was increased to €600 ($660) for very high-speed broadband for those with a family income of less than €700 ($770) per month, or who are beneficiaries of other government allowance plans. [17]

Demographic disparities in internet usage persist, though the government has attempted to reduce them. Under the aegis of the Mobile New Deal (see A1), the proportion of French territory not benefiting from very high-speed 4G mobile coverage has fallen from 11 percent to 1.9 percent since 2018, driven by improvements in coverage for rural areas. [18] Some 25 percent of the sites scheduled for rollout of 5G service by the end of 2025 will be in a zone combining communities in low-density areas and those in industrial areas, outside the main towns. [19]

Low digital literacy hinders internet access for some segments of the population. According to data from 2021, digital illiteracy affected more than 15 percent of the population in the 15+ age group. [20] Digital illiteracy was also higher in overseas French regions, where the rate stood at 20 percent. [21] This is consistent with 2021 data from the Digital Economy and Society Index (DESI), which found that 16.1 percent of French citizens had low digital literacy, though the European Union (EU) average was 17.1 percent. [22]

**A3** 0-6 pts

| **Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?** | **5**/6 |
|---|---|

*Score Change: The score declined from 6 to 5 because the government restricted access to TikTok in New Caledonia for two weeks during mass protests and related violence.*

In May 2024, the French government declared a state of emergency in New Caledonia and blocked access to the social media platform TikTok for 15 days, claiming that state actors from China and Azerbaijan were using the app to spread disinformation in support of New Caledonian separatists. [23] The state of emergency was declared after violence broke out during protests by members of the Indigenous Kanak community in opposition to a constitutional reform that

would extend local voting rights to more non-Indigenous French residents in the Pacific territory. [24] Social media users were able to circumvent the block via virtual private networks (VPNs).

Several groups challenged the block on TikTok, arguing that it infringed on freedom of expression and communication, but the Council of State's interim relief judge rejected the request to unblock the platform. In its decision, the council cited a lack of evidence that the blocking had immediate and concrete consequences that required urgent intervention. It noted that all other social media networks—as well as the press, television, and radio outlets—remained accessible, and that the government had said it would lift the block after the unrest ended. [25]

There is no central internet backbone, and internet service providers (ISPs) are not required to lease bandwidth from a monopoly holder, as is the case in many other countries. Instead, the backbone consists of several interconnected networks run by ISPs and shared through peering or transit agreements.

**A4** 0-6 pts

| **Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?** | **4**/6 |
|---|---|

There are no significant hurdles preventing businesses from providing access to digital technologies in France. Service providers do not need to obtain operating licenses. [26] However, the use of frequencies for mobile networks is subject to strict licensing by ARCEP. [27] Only four mobile providers are licensed: Orange, Free, Bouygues Telecom, and SFR. [28] Others, such as NRJ Mobile, make use of these providers' networks to resell internet and mobile services. [29]

Orange, Free, Bouygues Telecom, and SFR dominate both the fixed-line and the mobile service markets. Competition among the four is fierce, but there is little room for other players to enter and gain traction. As of January 2023, each of the four providers held between 20 and 29 percent of the mobile service market. Orange holds the most fixed-line subscribers, with 40 percent of the market as of 2023. [30] In February 2023, a judge ordered Bouygues Telecom to pay €308 million ($337 million) to Free for unfair competition practices that included selling discounted smartphones to new subscribers between 2014 and 2021. [31]

Discussions between ARCEP, Orange, and other telecommunications providers regarding the cost of network maintenance continued in 2024. [32] After complaints that Orange had failed to properly maintain its copper network, which provides ADSL (asymmetric digital subscriber line) internet service over copper telephone lines, Orange requested a 12 percent increase in the price for other operators to access its network in target areas, which ARCEP authorized. However, in February 2024, several other operators filed appeals contesting the decision before the highest administrative court. [33] The copper network was being phased out and was expected to be fully decommissioned by January 2027. [34]

A February 2023 consultation by the European Commission called on all digital market actors to make "fair and proportionate contributions" to the costs of public goods, services, and infrastructure. [35] The EU Digital Markets Act does not include specific details about the financial contributions that telecommunications providers should make to network infrastructure. Nevertheless, the law imposes obligations and rules on providers to promote fair competition, ensure service interoperability, and guarantee fair access to essential digital infrastructure. [36]

**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?** | **4** / 4 |
|---|---|

The telecommunications industry is regulated by ARCEP, [37] while competition is regulated by the Competition Authority and, more broadly, the European Commission. [38] In addition, the French Audiovisual and Digital Communications Regulatory Agency (ARCOM) deals with media and digital platforms that operate online. ARCEP and ARCOM are independent and impartial bodies.

ARCEP is governed by a seven-member panel. Three members are appointed by the French president, while the National Assembly and Senate appoint two each. [39] All serve six-year terms. In January 2021, National Assembly member Laure de la Raudière was nominated to serve as the agency's president. [40] As a member state of the EU, France must ensure the independence of its telecommunications regulators. Given that the government is the main shareholder in Orange, the leading telecommunications company, the European Commission stated in 2011

that it would closely monitor the situation in France to ensure that European regulations were upheld. [41]

ARCOM is a new agency that resulted from the January 2022 merger of the Audiovisual Council (CSA) and the High Authority for the Dissemination of Works and the Protection of Rights on the Internet (HADOPI). It is governed by a nine-member panel; the chair is appointed by the French president, while three members are appointed by the president of the National Assembly, three by the president of the Senate, one by the Council of State, and one by the Court of Cassation. Since June 2022, ARCOM has also been tasked with controlling the blocking of websites that contain terrorist material or child sexual abuse images (see B1). [42]

