

# France

	2016	2017		
<b>Internet Freedom Status</b>	Free	Free	Population:	66.9 million
Obstacles to Access (0-25)	3	3	Internet Penetration 2016 (ITU):	85.6 percent
Limits on Content (0-35)	6	7	Social Media/ICT Apps Blocked:	No
Violations of User Rights (0-40)	16	16	Political/Social Content Blocked:	No
<b>TOTAL* (0-100)</b>	<b>25</b>	<b>26</b>	Bloggers/ICT Users Arrested:	No
			Press Freedom 2017 Status:	Free

\* 0=most free, 100=least free

## Key Developments: June 2016 – May 2017

- Concerns about the impact of disinformation and political bot operations heightened in the run-up to the 2017 French presidential election, as leaked communications related to candidate Emmanuel Macron were dumped online and amplified by automated accounts in attempts to destabilize the race right before campaigning closed (see "**Limits on Content**").
- The number of requests to take down or block pro-terrorism content increased significantly during the coverage period. While some of the decisions were disputed, no cases of "over-blocking" were reported (see "**Limits on Content**").
- In February 2017, France's Constitutional Council struck down a new provision that criminalized the act of frequently visiting websites encouraging terrorism through the use of images of terrorist acts. Shortly after however, an amended version was reintroduced, imposing prison sentences on users who also "manifest adherence" to the ideology expressed on the site (see "**Violations of User Rights**").
- The Digital Republic Act adopted in October 2016 introduced new provisions to regulate the digital economy, including net neutrality and data protections. The law notably enables the French Data Protection Authority to impose heftier administrative fines for data protection violations (see "**Legal Environment**").

## Introduction

France's internet freedom environment declined slightly during a tense presidential election year, as the online sphere experienced a surge in disinformation and leaks aiming to destabilize the presidential race.

The past year was marked by a dramatic election campaign that resulted in the victory of centrist candidate Emmanuel Macron over far-right leader Marine Le Pen. The campaign was dominated by heightened concerns regarding the potential abuse of social media to deceive and manipulate public opinion. Although the surge in "fake news" and political bot operations did not ultimately manage to sway the result of the French election, the proliferation of disinformation and leaks seeking to disrupt the process raised alarm. Just hours before campaigning closed ahead of the runoff on May 7, 2017, thousands of leaked e-mails and documents from Emmanuel Macron's campaign team were dumped on the internet in a last minute effort to destabilize the race.

Measures to address terrorist threats have also continued to impact France's internet freedom environment by expanding surveillance powers and limiting judicial oversight. Following a string of deadly terrorist attacks, a series of legislative changes to address threats to national security have sought to boost government surveillance powers and introduce stricter measures to tackle terrorist content online. Under the law prolonging the state of emergency following the deadly terrorist attack in Nice on July 14, 2016, an amendment authorized real-time collection of metadata of individuals not only "identified as a terrorist threat," but also those "likely to be related" to a terrorist threat, or those who belong to the "entourage" of the person concerned. In October 2016, the Constitutional Council declared unconstitutional a section regarding surveillance of wireless communications in the Intelligence Law passed in July 2015, finding it disproportionate and in violation of the right to privacy and confidentiality of communications.

Since November 2015, France's State of Emergency has been repeatedly extended for two years. These emergency measures significantly expanded authorities' powers, such as allowing house arrests and searches without judicial oversight. In this context, United Nations human rights experts raised concerns about "excessive and disproportionate restrictions on fundamental freedoms" in France, including "the lack of clarity and precision of several provisions of the state of emergency and surveillance laws."<sup>1</sup> In June 2017, newly-elected President Macron announced plans for a new counter-terrorism law, which would seek to transfer some critical provisions of the state of emergency into permanent law.<sup>2</sup>

## Obstacles to Access

*France's internet penetration continued to increase, although regional disparities persist. The current ICT market is open, highly competitive, and has benefited from the privatization of the state-owned company France Telecom.*

---

<sup>1</sup> OHCHR, "UN rights experts urge France to protect fundamental freedoms while countering terrorism," January 19, 2016, <http://bit.ly/20e9Jkh>

<sup>2</sup> On November 1, 2017, France officially lifted the state of emergency, and introduced a new anti-terror law. "Anti-terrorism: the Government wants the state of emergency to be the common law", Le Monde, June 7, 2017, <http://lemde.fr/2sSf31D>

## Availability and Ease of Access

Key Access Indicators		
Internet penetration (ITU) <sup>a</sup>	2016	85.6%
	2015	84.7%
	2011	77.8%
Mobile penetration (ITU) <sup>b</sup>	2016	103%
	2015	103%
	2011	94%
Average connection speeds (Akamai) <sup>c</sup>	2017(Q1)	10.8 Mbps
	2016(Q1)	9.9 Mbps

<sup>a</sup> International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2016," <http://bit.ly/1cblxxY>.

