

France

FREE

76
/100

A. <u>Obstacles to Access</u>	23 / ₂₅
B. <u>Limits on Content</u>	29 / ₃₅
C. <u>Violations of User Rights</u>	24 / 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.

[TOP](#)

Overview

Internet freedom is relatively robust in France. Authorities do not block social media platforms, and most websites hosting political or social speech are accessible, though several Russian state-linked websites have been blocked in response to a 2022 order from the European Union (EU). Laws adopted in recent years have expanded censorship of online content or increased online surveillance, but the rights of users remain largely protected. Several new laws were passed during or shortly after the coverage period, including legislation that places advertising restrictions on influencers and new regulations that require social media platforms to verify users' ages.

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.

Key Developments, June 1, 2022 – May 31, 2023

- The EU's Digital Services Act came into force in November 2022, requiring platforms to establish notification mechanisms that enable the identification and removal of illegal content (see B2 and B3).
- In March 2023, a woman was arrested and faced a possible fine for insulting President Emmanuel Macron in a social media post (see C3).
- In July 2023, after the coverage period, French lawmakers advanced amendments to a justice reform bill that would increase surveillance by allowing police officers to remotely access criminal suspects' electronic devices (see C5).

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 January 2023, DataReportal estimated the country's internet penetration rate at 92.6 percent. ¹ According to Organisation for Economic Co-operation and Development (OECD) data from June 2022, there were 100.3 mobile broadband subscriptions per 100 inhabitants. ²

The government has pledged to provide widespread access to high-speed broadband service, with connection speeds of at least 30 megabits per second (Mbps). It has been implementing a national plan to deploy fiber-optic cable, very high-speed digital subscriber line (VDSL), terrestrial, and satellite networks throughout the country, mobilizing public and private investments totaling €20 billion (\$20.7 billion) over 10 years. ³ In 2022, very high-speed broadband coverage accounted for 67 percent of all high-speed broadband connections, according to the Regulatory Authority for Electronic Communications and Post (ARCEP). ⁴

According to an October 2022 report from ARCEP, the average mobile download speed stood at 94 Mbps in 2022, an increase from the previous year. ⁵ According to February 2023 data from Ookla's Speedtest, France had an average fixed-line broadband download speed of 163.8 Mbps. ⁶

In 2018, ARCEP and the government enacted a mobile "New Deal" to develop fourth generation (4G) networks by 2022. According to a 2022 report from ARCEP, the project met its goal of 90 percent of rural areas having 4G coverage by January of that year. ⁷ The 4G networks of the country's four main mobile service providers cover a vast majority (99 percent) of the metropolitan French population. ⁸ Providers have been piloting 5G technology across France since 2020. The rollout is concentrated in the largest cities, including Paris, Lyon, Nice, Marseille, Montpellier, and Bordeaux. ⁹

While many cities benefit from high broadband connection speeds, the promised "universal electronic communications service" has not yet ensured such access for rural areas (see A2). According to the consumer protection association UFC-Que Choisir, 32 percent of users in rural areas did not have access to download speeds higher than 8 Mbps as of January 2022. 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 October 2022, fiber-optic cables were sabotaged in Aix-en-Provence, leading to short-term service disruptions. 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.

In 2022, the Economist Impact's Inclusive Internet Index ranked France 10th out of 100 countries for affordability of internet connections. ¹³ According to Cable UK data, the average package cost of a mobile subscription in France is \$35.66. ¹⁴ The Digital European and Society Index (DESI) reports that 4.5 percent of French citizens do not have access to the internet because it is too expensive. This is above the EU average of 3.2 percent. ¹⁵

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. ¹⁶ There are several internet exchange points (IXPs) in France, ¹⁷ contributing to improved access and lower consumer prices. ¹⁸

Demographic disparities in internet usage persist, though the government has attempted to reduce them. A map produced by ARCEP illustrates some of the regional disparities in mobile penetration, showing patchy 4G coverage in rural areas and overseas territories. ¹⁹ Most at-home users have access to broadband connections, while the remaining households, usually in rural areas, must rely on dial-up or satellite services. ²⁰ The mobile "New Deal" aims to reduce these disparities across the four main mobile service providers; one company, Free, covers 91 percent of French territory, while Société française du radiotéléphone (SFR) covers 95 percent of the country (see A4). ²¹ The government provides support to the lowest-income households for installation of broadband service. In