The 2016 Digital Republic Act broadened ARCEP's mandate, granting the agency investigatory and sanctioning powers to ensure net neutrality. [43] In 2019, ARCEP reiterated its commitment to promoting net neutrality, digital transformation, and technological innovation in France. [44] Since 2018, a series of laws have provided ARCOM with regulatory powers over digital platforms (see B3). [45]

# B. Limits on Content

**B1** 0-6 pts

| **Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?** | **4**/6 |
|---|---|

The government does not generally block websites in a politically motivated manner, though the current coverage period featured the first block on a social media platform during a period of civil unrest. Russian state-owned websites that were blocked in 2022 remained inaccessible during the coverage period. ARCOM frequently blocks websites to combat piracy, particularly in the cases of sporting events and streaming websites; ARCOM announced that it worked with ISPs to block access to 1,544 domain names as of 2023, compared with 772 in 2022. [46]

In May 2024, the government implemented a two-week block on TikTok in New Caledonia during a state of emergency, after violence erupted in connection with

protests against a controversial electoral reform bill (see A3). [47]

In early March 2022, following the Russian military's full-scale invasion of Ukraine, the EU Council issued Regulation 2022/350, ordering member states to "urgently suspend the broadcasting activities" and block the websites of the Russian state-run media outlets RT, Sputnik, RT France, RT Germany, RT Spanish, and RT UK, on the grounds that they "engaged in continuous and concerted propaganda actions targeted at civil society." [48] Soon afterward, ARCOM confirmed in a press release that it was complying with the EU decision. [49]

In June 2022, the EU adopted a new package of sanctions that included directives to block the Russian state-owned broadcasters Rossiya RTR/RTR Planeta, Rossiya 24/Russia 24, and TV Centre International. [50] In July 2022, RT France appealed the EU blocking decision to the Court of Justice of the EU (CJEU), [51] but the court upheld the suspension later that month. [52] Some social media platforms, such as Rumble, preferred to close their services in France rather than ban Russian state media. [53]

Two well-known websites, Sci-Hub and LibGen, have been blocked for offering free access to millions of paywalled academic books, journals, and papers without authorization. Following a complaint from academic publishers Elsevier and Springer Nature, a court ordered the four major ISPs to block the two websites in 2019. [54] Both sites were still blocked during the coverage period, though they remained accessible via VPN.

In May 2024, Parliament adopted and the president signed the SREN law, [55] which enables ARCOM to request the blocking of sites that are found to allow minors to access pornographic content. Once given written notice, site owners have 15 days to take steps to prevent minors' access to pornographic content by verifying the ages of their users (see C4). If sites fail to comply after 15 days, service providers are required to block access to the sites within 48 hours of notification from ARCOM. [56] ARCOM may also instruct search engines, directories, and app stores to dereference the noncompliant websites within 48 hours.

The SREN law also allows ARCOM to request that ISPs prevent access to scam websites for up to three months, as well as to request that search engines and

directories dereference such sites. It requires internet browser providers, after being notified about scam websites, to display warning messages to users about the risk of harm from accessing websites that host scams, defined as content that falsely impersonates someone, illegally collects personal data, exploits security vulnerabilities to access a victim's terminal, or entails phishing attempts meant to deceive a victim into using a false payment or connection page. Browsers must make access to potential scam websites subject to explicit user confirmation for up to three months. La Quadrature du Net, an association that defends fundamental freedoms in the digital environment, stated in October 2023 that this provision of the law would hinder users' freedom and result in excessive censorship. [57]

Though the SREN law was intended to bring national legislation in line with EU law, the European Commission criticized its provisions related to pornographic content as contrary to the EU's Digital Services Act (DSA), because the age verification system required by the French law would encourage pornographic sites to surveil their users (see C4). [58]

Since a deadly series of terrorist attacks struck Paris in 2015, terrorism-related content and incitement to hatred have been subject to blocking. A decree issued in 2015 outlined administrative measures for blocking websites with material that incites or condones terrorism, as well as sites that display child sexual abuse images. [59] Shortly after the decree was promulgated, five websites were blocked, with no judicial or public oversight, for containing terrorism-related information. [60]

In 2018, a Paris court ordered nine French ISPs to block Participatory Democracy, a racist, antisemitic, and anti-LGBT+ French-language website hosted in Japan that was found to be inciting hatred. [61] As of August 2023, the website was accessible at a different URL hosted in the United States, where it remained accessible to users in France at the end of the coverage period. [62]

In 2022, the National Commission for Information Technology and Civil Liberties (CNIL), whose role is to check that requests for removal, blocking, and dereferencing are well-founded, received 36,157 reports. Of this total, 9,536 reports of child sexual abuse images and 208 reports of terrorist content were

deemed illegal. [63] In response, 393 blocking orders were issued, along with 2,951 orders to delist content.

**B2** 0-4 pts

| | |
|---|---|
| **Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?** | **2** / 4 |

The government continues to actively develop legislation regulating the online environment and issues content-removal requests to online platforms based on these laws.

The EU's DSA was adopted in November 2022 and fully implemented in February 2024. It obliges platforms to establish notification mechanisms that enable them to identify and remove illegal content, including illegal hate speech, with the help of users. Platforms must delete illegal content about which they have been notified. In addition, very large online platforms (VLOPs), which were designated in February 2023, are required to evaluate the larger societal risks posed by their systems, to take actions to mitigate those risks, and to evaluate these actions' efficacy. In the long run, the requirements are meant to encourage platforms to limit the visibility and potential harms of content that is problematic but not illegal. [64] In 2021, the French government had anticipated some of these measures by enacting the Guaranteeing the Respect of Republican Principles Law, which authorized ARCOM to oversee hate-speech compliance among very large platforms (see B3). [65] The SREN law enacted in May 2024 was designed in part to incorporate the DSA's requirements into French national law (see B1 and B3).