<sup>b</sup> International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2016," <http://bit.ly/1cblxxY>.

<sup>c</sup> Akamai, "State of the Internet - Connectivity Report, Q1 2017," <https://goo.gl/TQH7L7>.

Committed to providing widespread access to high-speed broadband, the French government has been implementing an ambitious national plan to deploy high-speed broadband throughout France by 2022, mobilizing public and private investments totalling 20 billion euros (US\$22 billion) over 10 years.<sup>3</sup> As of December 2016, this plan benefited 50 percent of the population.<sup>4</sup>

Reforms approved in 2015, known as the "Loi Macron," have sought to improve mobile broadband coverage in the country, requiring telecom operators to deploy 2G network in underserved municipalities by 2016, and ensure 3G/4G coverage by 2017.<sup>5</sup> Despite some improvement however, high-speed LTE coverage in rural areas remained below the EU average.<sup>6</sup>

Demographic disparities in internet usage persist: for example, mobile penetration ranged from 67.7 percent in the Paris area to 47.5 percent in urban areas with less than 50,000 inhabitants.<sup>7</sup> A map produced by regulator Arcep illustrates some of the regional disparities in mobile penetration, showing patchy coverage of 4G networks in rural areas.<sup>8</sup> Most at-home users have access to broadband connections, while the remaining households are connected either through dial-up or satellite services, usually due to their rural location.<sup>9</sup>

## Restrictions on Connectivity

There were no restrictions on connectivity reported during the coverage period. There is no central internet backbone, and ISPs are not required to lease bandwidth from a monopoly holder. Instead, the backbone consists of several interconnected networks run by ISPs and shared through peering

3 "Plan France Très Haut Débit," official website, accessed September 22, 2016, <http://www.francethd.fr>

4 "Le Plan France Très Haut Débit," gouvernement.fr, May 15, 2017, <http://bit.ly/21kmjzc>

5 "French government approves amendment mandating rural mobile expansion," TeleGeography, April 20, 2015, <http://bit.ly/2yuEqdf>

6 European Commission, "Broadband Coverage in Europe 2016," <https://ec.europa.eu/digital-single-market/en/news/study-broadband-coverage-europe-2016>

7 Statista, "Mobile internet usage penetration in France from 2010 to 2015, by urban area size," March 21, 2013, <http://bit.ly/2eku0Fs>

8 See website: <https://www.monreseau-mobile.fr/>

9 Ariase, "L'ADSL et la fibre optique en France," <http://bit.ly/2eHNZft>

or transit agreements. There are also a number of Internet Exchange Points (IXPs) in France,<sup>10</sup> which contribute to improved access and lower consumer prices.<sup>11</sup>

## ICT Market

There are no significant business hurdles to providing access to digital technologies in France. The main ISPs are Orange, Free, Bouygues Telecom, and Numericable-SFR (SFR was a division of Vivendi that was sold to Numericable).<sup>12</sup> Others such as NRJ Mobile, Virgin Mobile, Cofidis Mobile, and Darty make use of the main ISPs' networks, reselling the services.<sup>13</sup>

In July 2017,<sup>14</sup> regulator ARCEP announced it would impose certain constraints on market leader Orange in an effort to open up competition for high-speed fiber services among small and medium-sized companies.<sup>15</sup>

## Regulatory Bodies

The telecommunications industry in France is regulated by the Regulatory Authority for Electronic and Postal Communication (ARCEP),<sup>16</sup> while competition is regulated by France's Competition Authority and, more broadly, by the European Commission (EC).<sup>17</sup> The commissioner of ARCEP is appointed by the government, but as an EU Member State, France must ensure the independence of its national telecommunications regulator. Given that the French state is the main shareholder in Orange, the country's leading telecom company, the EC stated that it would closely monitor the situation in France to ensure that European regulations were being met.<sup>18</sup> ARCEP remains an independent and impartial body and decisions made by the regulator are usually seen as fair.

The Digital Republic Act enacted in October 2016 broadened ARCEP's investigatory powers, notably granting ARCEP with investigatory and sanctioning powers to ensure compliance with the principle of net neutrality introduced by the law.<sup>19</sup>

## Limits on Content

*Following a string of deadly terrorist attacks in France, much attention has focused on mechanisms to counter pro-terrorist content online, resulting in an uptick of removal and blocking requests. Meanwhile, concerns surrounding disinformation and political bot operations heightened in the run-up to the 2017 French presidential election.*

---

10 Internet Exchange Points, Data Centre Map, <http://bit.ly/2dzlzY4>

11 "Internet Service Providers and Peering v3.0," DrPeering International, <http://bit.ly/1joJCaC>