February 2022, then prime minister Jean Castex announced that the support would increase from €150 (\$155) to €300 (\$310). ²²

Low digital literacy hinders internet access for some segments of the population. According to data from 2019, 17 percent of the population struggled to use digital tools. ²³ This is consistent with 2021 data from DESI, which found that 16.1 percent of French citizens had low digital literacy, though this was less than the EU average of 17.1 percent. ²⁴

A3 0-6 pts

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

6/6

No restrictions on connectivity were reported during the coverage period. 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. The government does not have the legal authority to restrict the domestic internet during emergencies.

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. ²⁵ However, the use of frequencies for mobile networks is subject to strict licensing by ARCEP. ²⁶ Only four mobile providers are licensed: Orange, Free, Bouygues Telecom, and SFR. ²⁷ Others, such as NRJ Mobile, make use of these providers' networks, reselling internet and mobile services. ²⁸

Orange, Free, Bouygues Telecom, and SFR dominate both the fixed-line and mobile service markets. Competition among the four is fierce, but there is little room for other players to enter and gain traction. In February 2023, a judge ordered Bouygues Telecom to pay €308 million (\$319 million) to Free for unfair

competition practices that included selling discounted smartphones to new subscribers between 2014 and 2021. **29**

Discussions between ARCEP, Orange, and other telecommunications providers regarding the cost of network maintenance continued in 2022. **30** Starting in mid-2022, service providers asked online businesses such as streaming platforms to contribute to the financing of telecommunications infrastructure, an idea that has been taken up by the European Commission (EC). **31**

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, **32** while competition is regulated by the Competition Authority and, more broadly, the EC. **33** 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.

34 All serve six-year terms. In January 2021, National Assembly member Laure de la Raudière was nominated to serve as the agency's president. **35** 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 EC stated in 2011 that it would closely monitor the situation in France to ensure that European regulations were upheld. **36**

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 president, while three members are appointed by the chair of the National Assembly, three by the chair of the Senate, one by the Council of State, and one by the Court of Cassation. Since June 2022, ARCOM has also been in charge of controlling the blocking of websites that contain terrorist material or child sexual abuse images (see B1). **37**

The 2016 Digital Republic Act broadened ARCEP's mandate, granting the body investigatory and sanctioning powers to ensure net neutrality. ³⁸ In 2019, ARCEP reiterated its commitment to promoting net neutrality, digital transformation, and technological innovation in France. ³⁹ Since 2018, a series of laws have provided ARCOM with regulatory powers over digital platforms (see B3). ⁴⁰

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. However, some Russian state-owned websites, which were originally blocked in March 2022, remained inaccessible during the coverage period. In June 2022, a new EU sanctions package led to additional blocking of Russian websites. All major social media platforms are accessible, but some, such as Rumble, preferred to close their services in France rather than ban Russian media. ⁴¹

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." ⁴² Soon afterward, ARCOM confirmed in a press release that it was complying with the EU decision. ⁴³

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. ⁴⁴ In July 2022, RT France appealed the EU blocking decision to the Court of Justice of the EU (CJEU), ⁴⁵ but the court upheld the suspension later that month. ⁴⁶

French lawmakers have advanced a bill on "protecting and regulating the digital space," which would grant ARCOM new powers to block pornographic websites

that do not verify the age of their users (see C4). ⁴⁷ As of June 2023, the draft law was still under discussion by Parliament.

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. ⁴⁸ Both sites were still blocked during the coverage period.

Since a deadly series of terrorist attacks struck Paris in 2015, terrorism-related content and incitement to hatred have been subject to blocking. 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. ⁴⁹ As of August 2023, the website was accessible at a different URL hosted in the United States. ⁵⁰

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 abuse images. ⁵¹ Shortly after the decree was promulgated, five websites were blocked, with no judicial or public oversight, for containing terrorism-related information. ⁵² France's data protection agency, the National Commission for Information Technology and Civil Liberties (CNIL), reported in May 2022 that the Central Office for the Fight against Crime related to Information and Communication Technology (OCLCTIC), a police body, had issued 439 blocking orders to ISPs in 2021, a 16 percent decrease compared with 2020. ⁵³

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 French 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 Digital Services Act came into force in November 2022. 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. In addition, very large online platforms (VLOPs), which were designated in February 2023, are required to evaluate the larger societal risks their systems pose, 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. ⁵⁴ 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). ⁵⁵ The platforms must delete illegal content about which they have been notified.