The SREN law includes measures that hold platforms accountable for removing "violent" online content. Under the law, a court may order a suspension of accounts used to access online services if the account owner has been convicted of spreading online hate, engaging in online harassment, or other serious offenses. [66] The suspensions may last up to six months, or up to one year for a repeat offender. During the sentence, convicted users are prohibited from using their accounts and from creating new accounts to access the same services. Service providers would be notified of the conviction decision, and may implement necessary and proportionate measures to block access to their services by the

convicted individual through other accounts (see B3). Service providers that do not comply with blocking such users and accounts could be fined up to €75,000 ($82,000).

Other EU regulations also facilitate the removal of online content. In June 2021, the EU enacted a regulation on preventing the dissemination of terrorist content online, often referred to as the "terrorist regulation," which obliges platforms to remove "terrorist" content in under one hour. [67] The measure gave ARCOM the authority to issue an injunction to platforms for the removal of terrorist content. La Quadrature du Net criticized the regulation, arguing that it posed a risk of excessive censorship. [68]

According to Google's transparency report, the government issued 983 requests to remove content between July and December 2023, a majority of which (561 requests) were for defamation. [69] Between July and December 2023, Facebook restricted access to 570 pieces of content to comply with local law, including 100 items from Russian state-controlled media that were in violation of EU sanctions, and 25 items for alleged defamation and hate speech. [70]

A government decree issued in 2015 allows for the deletion or deindexing of online content related to child abuse and terrorism (see B1), at the request of the Central Office for the Fight against Crime Related to Information and Communication Technologies (OCLCTIC), a police body. Orders under the decree use an administrative procedure that had been supervised by the CNIL, [71] but in June 2022 this oversight responsibility was transferred to ARCOM (see A5). [72]

The right to be forgotten (RTBF) was recognized in a 2014 ruling from the CJEU, [73] and it was later institutionalized throughout the EU with the implementation of the General Data Protection Regulation (GDPR) in 2018. [74] In recent years, companies like Google and Microsoft have deindexed thousands of URLs in France under the RTBF. [75]

**B3** 0-4 pts

| **Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?** | **3**/ 4 |
|---|---|

Historically, authorities have been fairly transparent about what content is prohibited and the reasons behind specific requests for content removal. Incitement of hatred, racism, Holocaust denial, child abuse and child sexual abuse imagery, copyright infringement, and defamation are all illegal and may be grounds for blocking or takedowns. [76]

The SREN law, enacted in May 2024 (see B1 and B2), allows ARCOM to request—without a court order—that service providers, search engines, and app stores block and dereference websites not in compliance with age verification requirements designed to prevent minors from accessing pornographic content (see C4). When a request to providers is sent by ARCOM, a copy is sent simultaneously to the owner of the website in question. Users who are prevented from accessing content under this law are also directed to an ARCOM page that explains the reason for the blocking. The affected site owner may appeal to an administrative court or magistrate within five days of receiving notification and request the annulment of any blocking or dereferencing measures. The courts then have one month to reach a decision. These judgments can in turn be appealed within 10 days of notification, after which an appellate court must rule within three months of the case referral.

The SREN law also requires service providers to block access for users who have been convicted of spreading online hate, engaging in online harassment, or other serious offenses (see B2). [77] The European Commission criticized this provision for a lack of proportionality, as well as for violating the country-of-origin principle, under which a service is supposed to be regulated primarily by the state where it is based. [78]

La Quadrature du Net raised concerns about the transparency of URL blocking lists under the SREN law's provisions aimed at protecting people from online scams (see B1), arguing that without a complete list of blocked URLs, browsers would have to query the authorities each time a page is requested by a user, so as to check whether it is currently subject to an injunction. This could ultimately reveal the browsing histories of users (see C6). [79]

Under the SREN law, ARCOM is required to submit an annual activity report to the government and Parliament that specifies its injunction decisions, the number of

addresses that have been subject to blocking or dereferencing, and court decisions taken as a result of appeals against the injunction decisions.

Article R645-1 of the criminal code outlaws the display of the emblems, uniforms, or badges of criminal organizations under penalty of a fine, and can justify the blocking or removal of such images when they appear online. [80]

The Guaranteeing the Respect of Republican Principles Law (see C2), often referred to as the antiseparatism law, was enacted in August 2021. [81] In addition to placing broad constraints on religious freedom, especially with respect to Islam, the law enabled an administrative authority to block mirror websites that contain "substantially the same" content as another that was already ruled illegal, without separate review from a magistrate. [82] Unlike the Avia law, an earlier measure on hate speech that was partly struck down by the Constitutional Council in 2020, [83] the antiseparatism law does not compel platforms to remove "manifestly illegal content" within 24 hours of notification by users. [84] The provisions of the Avia law that were left in force by the Constitutional Council simplified systems for notification about disputed content, strengthened the prosecution of online hate speech, and created an "online hate observatory." [85]

The antiseparatism law anticipated some of the notice-and-action procedures that were included in the EU's DSA, [86] which was adopted by the European Parliament in July 2022. For example, Article 42 of the antiseparatism law requires platforms to publish risk assessments, make their terms of service accessible, remove "illegal content" at the request of the CSA (later ARCOM), provide information on how their moderation processes work, quantify the results based on ARCOM's recommendations, and establish an appeals system for content removals. The law does not require judicial oversight of government requests for content removal. Platforms that fail to comply can be fined up to 6 percent of their revenue or €20 million ($21.9 million). [87]