12 Ruth Bender, "Vivendi Accepts Altice Offer to Buy 20% Numericable-SFR Stake," *Wall Street Journal*, February 27, 2015, <http://on.wsj.com/2f5YxrP>

13 Jerome Tranie, «Fastest ISPs 2014: France," *PC Mag*, June 19, 2014, <http://bit.ly/2eulzHk>

14 This announcement was made outside the coverage period of this report.

15 "French telecoms regulator to impose new constraints on Orange," Reuters, July 11, 2017, <https://www.reuters.com/article/france-telecoms/update-2-french-telecoms-regulator-to-impose-new-constraints-on-orange-idUSL8N1K20KC>

16 ARCEP, "Autorité de Régulation des Communications Électroniques et des Postes," <http://bit.ly/1RImAXo>

17 "Autorité de la concurrence," <http://bit.ly/1frpn7J>

18 "ARCEP must remain independent vis-a-vis government – EC," *Telecompaper*, January 14, 2011, <http://bit.ly/1k5gzJe>

19 ARCEP, "The Digital Republic Act strengthens Arcep's powers, opens the way for new forms of regulation and tasks the Authority with protecting net neutrality," Press Release, October 10, 2016, <http://bit.ly/2zsuULM>

## Blocking and Filtering

France does not generally engage in any politically-motivated blocking of websites. YouTube, Facebook, Twitter and international blog-hosting services as a whole are freely available. However, since the *Charlie Hebdo* and November 2015 attacks in Paris, the government has released statements suggesting that limiting fundamental rights of citizens would serve public safety,<sup>20</sup> and terrorist-related content has been subject to censorship.

A decree issued in February 2015 outlined administrative measures to block websites containing materials that incite or condone terrorism, as well as sites that display child pornography.<sup>21</sup> The decree implemented article 6-1 of the Law on Confidence in the Digital Economy (LCEN), passed in 2004, as well as article 12 of new antiterrorism law passed in November 2014.<sup>22</sup> The administrative authority, in this case the Central Office for the Fight against Crime related to Information and Communication Technology (OCLCTIC), is in charge of creating a blacklist of sites containing infringing materials, and must review the list every four months to ensure that blacklisted sites continue to contravene French law. OCLCTIC can request editors or hosts to remove the content, and after a 24 hour period it can request ISPs to block the site.<sup>23</sup> Users trying to access those pages are redirected to a website from the Ministry of Interior indicating why the site was blocked and avenues for appeal. Shortly after the decree was announced, five websites were blocked with no judicial or public oversight under suspicion of containing terrorism-related information.<sup>24</sup>

A chief concern related to blocking remains the lack of judicial oversight in the blocking of websites that incite or promote terrorist acts. The procedure is supervised by the National Commission on Informatics and Liberty (CNIL), the data protection agency. As an administrative authority, CNIL can also refer requests to the administrative court should they be unhappy with any action taken by the OCLCTIC. Some commentators have lamented that while CNIL was founded to protect internet freedoms, it is now overseeing the restriction of those same rights.<sup>25</sup>

The Paris attacks in November 2015 and the terrorist attack in Nice in July 2016 significantly impacted the number of overall requests to censor content linked to terrorism (see "Content Removal"). According to CNIL's activity report covering the period between March 2016 and February 2017, French authorities made 874 requests to block sites, compared to 312 during the previous period (some of them were made available again after the removal of infringing content). Administrative blocking requests for terrorist content targeted 165 sites, compared to 709 sites displaying child abuse.<sup>26</sup>

This mechanism does not report the detailed content of websites blocked, but it does report censorship decisions disputed by CNIL. In one case in February 2017, the OCLCTIC requested the removal of a video related to the July 2016 Nice terrorist attack, accompanied by the text "Nice

---

20 "Valls : La sécurité est la première des libertés," *La Depeche*, January 7, 2016, <http://bit.ly/2eydvoA>

21 Decree 2015-125 of February 5, 2015, <http://bit.ly/2cqSoRr>

22 "L'impossible et controversé blocage des sites Internet djihadistes," *Le Monde*, September 13, 2014, <http://bit.ly/2dfofWV>

23 The blocking order can be issued immediately if the editor does not provide information stipulated under article 6-III of LCEN. See: Article 12, Law 2014-1353 of November 13, 2014, <http://bit.ly/2eeaTwZ>

24 Lucie Ronfaut, "La France bloque pour la première fois des sites Web de propagande terroriste" [France blocks terrorist propaganda websites for the first time], *Le Figaro*, March 16, 2015, <http://bit.ly/2eAyTsT>

25 EDRI, "France implements Internet censorship without judicial oversight," March 11, 2015, accessed February 12, 2016 <http://bit.ly/1CasJYJ>

26 Alexandre Linden, "Rapport d'activité de la personne qualifiée" [Activity Report], March 2016 – February 2017, CNIL, accessed October 1, 2017, <http://bit.ly/2eAO4Ch>