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. ⁵⁶ In August 2022, France's Constitutional Council dismissed a challenge from members of Parliament to a bill adapting French law to this regulation. ⁵⁷ The legislation gave ARCOM the authority to issue an injunction to platforms for the removal of terrorist content. The French nongovernmental organization (NGO) La Quadrature du Net criticized the measure, arguing that it posed a risk of excessive censorship. ⁵⁸

According to Google's transparency report, the government issued 291 requests to remove content between July and December 2022, invoking privacy and security or copyright violations in a majority of the cases. ⁵⁹ Between January and June 2022, Facebook restricted access to 250 pieces of content, including material from Russian state-controlled media outlets and items that were reported for spreading electoral propaganda, at the request of French authorities.

60

A government decree issued in 2015 allows for the deletion or deindexing of online content related to child abuse and terrorism, at the request of the OCLCTIC and using an administrative procedure, previously supervised by the CNIL. ⁶¹ In June 2022, this oversight responsibility was transferred to ARCOM (see A5). ⁶² According to its 2022 report, between January and December 2022 the OCLCTIC issued 82,754 removal requests targeting such content, as well as

2,951 deindexing requests. ⁶³ Content was deleted in response to 73,685 of the removal requests; of those, 61,135 were related to child abuse and 11,950 were related to terrorism. ⁶⁴

The right to be forgotten (RTBF) was recognized in a 2014 ruling from the CJEU, ⁶⁵ and it was later institutionalized throughout Europe with the implementation of the General Data Protection Regulation (GDPR) in 2018. ⁶⁶ In recent years, companies like Google and Microsoft have deindexed thousands of URLs in France under the RTBF. ⁶⁷

In March 2022, far-right presidential candidate Éric Zemmour was found guilty of copyright infringement by the Paris Judicial Court for his unauthorized use of content in a campaign video. ⁶⁸ YouTube removed the video from its platform due to these concerns. ⁶⁹

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 content removal requests. 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. ⁷⁰ 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. ⁷¹

In August 2021, the Guaranteeing the Respect of Republican Principles Law (see C2), often referred to as the antiseparatism law, was enacted. ⁷² In addition to placing broad constraints on religious freedom, especially with respect to Islam, the law enables an administrative authority to block mirror websites—specifically websites that contain “substantially the same” content as another that was already ruled illegal—without separate review from a magistrate. ⁷³ The law also anticipated some of the notice-and-action procedures included in the EU’s Digital Services Act, ⁷⁴ 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 (\$20.7 million). **75**

The antiseparatism law resembles an earlier measure on hate speech, known as the Avia law, which was largely voided by the Constitutional Council in June 2020 after being adopted by Parliament that May. **76** Unlike the nullified components of the Avia law, the Guaranteeing the Respect of Republican Principles Law does not compel platforms to remove “illegal content” within 24 hours. **77** 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.” **78**

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). **79**

In 2018, Parliament passed a law that aims to combat disinformation surrounding elections by empowering judges to order the removal of “fake news” within three months of an election. **80** 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. **81** There was no significant application of this law during recent elections. **82** In July 2022, ARCOM published the annual reports that platforms are required to complete under the law. The reports from Twitter and Meta were criticized for providing vague answers about the type and scope of false information that was removed. **83**

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. ⁸⁴ In August 2022, Parliament passed legislation that adapted French law to European 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.

During the coverage period, Parliament discussed the draft Protecting and Regulating the Digital Space Law. The bill would address a broad range of threats to French users, with provisions aimed at banishing cyberbullies from social networks and filtering content that links to financial scams. ⁸⁵

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. ⁸⁶ 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). ⁸⁷ Under this decree, the OCLCTIC submits requests to search engines, which then have 48 hours to comply. ⁸⁸ 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 oversight of internet users, which could encourage self-censorship (see B2 and B3). Articles 36 and 38 of the Guaranteeing the Respect of Republican Principles 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), ⁸⁹ which could also foster self-censorship.