In May 2021, the government transposed into French law the EU Copyright Directive. Among other features, the directive establishes ancillary copyright for digital publishers and makes "online content-sharing service providers" partially liable for copyright violations on their platforms (see B6). [88]

In 2018, Parliament passed a law that aimed to combat disinformation surrounding elections by empowering judges to order the removal of "fake news" within three months of an election. [89] The law places a significant strain on judges, who have 48 hours—following a referral by a prosecutor, political party, or interested individual—to decide whether an accused website is spreading false news. [90]

In March 2024, ahead of the European Parliament elections, the European Commission published guidelines for VLOPs, as part of the DSA, to mitigate risks to electoral processes while safeguarding freedom of expression. [91] The guidelines included recommendations for platforms to provide clear information to the public about the mitigation measures they put in place, including their actions to demote and remove false or misleading content generated by artificial intelligence (AI) tools.

A set of decrees issued in 2015 outlined administrative measures for blocking websites with materials that incite or condone terrorism, as well as sites that display child sexual abuse images (see B1). The decrees implemented Article 6-1 of the 2004 Law on Confidence in the Digital Economy (LCEN), as well as Article 12 of a 2014 counterterrorism law. [92] In August 2022, Parliament passed legislation that adapted French law to EU regulations requiring the swift removal of terrorist content (see B2). The lack of judicial oversight for the blocking of websites that allegedly incite or condone terrorism remains a concern; the National Digital Council has on several occasions emphasized the importance of judicial supervision when implementing removals, monitoring, filtering, or blocking of illicit content. [93]

The OCLCTIC is responsible for maintaining a list of sites that contain prohibited content and must review the list every four months to determine whether such sites continue to contravene French law. The OCLCTIC can ask editors or hosts to remove the offending content, and after a 24-hour period, it can order ISPs to block sites that do not comply. [94] Users attempting to access a listed and blocked site are redirected to a website from the Ministry of the Interior that provides avenues for appeal. A government decree separately allows for the deletion or deindexing of online content from search results using an administrative procedure supervised by ARCOM (see B2). [95] Under this decree, the OCLCTIC submits requests to search engines, which then have 48 hours to comply. [96] The OCLCTIC is responsible for reevaluating deindexed websites every four months

and requesting the reindexing of websites when the incriminating content has been removed.

**B4** 0-4 pts

| **Do online journalists, commentators, and ordinary users practice self-censorship?** | **4**/4 |
|---|---|

Online self-censorship is minimal. However, laws aimed at countering hate speech might lead to increased government monitoring of internet users, which could encourage self-censorship (see B2 and B3).

Articles 36 and 38 of the antiseparatism law criminalize the publication of information about a person's private, family, or professional life that would expose them to a risk of harm (see B3 and C2). These provisions could also foster self-censorship. **97**

There are recurrent debates about freedom of expression and self-censorship in French media, with some outlets objecting to regulatory actions that they perceive as unduly restrictive. The television outlets CNews and C8, both owned by the Canal+ media group and right-wing billionaire businessman Vincent Bolloré, regularly call critical attention to ARCOM's content removal decisions. ARCOM in turn has sent several formal notices asking the outlets to respect their obligation to remove unlawful material. **98**

**B5** 0-4 pts

| **Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?** | **3**/4 |
|---|---|

Content manipulation remains a problem on some issues, especially those pertaining to the Russian invasion of Ukraine.

In February 2024, Viginum, a government agency created in 2021 to combat foreign digital interference, reported that it had identified a network of news portal websites, dubbed "Portal Kombat," that was designed to promote Russian propaganda about Moscow's full-scale invasion of Ukraine among audiences in

countries including France. [99] The sites shared news from Russian state media, translated into French, that portrayed the invasion positively and denigrated Ukrainian leadership. [100]

In May 2024, Viginum accused Azerbaijan's government of spreading anti-French propaganda by amplifying misleading photos on social media platforms during the protests in New Caledonia that led to violent civil unrest. [101] The French government later blocked the social media platform TikTok in New Caledonia for two weeks after declaring a state of emergency (see A3).

In June 2024, Viginum publicly identified another online Russian influence operation, dubbed "Matryoshka," that had been active since September 2023. It involved the coordinated dissemination of false reports and memes on the social media platform X (formerly Twitter), with the aim of affecting digital public debate in France. Frequent targets of the operation were French support for Ukraine, French political figures, and the 2024 Olympic Games, held in Paris. After sharing false content from Russian-language channels on the messaging application Telegram, the fake accounts on X challenged the media to verify the false information. [102]

According to the polling firm Ipsos, 72 percent of French people were worried about disinformation on social media platforms influencing their vote in the 2024 EU elections. Some 66 percent of French people reported believing in at least one piece of fake news. [103]

Ahead of the June 2024 European Parliament elections, EU-level political parties signed a code of conduct to protect the elections from foreign interference and disinformation. They agreed to avoid disseminating narratives that came from entities and actors outside the EU, particularly those that "seek to erode European values." [104] The agreement, however, did not apply to national parties, which were the groups conducting most campaigning for the EU elections.

Various groups tried to cast doubt on the validity of the April 2022 presidential election, but researchers later concluded that none of these efforts reached a level that could have altered the voting process or jeopardized the outcome. [105]

**B6** 0-3 pts

| Are there economic or regulatory constraints that negatively affect users' ability to publish content online? | 3/3 |
| --- | --- |

France has a long history of antipiracy laws and regulatory constraints on online content publication. However, users face few practical obstacles when publishing online.