Attack July 14, 2016 live video of truck.” Following the removal request, access was blocked. CNIL considered that the text was neutral and judged the blocking order disproportionate.<sup>27</sup>

One isolated case of “over-blocking” was reported during this coverage period, but was mainly due to a technical incident: for 3 hours on October 17, 2016, Orange blocked the traffic to Google, Wikipedia and several websites for its 11 million landline customers, due to a wrong update to its DNS servers.<sup>28</sup>

Under the extended state of emergency legislation first adopted in November 2015, the interior minister was given the power to block websites and social media, taking “any measure to ensure the interruption of any public communication service online that glorifies or incites acts of terrorism.”<sup>29</sup> Although the National Commission on Informatics and Liberty (CNIL) noted in its April 2016 report that the “implementation methods of this measure have not been specified, and to date, the Minister of Interior has not resorted to it.”<sup>30</sup>

## Content Removal

French authorities are fairly transparent about what content is prohibited and the reasons behind specific content removal requests. Incitement of hatred, racism, Holocaust denial, child pornography, copyright infringement, and defamation are illegal. Article R645-1 of the French criminal code outlaws the display of the emblems, uniforms, or badges of criminal organizations, under penalty of a fine.<sup>31</sup>

As stipulated in the 2014 anti-terrorism law, the administrative authority (OCLCTIC) can request editors and hosts to remove content that incites or apologizes for terrorism, as well as sites that display child abuse; after a 24 hour period it can request ISPs to block the site (see Blocking and Filtering).<sup>32</sup>

A government decree issued on March 4, 2015 also allows for the delisting of online content from search results using a similar administrative procedure supervised by CNIL.<sup>33</sup> Under this decree, OCLCTIC submits requests to search engines, which then have 48 hours to comply. The OCLCTIC is responsible for reevaluating de-indexed websites every four months, and requesting the relisting of websites where the incriminating content has been removed. According to CNIL’s report, between March 2016 and February 2017, French authorities submitted 2,077 de-indexing requests for content related to child abuse and terrorism (compared to 855 the previous year), as well as 2,561 removal requests (compared to 1,439 last year). Content was removed in 2,305 cases, 1,975 of

---

27 Alexandre Linden, “Rapport d’activité de la personne qualifiée” [Activity Report], March 2016 – February 2017, CNIL, accessed October 1, 2017, <http://bit.ly/2eAO4Ch>

28 Alix Guillard, “Main French Internet provider Orange blocks traffic to Google”, cz.nic, October 27, 2016, <https://en.blog.nic.cz/2016/10/27/french-orange-blocks-traffic-to-google/>

29 Law 2015-1501 of November 20, 2015, <http://bit.ly/1qraiKQ>

See also: Daniel Severson, “France’s Extended State of Emergency: What New Powers Did the Government Get?” *Lawfare*, November 22, 2015, <http://bit.ly/1OYBpSl>; Glynn Moody, “French state of emergency allows website blocking, device search powers,” *Ars Technica*, November 20, 2015, <http://bit.ly/1XeWkfl>

30 Alexandre Linden, “Rapport d’activité de la personne qualifiée” [Activity Report], March 2015 – February 2016, CNIL, accessed September 1, 2016, <http://bit.ly/2eAO4Ch>

31 Elissa A. Okoniewski, “Yahoo!, Inc. v. Licra: The French Challenge to Free Expression on the Internet,” *American University International Law Review* 18, 1, 2002, <http://bit.ly/1LOzaFS>

32 See Article 12, Law 2014-1353 of November 13, 2014, <http://bit.ly/2eeaTwZ>

33 The decree implements modifications to the 2004 LCE that were made under the 2011 LOPPSI 2 and the 2014 antiterrorism law. See: Decree 2015-253 of March 4, 2015, <http://bit.ly/2ctwhi3>

which concerned pro-terrorist content. CNIL disputed a handful of these removal and de-indexing requests.<sup>34</sup>

The anti-piracy law HADOPI, originally passed in June 2009<sup>35</sup> and supplemented by a second law in October 2009<sup>36</sup> was once again in the news in 2016. In a surprise move, parliament adopted a proposal in April 2016 to suppress HADOPI by February 2022,<sup>37</sup> but the Senate voted to reverse this move.<sup>38</sup> HADOPI functions by responding to copyright infringers with a graduated response, starting with an email warning for the first offense, followed by a registered letter if a second offence occurs within six months. If a third offence occurs within a year of the registered letter, the case can be referred to the court, and the offender may receive a fine as a possible sanction.<sup>39</sup> In June 2016, HADOPI published a report showcasing increased activity: it filed more than 688 referrals to court in the last year, more than twice than in the last five years (362 from 2010 to 2015). Most fines ranged from 50 to 1,000 euros.<sup>40</sup>