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 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. ⁹⁰

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 the Russian invasion of Ukraine. Similarly, during the height of the COVID-19 pandemic, false reports and misinformation about the virus spread online, ⁹¹ as did conspiracy theories propagated by far-right and extremist political parties. ⁹²

In the run-up to the April 2022 presidential election, various groups tried to cast doubt on the validity of the election process or polls. ⁹³ A report from the EU DisinfoLab found 169 “debunks” based on reports by fact-checking organizations, but concluded that none “reached a magnitude that could have altered the integrity of the voting process or jeopardized its outcome.” The report also found that there was no significant foreign interference in the election. ⁹⁴

A September 2022 Meta report noted that a Russian influence operation used “false media sites” mimicking those of prominent publications in the EU, including the French publication *20 Minutes*, to target Facebook users in France and elsewhere in the union with pro-Kremlin propaganda. The pages spread Russian government narratives about a potential energy crisis in Europe and denied evidence of war crimes committed by the Russian military in Ukraine. Ultimately, however, the propaganda network had little influence among the targeted audiences. ⁹⁵

In 2020, Facebook reported that it had detected a network of fake accounts linked to the French military that posed as residents of Francophone countries in Africa. The accounts spread messages in French and Arabic that aligned with France's regional policies. ⁹⁶ French officials “raised doubt” about the report of

coordinated inauthentic behavior, though the government did not directly deny the findings. ⁹⁷

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 to 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). ⁹⁸ Some commentators have criticized ARCOM's mandate as overly broad. ⁹⁹

Two laws adopted in 2009 were designed to combat online copyright infringement. ¹⁰⁰ 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. ¹⁰¹

In May 2021, the government enacted legislation that increased HADOPI's power by implementing the EU Copyright Directive (see B3). ¹⁰² The law includes an ad hoc liability system for platforms hosting copyrighted content. ¹⁰³

In June 2023, after the coverage period, Parliament adopted the Regulating Commercial Influence and Preventing Abuse from Influencers on Social Networks Law. 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. ¹⁰⁴

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. ¹⁰⁵

In July 2021, France's Competition Authority fined Google €500 million (\$518 million) for failing to negotiate licensing fees "in good faith" with French news outlets, which it had been mandated to do in April 2020. ¹⁰⁶ Google announced that it would appeal the ruling in September 2021, ¹⁰⁷ but the company dropped the appeal in June 2022. ¹⁰⁸

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). ¹⁰⁹

In 2021, the Senate, one of the two chambers of Parliament, opened an inquiry to examine the state of media ownership concentration, ¹¹⁰ forming a commission that summoned owners of prominent media outlets for questioning. The Senate commission noted that the number of media organizations had diminished by 5.5 percent between 2015 and 2019, and that the number of regional media organizations in particular had decreased by 8.9 percent. ¹¹¹

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 outlet Brut. ¹¹²

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 no restrictions on digital mobilization in France. The state and other actors do not block online organizing tools and collaboration websites.

Several digital rights and advocacy groups, such as La Quadrature du Net, are active and play a significant role in protesting the government's recent moves to expand censorship and surveillance measures without judicial oversight. ¹¹³

During the coverage period, a number of large-scale strikes and demonstrations were held in France to oppose government-backed pension reforms and to protest police violence after a teenager was shot and killed by an officer. Participants used social media to mobilize demonstrations across the country. ¹¹⁴

The COVID-19 pandemic temporarily changed the landscape of activism in France. Various strike movements were diminished by legislative and administrative restrictions related to the pandemic. A few protests moved online, including a May 2020 action to demand improved rights for workers. ¹¹⁵

In November 2020, an estimated 500,000 people gathered to protest Article 24 of the Global Security Bill, which would have criminalized posting images of on-duty police officers online and was ultimately voided by the Constitutional Council (see C2 and B4). ¹¹⁶

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 expressly protects press freedom and access to information, and it guarantees freedom of speech and the rights of journalists. ¹¹⁷

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.” ¹¹⁸ 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. **119**

A counterterrorism law that came into effect in 2017 has raised concerns among civil rights campaigners for giving 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). **120**

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 Digital Services Act, and some provisions have already been adopted as part of the Guaranteeing the Respect of Republican Principles Law (see C2 and B3). This 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 these 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 (\$104,000) 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 (\$77,700) fine. **121**

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.