As of January 2022, HADOPI and the CSA merged into ARCOM, a new regulatory body with a greater scope of action (see A5). [106] Some commentators have criticized ARCOM's mandate as overly broad. [107]

Two laws adopted in 2009 were designed to combat online copyright infringement. [108] ARCOM, which assumed HADOPI's role in enforcing the measures, employs a graduated response to alleged violations, starting with an email warning for the first offense, and following up with a registered letter if a second offense occurs within six months. If a third offense occurs within a year of the registered letter, the case can be referred to a court, and the offender may receive a fine. [109]

In May 2021, the government enacted legislation that increased HADOPI's power by implementing the EU Copyright Directive (see B3). [110] The law includes an ad hoc liability system for platforms hosting copyrighted content. [111]

In June 2023, Parliament adopted the Regulating Commercial Influence and Preventing Abuse from Influencers on Social Networks Law (see C3). With the aim of protecting young people, and particularly young women, the law sets new rules for online influencers. It requires the creation of legal contracts for all marketing placements and forbids advertisements on a variety of topics, such as cosmetic surgery, cryptocurrency services, and sports-betting platforms. [112]

The principle of net neutrality is enshrined in law. In 2018, a joint study published by ARCEP and Northeastern University indicated that net neutrality was better respected in France than in the rest of the EU. [113]

In July 2021, France's Competition Authority fined Google €500 million ($550 million) for failing to negotiate licensing fees "in good faith" with French news outlets, which it had been mandated to do in April 2020. [114]

**B7** 0-4 pts

| Does the online information landscape lack diversity and reliability? | 4 / 4 |
|---|---|

France is home to a highly diverse online media environment. There are no restrictions on access to independent online outlets. Platforms that provide content produced by different ethnic, religious, or social groups, including LGBT+ people, are generally not subject to censorship. However, commentators have observed increased online harassment of LGBT+ users (see C7). [115]

Nineteen French television channels were broadcasting online as of 2024. [116] Despite this diversity, ownership patterns have changed as wealthy businessmen with interests in other sectors increasingly acquire media enterprises. In 2022, the chief executive of CMA CGM, a major shipping and logistics company based in Marseille, acquired the regional newspaper *La Provence* and showed interest in purchasing the online video-based news outlet Brut. [117]

The prevalence of misinformation has affected trust in online information. A survey from Ipsos in 2024 found that only 35 percent of people in France trusted online media, compared with 61 percent who trusted print news. [118]

**B8** 0-6 pts

| Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues? | 6 / 6 |
|---|---|

There are few restrictions on digital mobilization in France.

In May 2024, the government blocked the social media platform TikTok for two weeks during a state of emergency in New Caledonia after accusing the Azerbaijani government of spreading misleading, proseparatist content (see A3 and B5). According to a lawyer from La Quadrature du Net, TikTok was blocked in New Caledonia while other social media applications remained accessible because the short-video platform is especially popular among younger residents, whom the government saw as more likely to be involved in civil unrest. [119]

Also during the coverage period, a number of large-scale strikes and demonstrations were held in France. Farmers participating in mass protests against EU environmental regulations used hashtags on social media platforms to mobilize demonstrations across the country. [120]

In 2023, animal welfare topics accounted for 15.9 percent of online activist discussions, according to a study from a communications consultancy, followed by pension reform and police violence as the second and third most popular topics, respectively. [121]

Several digital rights and advocacy groups, such as La Quadrature du Net, are active and have played a significant role in protesting the government's recent moves to expand censorship and surveillance measures without judicial oversight. [122]

# C. Violations of User Rights

**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?** | **5**/6 |

The French constitution explicitly protects press freedom and access to information, and it guarantees freedom of speech and the rights of journalists. [123]

The European Convention on Human Rights, to which France is a signatory, provides for freedom of expression, subject to certain restrictions that are considered "necessary in a democratic society." [124] Since a series of terrorist attacks struck Paris in 2015, the government has adopted various laws, decrees, and administrative provisions that limit fundamental rights, citing the need to ensure public safety. [125]

A counterterrorism law that came into effect in 2017 has raised concerns among civil rights campaigners, as it gave prefects and security forces wide-ranging powers with limited judicial oversight. It included a new legal framework for the surveillance of wireless communications (see C5). [126]

France has an independent judiciary, and the rule of law generally prevails in court proceedings. In some cases, the Constitutional Council has made decisions that protect free expression and access to information in practice (see B2, B3, and C2).

France is working on implementation of the EU's DSA, and some provisions had already been adopted as part of the Guaranteeing the Respect of Republican Principles Law (see C2 and B3). DSA implementation will increase regulation of online expression within the limits of existing European and French laws that define what is acceptable public speech. Critics argue that such regulations are improper infringements on freedom of expression.

**C2** 0-4 pts

| **Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?** | **2**/4 |
|---|---|

Several laws assign criminal or civil penalties for potentially legitimate online activities.