Legal debates over the right to be forgotten have also escalated in recent years. In June 2015, the French data protection agency CNIL ordered Google to extend the “right to be forgotten” ruling across all of its sites that can be accessed within the country, including Google.com and not just Google.fr.<sup>41</sup> Google raised concerns that the move would set a dangerous precedent for authoritarian governments, who could also request that Google apply national laws extraterritorially.<sup>42</sup> An informal appeal by Google was rejected in September 2015, and CNIL threatened to take action against Google with fines of approximately EUR 300,000 should they refuse to comply.<sup>43</sup> In early February 2016, Google announced that it would comply by removing certain search results across all EU domains.<sup>44</sup> In March 2016, Google was fined \$112,000 by the CNIL for not complying with demands to remove results across its global domains.<sup>45</sup> Google appealed to France’s Council of State, which in July 2017 decided to refer the matter to the Court of Justice of the European Union (ECJ).<sup>46</sup>

A ruling in early February 2016 by a Paris court established that Facebook could be sued in France for removing the account of a French user who posted an image of a 19th century painting of a naked woman by Gustave Courbet. A French court will now be entitled to hear the case, brought by the account’s Parisian user. Facebook had argued that cases concerning their terms and conditions

---

34 Alexandre Linden, “Rapport d’activité de la personne qualifiée” [Activity Report], March 2016 – February 2017, CNIL, accessed October 1, 2017, <http://bit.ly/2eAO4Ch>

35 Law 2009-669 of June 12, 2009, <http://bit.ly/2dAON3J>

36 Law 2009-1311 of October 28, 2009, <http://bit.ly/2eAOvw7>

37 Amaelle Guiton, “La fin d’Hadopi, une agonie politique” [The end of Hadopi, a political agony], *Libération*, April 30, 2016, <http://bit.ly/1SUW2np>

38 Elsa Trujillo, “Les sénateurs sauvent la Hadopi de la disparition,” [Senators vote to save Hadopi from disappearance], *Le Figaro*, May 26, 2016, <http://bit.ly/1RxskAH>

39 Guillaume Champeau, “HADOPI: An FAQ to learn all,” *Numerama*, February 10, 2016, <http://bit.ly/2dRVwdH>

40 HADOPI, “annual report”, June 2016, <https://hadopi.fr/sites/default/files/ChiffresRGJuin16.pdf>

41 CNIL, “Right to delisting: Google informal appeal rejected,” September 21, 2015, <http://bit.ly/1NGpDz2>

42 Peter Fleischer, “Implementing a European, not global, right to be forgotten,” Google Europe Blog, July 30, 2015, <http://bit.ly/2dgeyHK>

43 Samuel Gibbs, “French data regulator rejects Google’s right-to-be-forgotten appeal,” *The Guardian*, September 21, 2015, <http://bit.ly/1Kvr6nf>

44 Danielle Correa, “‘Right to be forgotten’ extended to all Google domains in EU,” *SC Magazine UK*, February 12, 2016, <http://bit.ly/2dzFTbB>

45 Mark Scott, “Google fined by French privacy regulator,” *New York Times*, March 24, 2016, [https://www.nytimes.com/2016/03/25/technology/google-fined-by-french-privacy-regulator.html?\\_r=0](https://www.nytimes.com/2016/03/25/technology/google-fined-by-french-privacy-regulator.html?_r=0)

46 “French court refers ‘right to be forgotten’ dispute to top EU court,” Reuters, July 19, 2017, <https://www.reuters.com/article/us-google-litigation/french-court-refers-right-to-be-forgotten-dispute-to-top-eu-court-idUSKBN1A41AS>

could only be heard by a Santa Clara, CA court, where its headquarters are based. This was dismissed by a Paris appeals court, which ruled that should the case involve a French user, it can be heard in France. The decision can be appealed to France's highest court.<sup>47</sup>

## Media, Diversity, and Content Manipulation

France is home to a highly diverse online media environment. Self-censorship online is minimal, and there were no reports of the French government proactively manipulating content online. However, concerns about disinformation and political bot operations heightened in the run-up to the 2017 French presidential election, and a trove of leaked documents sought to destabilize candidate Emmanuel Macron.