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 (\$46,600) fine, but in cases involving the personal information of public officials, the perpetrators face up to five years in prison and a €75,000 (\$77,700) 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. ¹²³

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?

5/6

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

In March 2023, a woman was arrested for insulting President Macron in a social media post. She faced a possible fine of €12,000 (\$12,400). 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. ¹²⁴ The woman had not stood trial as of June 2023.

In 2020, a court convicted an elected member of the Brittany regional legislature, who had previously been expelled from the far-right National Front (now National Rally) party, of sympathizing with terrorist acts; she had posted an Islamophobic message on Twitter following a white supremacist's mass-shooting attack on two mosques in Christchurch, New Zealand. The regional legislator received a suspended one-year prison sentence and was ruled ineligible to run in elections for three years. ¹²⁵

In January 2022, presidential candidate Éric Zemmour was found guilty of hate speech after he described unaccompanied migrant children as "thieves," "rapists," and "murderers." ¹²⁶ In May 2021, National Rally leader Marine Le Pen was

acquitted of violating hate-speech laws by sharing images on Twitter of Islamic State (IS) terrorists beheading a journalist. ¹²⁷

A growing number of individuals, including minors, ¹²⁸ have been investigated and given fines and prison sentences for “glorifying” terrorism. ¹²⁹ 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 IS and claiming that terrorist attacks in France had been “reprisals” for French attacks abroad. ¹³⁰

Penalties for threatening state officials are applied to online activities. In 2019, a man was fined €500 (\$520) for sending President Macron a death threat on Facebook. ¹³¹ In 2017, a court sentenced a 42-year-old man to three months in jail for a Twitter post that threatened National Assembly member Éric Ciotti. ¹³²

C4 0-4 pts

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

Users are not prohibited from using encryption services to protect their communications, though mobile users must provide identification when purchasing a SIM card, potentially reducing anonymity for mobile communications. ¹³³

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. ¹³⁴ 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. ¹³⁵

Also in 2020, following the terrorist murder of schoolteacher Samuel Paty, a group of politicians argued that online anonymity should be restricted (see B4). ¹³⁶ These debates continued during the coverage period. In March 2023, the National Assembly advanced a bill that would require minors to verify their age online. The proposal raised concerns about the ability of government agencies to identify internet users. ¹³⁷ The legislation was passed in June 2023, after the coverage period. ¹³⁸

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

2/6

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

The 2015 Intelligence Law allows intelligence agencies to conduct electronic surveillance without a court order. ¹³⁹ 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. ¹⁴⁰

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 sent to or received from abroad was adopted later in the year. ¹⁴¹ 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. ¹⁴²

In July 2023, after the coverage period, French lawmakers advanced amendments to a justice reform bill that would allow police officers to activate geolocation tracking as well as camera and microphone access on suspects’ mobile phones and other devices. While these surveillance tactics would only be permitted for criminal suspects facing at least five years in prison, rights groups have criticized the decision as an infringement on fundamental security and privacy rights. ¹⁴³

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. ¹⁴⁴ 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. ¹⁴⁵ Under the law, the government is also allowed to use an increasing number of algorithms to identify individuals who have visited extremist

websites. ¹⁴⁶ Though the law was passed quickly, it received strong criticism from civil society groups and academics. ¹⁴⁷

Following an October 2020 CJEU decision confirming the ban on indiscriminate metadata collection and retention, ¹⁴⁸ the French government asked the Council of State to ignore the four EU rulings on that issue, asserting France's national sovereignty. ¹⁴⁹ 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). ¹⁵⁰ In the new counterterrorism law, this regime was modified, according to the government, to respond to some of the Council of State's concerns. The NGO La Quadrature du Net argued that this modification was insufficient to protect individuals' right to privacy. ¹⁵¹

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. ¹⁵² 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. ¹⁵³

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. ¹⁵⁴ Although the CJEU ruled against this practice, in April 2021 the Council of State determined that the retention rules were justified (see C5). ¹⁵⁵

The 2015 Intelligence Law requires ISPs to install so-called "black boxes," algorithms that analyze users' metadata for "suspicious" behavior in real time. ¹⁵⁶ The first black box was deployed in 2017, ¹⁵⁷ and two more were added in 2018.