The counterterrorism law passed in 2014 prohibits online speech that is deemed to sympathize with terrorist groups or acts, assigning penalties of up to seven years in prison and a €100,000 ($109,000) fine. Speech that incites terrorism is also penalized. The punishments for online offenses are harsher than for offline offenses, which can draw sentences of up to five years in prison and a €75,000 ($82,000) fine. [127]

Defamation can be a criminal offense in France, punishable by fines or—in circumstances such as "defamation directed against a class of people based on their race, ethnicity, religion, sex, sexual orientation or disability"—by prison time. [128]

In March 2024, Parliament adopted a law strengthening the security and protection of local elected officials. The law added a new aggravating circumstance in cases of online harassment against elected officials, with penalties of up to three years' imprisonment and a fine of €45,000 ($49,200). [129]

Article 36 of the Guaranteeing the Respect of Republican Principles Law, enacted in August 2021, criminalizes the publication of information about a person's

private life, family life, or professional life that would allow the individual to be identified or located for the purpose of exposing them or their family members to a risk of harm (see B3). In most cases, violators face up to three years' imprisonment and a €45,000 ($49,200) fine, but in cases involving the personal information of public officials, the perpetrators face up to five years in prison and a €75,000 ($82,000) fine. The higher penalties for offenses committed against public officials have raised concerns that the law could be used to suppress legitimate criticism of such officials. [130]

In January 2023, the Law on the Orientation and Programming of the Ministry of the Interior (LOPMI) introduced a new criminal penalty for complicity in administering an online platform that enables the transfer or acquisition of illicit content, products, or services. The offense carries maximum penalties of up to €500,000 ($551,820) and up to ten years in prison. [131]

France enacted a law regulating the activities of social media influencers in June 2023 (see B6). Influencers must specify when they are paid to promote products and brands, and are prohibited from promoting certain categories of products, including sports-betting services, tobacco, and cosmetic surgery. Those who violate the law can incur a maximum of two years in prison or up to €300,000 ($330,000) in fines, as well as temporary or permanent bans. Influencers who violate the rules must also display a banner on their social media accounts for 30 days, stating when they have misled users or failed to disclose advertising partnerships. [132]

**C3** 0-6 pts

| **Are individuals penalized for online activities, particularly those that are protected under international human rights standards?** | **5**/6 |
|---|---|

During the coverage period, no citizens faced politically motivated arrests or prosecutions in retaliation for online activities that are protected under international human rights standards. However, users have been convicted in past years of insulting public officials or of inciting or sympathizing with terrorism online.

In September 2023, journalist Ariane Lavrilleaux was held overnight and questioned by police in connection with a story she had written in 2021 for the

investigative journalism website Disclose. The article cited leaked classified documents that implicated French intelligence services in the bombing of civilians on the border between Egypt and Libya. [133] Lavrilleaux's arrest followed a preliminary investigation prompted by a complaint in which the Ministry of the Armed Forces accused her of "compromising the security of national defense" and "revealing information that could lead to the identification of a protected agent." [134] She was released after 48 hours in police custody, during which police reportedly searched her devices (see C5). [135]

In March 2023, a woman was arrested for insulting President Emmanuel Macron in a social media post. She faced a possible fine of €12,000 ($13,100). According to French law, it is illegal to insult a representative of a public body, such as a member of Parliament, a police officer, or a firefighter. [136] The court threw out the case in July 2023, stating that the proceedings were null because a subprefect had filed the case; for the case to be valid, it would have to be filed by Macron himself. [137]

A growing number of individuals, including minors, [138] have been investigated and given fines and prison sentences for "glorifying" terrorism. [139] In October 2021, a 19-year-old man was sentenced to 13 months in prison for glorifying terrorism on Twitter, after he repeatedly posted comments praising the Islamic State terrorist group and claiming that terrorist attacks in France had been "reprisals" for French attacks abroad. [140]

Penalties for threatening state officials are applied to online activities. In 2019, a man was fined €500 ($550) for sending President Macron a death threat on Facebook. [141]

**C4** 0-4 pts

| **Does the government place restrictions on anonymous communication or encryption?** | **2**/4 |
|---|---|

Users are not prohibited from employing encryption services to protect their communications, though mobile users must provide identification when purchasing a SIM card, potentially reducing anonymity for mobile communications. [142] New regulations requiring online platforms to implement age verification systems could threaten online anonymity.

In October 2023, during a trial for seven people facing terrorism charges in the "December 8" case, privacy advocates noted that prosecutors were citing the group's use of encrypted messaging platforms to communicate with one another as evidence of guilt, in the absence of more concrete proof that the seven were planning terrorist acts. [143] La Quadrature du Net and European Digital Rights (EDRi) expressed concern that a conviction would reinforce the narrative that using tools for digital privacy amounts to evidence of criminal behavior, setting a dangerous legal precedent and threatening the right to privacy. [144] The seven defendants were eventually sentenced in December 2023, and all but the one who received a suspended sentence filed to appeal the verdict in January 2024. [145]

There are no laws requiring providers of encryption services to install "back doors" in their products, but those with decryption keys are required to turn them over to investigating authorities. [146] In 2020, the Court of Cassation ruled that any person who is asked, even by a police officer, to turn over decryption keys should comply with the request or face incrimination, overturning a 2019 ruling by a lower court. [147]

Any company that offers encryption tools is required to notify the National Information Systems Security Agency (ANSSI), as well as to retain a description of the technical characteristics of the encryption tool and the source code of its software, according to the 2004 law on confidence in the digital economy. [148] The law prohibits offering encrypted technology services and the import of encrypted messaging applications without prior declaration.