During the last months of the presidential election in April-May 2017, social media users were deluged with fake news stories.<sup>48,49</sup> In April, Facebook said that it had suspended 30,000 automated spam accounts in France, including many profiles that were distributing politically driven disinformation.<sup>50</sup> While all presidential candidates were attacked, a large number of fake news reports were created and promoted by far-right online communities, promoting Marine Le Pen and attempting to undermine other candidates such as Emmanuel Macron.<sup>51</sup> One study found that in April nearly one in five links shared on social media were from sources contesting the legitimacy of traditional media, and that some of these disruptive narratives emerged as "fake news."<sup>52</sup>

On May 5, 2017, confidential documents from the campaign of Emmanuel Macron were leaked on the internet. The election commission warned media outlets to respect the campaign blackout period and not to comment on the leaks before election day, noting that some of the data appeared to be mixed with "false information."<sup>53</sup> Moreover, a study looking at tweets between the end of April and election day found that many automated accounts used in the context of #MacronLeaks had been created shortly prior to the 2016 U.S. presidential election, pointing to a "black market" of reusable political bots.<sup>54</sup>

In February 2017, the National Assembly adopted a bill to criminalize websites spreading disinformation about abortion. For instance, some websites on the "voluntary interruption of pregnancy" and dedicated to "inform future mother on abortion and offer neutral and medical

---

47 "Court says Facebook nude painting case can be tried in France," Reuters, February 12, 2016, <http://reut.rs/1PKGzCL>

48 Marie Mawad, "French Election Is Facebook's Fake News Litmus Test", April 27, 2017, <https://www.bloomberg.com/news/articles/2017-04-27/france-is-facebook-s-fake-news-litmus-test-as-elections-near-end>

49 Reuters, "Experts say automated accounts sharing fake news ahead of French election", April 21, 2017, <http://www.reuters.com/article/us-france-election-socialmedia-idUSKBN17M31G>

50 "Facebook cracks down on 30,000 fake accounts in France," Reuters, April 13, 2017, <http://www.reuters.com/article/us-france-security-facebook/facebook-cracks-down-on-30000-fake-accounts-in-france-idUSKBN17F25G>

51 Clavel and Herreros, "The journey of a fake news promoted by Marine LePen and aiming at Emmanuel Macron", Huffington Post, May 4, 2017, [http://www.huffingtonpost.fr/2017/05/04/voici-litineraire-de-la-fake-news-que-propage-marine-le-pen-sur\\_a\\_22068793/](http://www.huffingtonpost.fr/2017/05/04/voici-litineraire-de-la-fake-news-que-propage-marine-le-pen-sur_a_22068793/)

52 Bamako, "Patterns of Disinformation in the 2017 French Presidential Election," <https://static1.squarespace.com/static/58495e3329687f8bfbb3f25c/t/590904cb15cf7da7dc3b15d8/1493763322834/Patterns+of+Disinformation+in+the+2017+French+Presidential+Election+-+Report+2+-+Bakamo.pdf>

53 Commission nationale de contrôle de la campagne électorale, "Suites de l'attaque informatique qu'a subie l'équipe de campagne de M. Macron," Press Release, May 6, 2017, <http://www.cnccpe.fr/communiqués/cp15.html>

54 Emilio Ferrara, "Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election," First Monday, 22(8), 2017, <http://www.emilio.ferrara.name/2017/07/06/macronleaks-bots-and-the-2017-french-election/>

information” were in fact websites managed by anti-abortion activists.<sup>55</sup>

## Digital Activism

French digital rights and advocacy groups, such as La Quadrature du Net (LQDN), are very active in the country, playing a significant role in protesting the government’s recent moves to expand surveillance and blocking measures without judicial oversight.<sup>56</sup> In the past, LQDN successfully lobbied the European Parliament for an amendment to the European Union Telecoms Package to ensure that no restrictions on internet access could be imposed without prior judicial approval.<sup>57</sup>

In late 2015, users were able to share comments and interact via an online consultation platform designed to increase citizen engagement around the Digital Republic Bill that was finally adopted in October 2016, collecting 8,500 online contributions and almost 150,000 votes.<sup>58</sup>

## Violations of User Rights

*New laws to address threats to national security have bolstered the state’s surveillance powers and introduced stricter measures to tackle terrorist propaganda online. The prolonged state of emergency initiated after the Paris terrorist attacks in November 2015 has significantly expanded the powers of authorities to conduct house arrests, raids, and searches and seizures of devices, without judicial oversight.*

## Legal Environment

In accordance with the 1789 Declaration of the Rights of Man,<sup>59</sup> France’s constitution guarantees freedom of speech.<sup>60</sup> The European Convention on Human Rights, of which France is a signatory, provides for freedom of expression, subject to certain restrictions which are “necessary in a democratic society.”<sup>61</sup>

Since November 2015, broad new powers under the state of emergency have raised concerns among human rights and digital activists.<sup>62</sup> While then Prime Minister Manuel Valls declared on

