

France

C Violations of User Rights

Laws to address threats to national security have bolstered the state's surveillance powers and introduced stricter measures to tackle terrorist propaganda online. A new amendment to the Military Planning Law increased the state's surveillance capabilities. The COVID-19 pandemic and corresponding national lockdown raised the specter of the monitoring of confined and sick people without their consent. The telecommunications provider Orange provided anonymized aggregate subscriber data to the French government and the French government decided to create a centralized app for COVID-19 contact-tracing, enabling them more control at the cost of citizens' privacy.

C1 1.00-6.00 pts0-6 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?	4.004 6.006
--	----------------

The French constitution reinforces press freedom and access to information, and guarantees freedom of speech and the protection of journalists.[103](#)

However, the government's response to the 2015 terror attacks have curtailed human rights online in practice. The European Convention on Human Rights, to which France is a signatory, provides for freedom of expression, subject to certain restrictions considered "necessary in a democratic society."[104](#) Since the *Charlie Hebdo* attack and November 2015 terrorist attacks in Paris, the government has suggested on a number of occasions that limiting fundamental rights would serve public safety.[105](#)

Broad new powers under the state of emergency proclaimed in 2015 raised concerns among human rights and digital rights activists.[106](#) While then prime minister Manuel Valls declared that it was a "short term response,"[107](#) the state of emergency was subsequently extended six times until November 2017.[108](#) The new counterterrorism law that came into effect in 2017 has also raised concerns among civil rights campaigners for giving prefects and security forces wide-ranging powers with limited judicial oversight. It also introduced a new legal framework for surveillance of wireless communications (see C5).[109](#)

C2 1.00-4.00 pts0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	2.002 4.004
---	-------------

There are a number of laws that assign criminal or civil penalties for potentially legitimate online activities. In particular, the myriad counterterrorism laws threaten to punish users for such activities. Measures to address terrorism were already in place prior to the 2015–17 state of emergency. The counterterrorism law passed in 2014 penalizes online speech deemed to sympathize with terrorist groups or acts with up to seven years in prison and a €100,000 (\$110,000) fine. Speech that incites terrorism is also penalized. Penalties for online offenses are harsher than offline offenses, which are punishable by up to five years in prison and a €75,000 (\$83,000) fine.[110](#)

Another counterterrorism and organized crime law enacted in 2016 imposes up to two years in prison or a €30,000 (\$33,000) fine for frequently visiting sites that glorify or incite terrorist acts, unless these visits are in “good faith,” such as conducting research.[111](#) The Constitutional Council rejected this law in 2017, arguing that the notion of “good faith” was unclear and that the law was not “necessary, appropriate, and proportionate.”[112](#) An amended version was reintroduced as part of a public security law—imposing prison sentences on users who also “manifest adherence” to the ideology expressed at the visited sites[113](#)—but was once again struck down by the Constitutional Court in December 2017.[114](#) While at least one member of Parliament contemplated reintroducing the law during the coverage period, the government has opposed this effort.[115](#)

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 handicap,” prison time.[116](#)

C3 1.00-6.00 pts0-6 pts

Are individuals penalized for online activities?	5.005 6.006
--	-------------

While no citizens faced politically motivated arrests or prosecutions in retaliation for online activities, users have been convicted of inciting or sympathizing with terrorism online. The broad terms “inciting” and “glorifying” terrorism risk targeting speech that has tenuous connections to terrorist acts.

In February 2020, a court convicted an elected member of the Brittany regional legislature of sympathizing with terrorist acts. The official, who had previously been expelled from the far-right National Front party, posted an Islamophobic message on Twitter following the attacks by a far-right activist in Christchurch, New Zealand against two mosques. She was sentenced to one year’s suspended sentence and three years of ineligibility to contest elections.[117](#)

In June 2019, a 21-year-old woman was handed a six-month suspended prison sentence for possessing, but not sharing, videos and pictures glorifying terrorism. Following an electronic search, the police found 82 incriminating videos, along with 735 pictures. She was also accused of being in contact with the Islamic State (IS) militant group through social networks.[118](#)

In June 2019, Marine Le Pen, leader of the far-right National Rally party, was ordered to stand trial by a correctional court for sharing videos of IS terrorists beheading a journalist on Twitter. The trial was postponed to February 2021.[119](#)

Penalties for threatening state officials are applied to online activities. In May 2019, a man was fined €500 (\$550) for sending President Macron a death threat on Facebook.[120](#)

C4 1.00-4.00 pts0-4 pts

Does the government place restrictions on anonymous communication or encryption?	2.002 4.004
--	-------------

Users are not prohibited from using encryption services to protect their communications, although mobile users must provide identification when purchasing a SIM card, potentially reducing anonymity for mobile communications.[121](#) There are no laws requiring providers of encryption services to install backdoors, but providers are required to turn over decryption keys to the government.[122](#) In June 2019, a drug dealer who was using encryption services refused to unlock his phone during his arrest and was also charged for this refusal. A court later ruled that the suspect was not required to unlock his phone in the absence of a court order, setting a legal precedent.[123](#)

Anonymous communication using tools such as Tor is not prohibited.