The 2004 law, which had been scarcely used against encrypted communication platforms since its introduction, was invoked after the coverage period to charge Telegram founder Pavel Durov in August 2024 (see C6). Privacy advocates expressed alarm about the case's implications for other encrypted messaging services. [149]

The SREN law requires websites and video-hosting platforms to verify the ages of their users to prevent minors from accessing pornographic content, with those that fail to comply facing financial penalties and potential blocking (see B1 and B3). Once notified that they have allowed unlawful access to pornographic content, site owners have one month to remedy the problem, after which they can draw penalties of up to €150,000 ($164,000) or 2 percent of global revenues, and twice

that amount for subsequent breaches. [150] The technical details of the age verification systems that must be put in place had not been determined by the end of the coverage period; ARCOM was expected to provide guidance in July 2024. [151]

Individuals who operate online public communication services are required to display their full name, address, and telephone number, as well as the name and contact information for their hosting service provider. The SREN law specifies that those who operate an online public communication service in their personal, nonprofessional capacity may preserve their anonymity by publishing only the name of their hosting service provider, so long as they have shared their personal identification details with the hosting provider. [152]

In July 2023, the government enacted Law No. 2023-566 "to establish a digital majority and combat online hate." The law sets 15 as the minimum age for children to register on social media platforms, unless given permission by a parent or guardian to register earlier. [153] The law also applies to accounts on social media platforms created by users under 15 prior to its enactment. Platforms are required to verify the ages of their users and to obtain parental consent for minors 15 and below. [154] Social media companies would be required to implement age verification systems in order to comply, or face fines of up to 1 percent of their annual global revenue. The law raised concerns about the ability of government agencies to identify internet users. [155] In October 2023, the European Commission strongly criticized the law, stating that its age verification requirements were in conflict with the DSA. [156]

**C5** 0-6 pts

| **Does state surveillance of internet activities infringe on users' right to privacy?** | **2** / 6 |
|---|---|

Surveillance has escalated in recent years, including through a surveillance law that was enacted in the wake of a terrorist attack in 2015.

In September 2023, journalist Ariane Lavrilleaux reported that police used surveillance technology to search her emails while she was being detained and questioned in connection with a story she had written in 2021 for the investigative

journalism website Disclose, which referred to leaked classified documents (see C3). [157]

In an internal memo released to the public by Reporters Without Borders (RSF), the Ministries of the Armed Forces and the Interior expressed concerns that provisions of the European Media Freedom Act (EMFA), which was adopted by the European Parliament in March 2024 with the aim of protecting journalists from surveillance, would affect the ability of police and intelligence services to investigate foreign agents and foreign intelligence officers. According to the memo, the ministries both favored a national security exemption that would maintain the possibility of monitoring journalists. [158] The final version of the law prohibits authorities from pressuring journalists and editors to reveal their sources but allows authorities to use spyware "on a case-by-case basis," subject to judicial authorization. [159]

The Ministry of Justice Orientation and Programming Act 2023–27, promulgated in November 2023, allows for a judge to authorize investigators to remotely activate devices in order to geolocate individuals in real time, if the investigation involves crimes punishable by five or more years in prison. [160] The law excludes devices used by members of Parliament, magistrates, journalists, doctors, and justice commissioners. Rights groups have criticized the measure as an infringement on fundamental security and privacy rights. [161]

The 2015 Intelligence Law allows intelligence agencies to conduct electronic surveillance without a court order. [162] An amendment passed in 2016 authorized real-time collection of metadata not only from individuals "identified as a terrorist threat," but also from those "likely to be related" to a terrorist threat and those who belong to the "entourage" of the individuals concerned. [163]

The Constitutional Council declared three of the Intelligence Law's provisions unconstitutional in 2015, including one that would have allowed the interception of all international electronic communications. However, an amendment enabling surveillance of electronic communications received from or sent abroad was adopted later in the year. [164] Article 15 of the 2017 counterterrorism law reintroduced a legal regime for monitoring wireless communications, but it limited surveillance to certain devices such as walkie-talkies. [165]

In July 2021, Parliament passed a counterterrorism law that renewed measures from the 2017 law and expanded the scope of security agencies' surveillance powers, enabling them to use newer technologies. [166] For instance, French intelligence services are able to intercept satellite communications until 2025 and use algorithms to scan internet-connection and browsing data for possible terrorist activity. [167] Under the law, the government is also allowed to use an increasing number of algorithms to identify individuals who have visited extremist websites. [168] Though the law was passed quickly, it received strong criticism from civil society groups and academics. [169]

Following an October 2020 CJEU decision confirming the ban on indiscriminate metadata collection and retention, [170] the French government asked the Council of State to ignore the four EU rulings on that issue, asserting France's national sovereignty. [171] In April 2021, the Council of State ruled that the current data-retention regime was justified due to threats to national security, stipulating that the government should regularly reevaluate whether the security situation justified the continued retention of metadata (see C6). [172] In the 2021 counterterrorism law, this regime was modified, according to the government, to respond to some of the Council of State's concerns. La Quadrature du Net argued that the modification was insufficient to protect individuals' right to privacy. [173]

In 2019, an amendment to a military spending bill (the Military Planning Law, or LPM) expanded official access to data collected outside France's borders by providing domestic antiterrorism investigators with information obtained by the General Directorate for External Security, France's foreign intelligence agency. [174] According to Article 37 of the LPM, domestic investigators may perform, within the intercepted communications, "data spot checks for the sole purpose of detecting a threat to the fundamental interests of the nation," so long as the selected individual or entity can be traced to French territory. [175]

**C6** 0-6 pts

| **Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?** | **3**/ 6 |
|---|---|

Service providers are required to aid the government in monitoring their users' communications under certain circumstances. For instance, they must retain user

metadata for criminal investigations. [176] Although the CJEU ruled against this practice, in April 2021 the Council of State determined that the retention rules were justified (see C5). [177]

The 2015 Intelligence Law requires ISPs to install "black boxes"—algorithms that analyze users' metadata for "suspicious" behavior in real time. [178] The first black box was deployed in 2017, [179] and two more were added in 2018. [180] In 2023, a reported 24,209 people were monitored through intelligence techniques including "security interceptions" and real-time geolocation tracking, in the context of individual surveillance that was ostensibly for national security purposes. [181]