158 In 2022, a reported 20,958 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. This represented a 9.5 percent decrease from 2021. **159**

The French data protection authority continued to regularly enforce 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 2022, the CNIL fined Microsoft €60 million (\$62 million) for making it difficult for website visitors to refuse cookies. At the same time, the CNIL fined Apple €8 million (\$8.3 million) for its treatment of personal data on the Apple Store. **160** The CNIL has fined other companies, including Carrefour, Google, and Amazon, in previous coverage periods for similar data-related offenses. **161**

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?	3/5
--	------------

Violence against journalists, including online journalists, has increased in recent years. **162**

Members of the media have faced physical violence while covering protests. 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 (see B8). **163** In January 2022, two Agence France-Presse (AFP) journalists and their security guards were attacked during a protest against COVID-19-related public health measures that was organized by The Patriots, a right-wing political party. One of the protesters identified the AFP journalists, leading others to attack a videographer until security personnel intervened. **164**

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. **165**

Online harassment of LGBT+ people remains a problem. In January 2019, two associations defending LGBT+ rights filed 213 complaints related to insults,

incitements to hatred, and calls to murder LGBT+ users on social networks. **166**

Also in 2019, a group of journalists were accused of online harassment against women, obese people, and LGBT+ people. Though the journalists carried out harassment campaigns primarily on Twitter, they coordinated their activities in a private Facebook group called the “League of LOL.” **167**

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.

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. **168**

Medical institutions, including hospitals, routinely face ransomware attacks and breaches of patients’ personal data. **169** In March 2022, l’Assurance Maladie, the country’s main insurance body, declared that data for more than half a million people had been stolen. Hackers illegally accessed the accounts of 19 pharmacists and other health care professionals, allowing them to obtain users’ personal data, including social security numbers. In March 2020, Assistance Publique–Hôpitaux de Paris (APHP), which manages 39 hospitals in and around the capital, experienced a DDoS attack, leading the hospital network to shut down its internet access for a day. **170**

Various other businesses and institutions also face hacking attempts. In June 2020, the public broadcaster France Télévisions experienced a malware attack, though it had no effect on broadcasting. **171**

During the 2017 presidential campaign, Macron’s campaign team announced that it was the “victim of a massive and coordinated hacking attack” in which thousands of leaked emails and documents were dumped on the internet in a last-minute effort to destabilize the race. **172** US and British authorities attributed the attack to Russian state-backed hackers, and a *Le Monde* investigation found that US-based far-right groups were involved in disseminating the leaked material, **173**

Footnotes

- 1** DataReportal, “Digital 2023: France,” February 9, 2023, <https://datareportal.com/reports/digital-2023-france>.
- 2** Organisation for Economic Co-operation and Development, “Broadband Portal - Historical penetration rates, fixed and mobile broadband,” accessed on March 21, 2020, <https://www.oecd.org/sti/broadband/broadband-statistics/>.
- 3** French Digital Agency “Plan France Très Haut Débit [French Very High-Speed Plan],” accessed September 30, 2020, <https://www.aménagement-numérique.gouv.fr/>.
- 4** Regulatory Authority for Electronic Communications and Post (ARCEP), “Observatoire haut et très haut débit : abonnements et déploiements [High and very high speed observatory: subscriptions and deployments],” 4th quarter, 2022, <https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/obser...>
- 5** ARCEP, “Qualité des services mobiles 2022,” October 2022, <https://www.arcep.fr/actualites/actualites-et-communiques/detail/n/qual...>

More footnotes



On France

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

See More >

Country Facts

Global Freedom Score

89/100 Free

Internet Freedom Score

76/100 Free

Freedom in the World Status

Free

Networks Restricted

No

Social Media Blocked

No

Websites Blocked

Yes

Pro-government Commentators

No

Users Arrested

Yes

In Other Reports

Freedom in the World 2023

Other Years

2022

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

Subscribe

Join the Freedom House weekly
newsletter

ADDRESS

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

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org

@2023 FreedomHouse