C5 1.00-6.00 pts0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	2.002 6.006
---	-------------

Surveillance has escalated in recent years, including through the enactment of a new surveillance law in 2015, which was passed in the wake of the attack on *Charlie Hebdo* that year.

The 2015 Intelligence Law allows intelligence agencies to conduct electronic surveillance without a court order.[124](#) An amendment passed in 2016 authorized real-time collection of metadata not only from individuals “identified as a terrorist threat,” but also those “likely to be related” to a terrorist threat and those who belong to the “entourage” of the individuals concerned.[125](#)

The Constitutional Council declared three of the 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 2015, shortly after the Paris attacks, for the purposes of “defending and promoting the fundamental interests of the country.”[126](#) In 2016, the Constitutional Council struck down part of the Intelligence Law related to the monitoring of hertz wave communications, ruling it “disproportionate.”[127](#) Article 15 of the new counterterrorism law of 2017 reintroduced a legal regime for monitoring wireless communications, but limits surveillance to certain devices such as walkie-talkies

and does not encompass Wi-Fi networks.[128](#)

The COVID-19 pandemic and the ensuing national lockdown raised the specter of the monitoring of confined and sick people without their consent. In March 2020, Orange shared statistics on mobile users' travels out of the Paris region area in response to a government request, and the telecommunications industry invited legislation to regulate such data-sharing (see C6).[129](#)

In April 2020, the government announced the development of a Bluetooth contact-tracing app that deploys pseudonymized identifiers and relies on centralized data storage.[130](#) The release of the app, named StopCovid, was originally intended to coincide with the deconfinement measures of May 11, but was released on June 2, after only one month of development.[131](#) The CNIL released opinions on the principles of the app on April 26[132](#) and May 26,[133](#) ultimately noting that its concerns had been addressed and approving the release of the app. On May 27, the National Assembly and Senate voted to approve the deployment of the app.[134](#) Critics in civil society and Parliament raised concerns about anonymity, the effectiveness of the tool, the potential for discriminatory effects, but also basic interoperability issues (as of June 2020, the French app lacked any form of interoperability with neighboring countries).[135](#) As of June 2020, only 2.8 percent of French citizens downloaded the app.

The state of emergency imposed from 2015 and 2017 included provisions on electronic searches[136](#) and empowered the minister of the interior to take “any measure to ensure the interruption of any online public communication service that incites the commission of terrorist acts or glorifies them.”[137](#)

In 2019, an amendment that was passed as part of a routine military spending bill (the Military Planning Law, or LPM) extended the state's surveillance capabilities. To be implemented from 2019 to 2025, the amendment expands 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.[138](#) According to Article 37 of the new LPM, it will be possible to “perform within the intercepted connection data spot checks for the sole purpose of detecting a threat to the fundamental interests of the nation, linked to subscription numbers or technical identifiers attributable to French territory and geographical areas.”[139](#) Digital rights groups have criticized this expansion of surveillance that previously only affected French citizens living abroad.[140](#)

The LPM covering 2014 to 2019 extended administrative access to user data by enabling designated officials to request such data from ISPs for “national security” reasons, to protect France's “scientific and economical potential,” and to prevent “terrorism” or “criminality.”[141](#) The office of the prime minister authorizes surveillance, and the National Commission for Security Interception (CNCIS, later renamed the National Intelligence Control Commission, or CNCTR) must be informed within 48 hours in order to approve it.[142](#) Early critics pointed out that the CNCIS lacked appropriate control mechanisms and independence from potential political interference, given that the body was comprised of only three politicians in 2014.[143](#) While the government argued that the law provided an improved legal framework for practices that had been in place for years,[144](#) it finally replied to these criticisms at the end of 2015 by enlarging its composition from three members to nine, making room for judges.[145](#)

A law related to the fight against organized crime and terrorism, enacted in 2016, also elicited strong reactions from the public.¹⁴⁶ The law notably expanded the range of special investigation methods available to prosecutors and investigating judges, which were previously reserved for intelligence services. These include bugging private locations, using phone eavesdropping devices such as international mobile subscriber identity (IMSI) catchers, and conducting nighttime searches.¹⁴⁷ Relatedly, Article 23 of the Law on Guidelines and Programming for the Performance of Internal Security (LOPPSI 2), adopted in 2011, granted the police with the authority to install malware—such as keystroke logging software and Trojan horses—on suspects’ computers in the course of counterterrorism investigations, although a court order must first be obtained.¹⁴⁸

The Digital Republic Act adopted in 2016 seeks to enhance individuals’ rights to control the use of their personal data. Companies will face hefty fines if they fail to comply; with the GDPR coming into force in 2018, the CNIL will be able to fine a company up to 4 percent of its total worldwide annual turnover for any data protection violations.¹⁴⁹

C6 1.00-6.00 pts 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	3.003 6.006
--	----------------