In August 2024, after the end of the coverage period, Telegram founder Pavel Durov was arrested in France, partly because the company had refused to share required information with investigators. [182] Durov was charged with failing to comply with law enforcement, complicity in drug trafficking and the spread of child abuse imagery, and violating a 2004 law that prohibits the import of encryption tools without declaration (see C2 and C4). [183] In September, the company announced that it would begin to share users' internet protocol (IP) addresses and phone numbers with authorities in response to search warrants or legal requests. [184]

La Quadrature du Net cited surveillance concerns arising from what it called a lack of transparency on the URL blocking lists that browsers would be required to enforce under the SREN law's provisions to protect people from online scams (see B1 and B3). In the absence of a publicly available blocking list, internet browsers would presumably have to query authorities on the status of every page requested by every user, meaning users' browsing histories could theoretically be tracked by police. [185]

The CNIL, as France's data protection authority, regularly enforces the data protection measures enshrined in the EU's GDPR and e-privacy directive, as well as competition rules related to the protection of personal data. In December 2023, the CNIL fined Yahoo €10 million ($10.9 million) for using advertising cookies without users' consent on Yahoo.com, and for failing to allow users of its email service to freely withdraw their consent for cookies. [186] The CNIL has fined other companies, including Carrefour, Google, Amazon, Apple, and Microsoft, in previous coverage periods for similar data-related offenses. [187] According to the

CNIL, it handed down 42 sanctions for a total of nearly €90 million ($98.4 million) in 2023 in response to data-related violations. [188]

The European Commission validated a new Data Protection Framework with the United States in July 2023, in accordance with the GDPR. [189] The decision made the transfer of data to the United States subject to strict conditions, including an annual certification regime for recipient companies, compliance with the protective principles stemming from the GDPR, and the introduction of a right of appeal for Europeans at a newly created venue, the Data Protection Review Court (DPRC). [190] The framework drew criticism from privacy activists, who argued that the new agreement was a replica of the previous Privacy Shield agreement, without any improved protection for Europeans' personal data. [191] The DPRC has also been criticized for its lack of direct interaction with data subjects, which could hamper the exercise of their rights. [192]

**C7** 0-5 pts

| | |
|---|---|
| **Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?** | **4**/5 |

*Score Change: The score improved from 3 to 4 because there were fewer reported cases of violence against online journalists during the coverage period.*

Violence against journalists, including online journalists, has been a problem in recent years, particularly for those attempting to cover street protests. [193] In March 2023, as demonstrations against pension reforms degenerated into violent clashes with police, several journalists were intimidated or injured by security officers, and some were taken into custody. [194] However, fewer cases of this kind were reported during the latest coverage period.

In June 2022, Radio BIP, a left-leaning independent radio station in Besançon, faced threats and experienced vandalism, some of which came in response to viral videos posted by one of its journalists on social media. [195]

Online harassment of LGBT+ people remains a problem. [196] Six LGBT+ rights associations filed a complaint against far-right politician Marion Maréchal in May 2024, after she made transphobic remarks on X about a transgender woman who won a joint award for best actress at the Cannes Film Festival. [197]

**C8** 0-3 pts

| | |
|---|---|
| **Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?** | **2**/3 |

Government-affiliated websites experience cyberattacks with some regularity. Local authorities that process and store personal data are also frequently targeted by cybercriminals.

Medical institutions, including hospitals, routinely face ransomware attacks and breaches of patients' personal data. **198** In February 2024, two major French billing operators were hit with a cyberattack in which hackers stole the data of millions of social security beneficiaries and health care professionals. **199**

In March 2024, personal data belonging to 43 million people was exfiltrated in a hack on the job-seeking website France Travail. Though banking details and passwords were not stolen, the exposed personal data increased the risk of phishing attempts for those affected. **200**

In March 2023, the website of the National Assembly was targeted in a distributed denial-of-service (DDoS) attack orchestrated by a pro-Russian hacking collective, NoName057(16), which rendered the website inaccessible for several hours. **201**

## *Footnotes*

1 Simon Kemp, "Digital 2024: France," DataReportal, February 21, 2024, https://datareportal.com/reports/digital-2024-france.

2 "Broadband Portal - Historical penetration rates, fixed and mobile broadband, G7," Organisation for Economic Co-operation and Development, accessed on May 16, 2024, https://www.oecd.org/sti/broadband/broadband-statistics/.

3 ACREP, "Press release - Mobile networks, Mobile coverage, Mobile New Deal: Arcep gives a progress report", February 1st, 2024, https://www.arcep.fr/actualites/actualites-et-communiques/detail/n/couv....

4 Regulatory Authority for Electronic Communications and Post (ARCEP), "Tableau de bord du New Deal Mobile [Dashboard of the Mobile New Deal]," December 16, 2021, https://www.arcep.fr/cartes-et-donnees/tableau-de-bord-du-new-deal-mobi....

5 ARCEP, "New Deal mobile: an update," February 1, 2024, 14, https://www.arcep.fr/fileadmin/user_upload/grands_dossiers/new-deal-mob....

More footnotes

**On France**

See all data, scores & information on this country or territory.

See More ›

*Country Facts*

Population
**67,970,000**

Global Freedom Score
**89** /100 **Free**

Internet Freedom Score
**76** /100 **Free**

Freedom in the World Status
**Free**

Networks Restricted
**No**

Social Media Blocked
**Yes**

Websites Blocked

**Yes**

Pro-government Commentators

**No**

Users Arrested

**Yes**

*In Other Reports*

Freedom in the World 2024

*Other Years*

2023

## Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org