---

55 Cécile Chambraud, Gaëlle Dupont “Debate on adoption”, *Le Monde*, November 29, 2016, [http://www.lemonde.fr/societe/article/2016/11/29/le-debat-sur-l-avortement-se-crispe\\_5040087\\_3224.html](http://www.lemonde.fr/societe/article/2016/11/29/le-debat-sur-l-avortement-se-crispe_5040087_3224.html); Le délit d’entrave à l’IVG définitivement adopté par le Parlement,” *Le Monde*, February 16, 2017, [http://www.lemonde.fr/societe/article/2017/02/16/le-delit-d-entrave-a-l-ivg-definitivement-adopte-par-le-parlement\\_5080652\\_3224.html#fGiWif4C5b5qSPhR.99](http://www.lemonde.fr/societe/article/2017/02/16/le-delit-d-entrave-a-l-ivg-definitivement-adopte-par-le-parlement_5080652_3224.html#fGiWif4C5b5qSPhR.99)

56 La Quadrature du Net, “Who are we?” accessed February 15, 2016, <http://bit.ly/2dzGBpm>

57 Danny O’Brien, “Blogging ACTA across the globe: the view from France,” Electronic Frontier Foundation, January 2010, accessed February 15, 2016, <http://bit.ly/2eXcb1u>

58 “Loi République numérique : Consultation terminée, près de 148 000 votes,” *Le Monde Informatique*, October 19 2015, <http://www.lemondeinformatique.fr/actualites/lire-loi-republique-numerique-consultation-terminee-pres-de-148-000-votes-62704.html>

59 “The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law.” See: Declaration of the Rights of Man 1789, September 1, 2016, <http://bit.ly/1AgkDwp>

60 Guy Carcassonne, “The Principles of the French Constitution,” published on the website of the Embassy of France in Washington, DC, November 28, 2007, <http://bit.ly/1X4r11P>

61 European Court of Human Rights, European Convention on Human Rights, accessed September 1, 2016, <http://bit.ly/1foTq0D>

62 “Human Rights Watch, “France: New Emergency Powers Threaten Rights,” November 24, 2016, <http://bit.ly/1P8yL1Q>

November 19 that it was a “short term response,”<sup>63</sup> the state of emergency was subsequently extended at least five times through July 2017.<sup>64</sup> The state of emergency includes provisions on electronic searches (see “Surveillance, Privacy, and Anonymity”).<sup>65</sup> The state of emergency also empowered the interior minister to take “any measure to ensure the interruption of any online public communication service that incites the commission of terrorist acts or glorifies them.”<sup>66</sup>

Measures to address terrorism were already in place prior to the November 2015 state of emergency. The antiterrorism law passed in November 2014 penalizes online speech deemed as “apology for terrorism” (apologie du terrorisme) with up to seven years in prison and a EUR 100,000 (US\$100,000) fine. Online penalties are harsher than offline, which is subject to five years in prison and a EUR 75,000 fine.<sup>67</sup> Another law adopted by parliament in May 2016 and enacted in June 2016 “on the fight against terrorism and organized crime” also provides sentences of up to two years in prison or a EUR 30,000 fine for frequently visiting sites that glorify or incite terrorist acts, unless these consultations are done in “good faith,” such as journalistic or research activities (see also “Surveillance, Privacy, and Anonymity”).<sup>68</sup>

France’s Constitutional Council finally rejected this last law in February 2017, arguing that the notion of “good faith” was unclear, and that the law was not “necessary, appropriate and proportionate.”<sup>69</sup> Shortly after however, 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 on the site.<sup>70</sup>

In a positive step, following a process of public consultation, the National Assembly adopted a “Digital Republic” bill in January 2016, covering a wide range of issues such as access to public data, safeguards for net neutrality, and the protection of personal data. The law was enacted in October 2017 with a final vote from the Senate.<sup>71</sup>

## Prosecutions and Detentions for Online Activities

No citizens faced politically motivated arrests or prosecutions, but multiple users have been

---

63 “Discours de Manuel VALLS, Premier ministre, Projet de loi sur la prorogation de l’état d’urgence, Assemblée nationale” [Speech by Manuel Valls, Prime Minister: bill on the extension of the state of emergency, National Assembly], gouvernement.fr, November 19, 2015, <http://bit.ly/2duhrJ>

64 See: Declaration of the State of Emergency, November 14, 2015; First extension of three months, Law 2016-162, February 19, 2016; Second extension of two months, Law 2016-629, May 20, 2016; Third extension of six months, Law 2016-987, July 21, 2016.