Service providers are required to aid the government in monitoring their users’ communications under certain circumstances. For instance, they must retain user metadata for use in criminal investigations.¹⁵⁰ The 2015 Intelligence Law requires ISPs to install so-called “black boxes,” algorithms that analyze users’ metadata for “suspicious” behavior in real time.¹⁵¹ The first black box was set in 2017.¹⁵² Intelligence services released data on the use of three black boxes in 2018, and two additional black boxes were added during the coverage period.¹⁵³ Related to this increase in surveillance capabilities, 10,562 “security interceptions” were undertaken in 2018—an increase of 20 percent from 2017. Real-time geolocation tracking in the context of individual surveillance for national security purposes increased by 38.4 percent (from 3,751 to 5,191). The number of individuals subject to this surveillance only slightly increased (from 21,386 to 22,038).¹⁵⁴

In March 2020, Orange shared public statistics on mobile users’ travels out of the Paris region area in response to a government request, to aid contact-tracing efforts of people with symptoms of COVID-19.¹⁵⁵ The telecommunications industry then invited the government to adopt legislation in case that more advanced measures were needed. The government created a consultation committee in March 2020 to assess the use of geolocation data as part of the surveillance of the spread of the COVID-19 pandemic,¹⁵⁶ raising concern among activists that there will be mapping of every patient or confined person without their consent.¹⁵⁷

In June 2019, the Ministry of the Interior proposed a new intelligence law in order to extend the use of black boxes, with the aim of improving automation, prolonging data collection, and taking into account new technologies such as 5G networks.¹⁵⁸

Despite these surveillance efforts, the data protections enshrined in the GDPR are strongly enforced in France. In

January 2019, the CNIL fined Google a record €50 million (\$55 million) for violating the regulation.[159](#)

C7 1.00-5.00 pts0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	4.004 5.005
---	----------------

There were no reported physical attacks against journalists or ordinary users during the coverage period. However, there were several high-profile cases of online harassment.

In February 2020, Benjamin Griveaux, a candidate running for mayor of Paris, stepped down from the race after a video of him engaging in a sex act, self-recorded for a lover who was not his spouse, was leaked online.[160](#)

In February 2019, a group of mostly male journalists were accused of online harassment against women, obese people, and LGBT+ people. Though they carried out harassment campaigns primarily on Twitter, they coordinated their activities in a private Facebook group called the “League of LOL.”[161](#)

In April 2019, journalists from the investigative online outlet Disclose were summoned to the General Directorate for Internal Security (DGSI), France’s domestic intelligence agency, after publishing confidential documents about the export of weapons later used by Saudi Arabia and the United Arab Emirates (UAE) in the war in Yemen.[162](#)

Online harassment of LGBT+ people increased during the coverage period. The NGO called SOS Homophobia highlighted in its 2020 report an increase of anti-LGBT+ content on social networks, from 383 cases reported in 2018, to 596 in 2019.[163](#) 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.[164](#) Also in January 2019, YouTuber and LGBT+ advocate Bilal Hassani filed a lawsuit asserting that he was the victim of a large-scale cyberbullying campaign.[165](#)

C8 1.00-3.00 pts0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	2.002 3.003
---	----------------

Several government-affiliated websites experienced cyberattacks during the coverage period, and businesses routinely experience hacking attempts.

During the COVID-19 crisis in March 2020, l’Assistance publique-Hôpitaux de Paris, which manages 39 hospitals in Paris and the surrounding region, experienced a distributed denial-of-service (DDoS) attack, leading the hospital network to close temporarily its internet access for a day. [166](#)

In June 2019, the government's tax collection website went down on the last day for fiscal declarations. The National Cybersecurity Agency (ANSSI) is investigating the case and suspects that the attack originated from abroad.¹⁶⁷ It was also reported that 2,000 fiscal declarations were altered by hackers.¹⁶⁸

In June 2020, after the coverage period, the national French Television group experienced a malware attack, though it had no effect on broadcasting.¹⁶⁹

According to the Global State of Information Security Survey 2018, French business losses related to cyberattacks grew by 50 percent in 2017, with companies losing an average of €2 million (\$2.2 million). More than 4,550 cybersecurity incidents were recorded by French companies in one year.¹⁷⁰ Companies and institutions also frequently experience ransomware attacks, which are sometimes targeted attacks where cybercriminals manually intrude the network and encrypt data; the petroleum company Picoty SA suffered such an attack in May 2019.¹⁷¹ There are also automated viruses using ransomware from the black market, which are injected via phishing schemes. A public hospital's network was affected in this manner in May 2019.¹⁷²

During the 2017 presidential campaign, Macron's campaign team announced that they were the "victim of a massive and coordinated hacking attack" after thousands of leaked emails and documents were dumped on the internet in a last minute effort to destabilize the race.¹⁷³ Macron had previously confirmed being the target of phishing operations by a group of hackers and denounced the "interference."¹⁷⁴ Later, an investigation by *Le Monde* indicated that these cyberattacks were directed by a US-based neo-Nazi group.¹⁷⁵ Observers noted that there was no real police investigation into the leaks.¹⁷⁶ Indeed, after Macron was elected, the government did not follow up on the investigation of the origins of this cyberattack.