65 La Quadrature du Net, “A Police State to Avoid any Critical Evaluation?” November 19, 2015 <http://bit.ly/1kNOJlk>; See also: Glynn Moody, “French state of emergency allows website blocking, device search powers,” *Ars Technica*, November 20, 2015, <http://bit.ly/1XeWKf1>

66 Law 2015-1501 of November 20, 2015, Article 11, <http://bit.ly/2evb2MQ>

67 Law 2014-1353 of November 13, 2014, <http://bit.ly/1T1dzwE>

68 Law 2016-731 of June 3, 2016, <http://bit.ly/2cS1zAO>

69 EBLnews, “French ban on habitual viewing of jihadist websites struck down”, February 10, 2017, <https://eblnews.com/news/europe/french-ban-habitual-viewing-jihadist-websites-struck-down-55633>

70 “Le nouveau délit de consultation de sites terroristes : six questions, six réponses,” NextImpact, March 1, 2017, <https://www.nextinpact.com/news/103497-le-nouveau-delit-consultation-sites-terroristes-six-questions-six-reponses.htm>

71 Law 2016-1321 of October 7, 2016, <http://bit.ly/2eAVW6D>

sentenced for glorifying terrorism online.<sup>72</sup> According to the figures from the Ministry of Justice, at least thirty-nine cases involved frequent visits to terrorist sites, after a new law passed in June 2016 criminalized the act of frequently consulting sites that glorify or incite terrorist acts (see “Legal Environment”). Twelve of these reported cases resulted in convictions.<sup>73</sup>

## Surveillance, Privacy, and Anonymity

Surveillance has escalated in recent years, not least with the enactment of a new surveillance law in July 2015, which was passed in the wake of the attacks on *Charlie Hebdo* by armed extremists earlier that year.

The *Loi Relatif au Renseignement*, or Intelligence Law,<sup>74</sup> allowed for intelligence agencies to conduct electronic surveillance without a court order and required ISPs to install so-called “black boxes,” algorithms that analyze users’ metadata for “suspicious” behavior in real time.<sup>75</sup> In July 2016, an amendment authorized real-time collection of metadata of individuals not only “identified as a terrorist threat,” but also those “likely to be related” to a terrorist threat, or those who belong to the “entourage” of the person concerned.<sup>76</sup>

The French Constitutional Council had declared three of the law’s provisions unconstitutional in July 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 later adopted on November 30, 2015, shortly after the Paris attacks on November 13, for the purposes of “defending and promoting the fundamental interests of the country.”<sup>77</sup> In October 21, 2016, the Constitutional Council censored part of the Intelligence Law related to the monitoring of Hertz wave communications after qualifying it as “disproportionate.”<sup>78</sup>

Under the state of emergency established in November 2015, the authorities were granted powers to access and copy user data, with little judicial oversight and without clarifying safeguards concerning the use of this data.<sup>79</sup> The constitutional council struck down the provision allowing the authorities to copy user data in February 2016, citing the lack of judicial oversight.<sup>80</sup> A new version of

---

72 See for example: “A Nice, une Franco-Tunisienne condamnée à trois ans de prison pour apologie du terrorisme,” [Franco-Tunisian woman sentenced to three years in prison in Nice for apology of terrorism] *Le Monde*, 18 June, 2016, <http://bit.ly/2elhRbJ>; Une peine record à Montpellier pour un homme accusé d’apologie du terrorisme sur internet [Record sentence in Montpellier for man accused of apology of terrorism online], *France 3 Languedoc-Roussillon*, August 31, 2016, <http://bit.ly/2dAXv24>

73 “Consultation de sites terroristes : douze condamnations, et plusieurs questions,” *Le Monde*, February 16, 2017, [http://www.lemonde.fr/pixels/article/2017/02/16/consultation-de-sites-terroristes-douze-condamnations-et-plusieurs-questions\\_5080855\\_4408996.html#oBOrmcW589t5y969.99](http://www.lemonde.fr/pixels/article/2017/02/16/consultation-de-sites-terroristes-douze-condamnations-et-plusieurs-questions_5080855_4408996.html#oBOrmcW589t5y969.99)

74 Law 2015-912 of July 24, 2015, <http://bit.ly/1SMCPq3>

75 Angélique Chrisafis, “France passes new surveillance law in wake of Charlie Hebdo attack,” *The Guardian*, May 5, 2015, <http://bit.ly/1Qj1XAK>

76 Prorogation de l’état d’urgence, July 20, 2016, [http://www.senat.fr/amendements/commissions/2015-2016/803/Amdt\\_COM-15.html](http://www.senat.fr/amendements/commissions/2015-2016/803/Amdt_COM-15.html)

77 Law 2015-1556 of November 30, 2015, <http://bit.ly/2eWT2N1>

78 France Info, [http://www.francetvinfo.fr/politique/loi-sur-le-renseignement/loi-renseignement-un-article-sur-la-surveillance-des-communications-hertziennes-censure\\_1882987.html](http://www.francetvinfo.fr/politique/loi-sur-le-renseignement/loi-renseignement-un-article-sur-la-surveillance-des-communications-hertziennes-censure_1882987.html)

79 La Quadrature du Net, “A Police State to Avoid any Critical Evaluation?” November 19, 2015, <http://bit.ly/1kNOJlk>; See also: Glynn Moody, “French state of emergency allows website blocking, device search powers,” *Ars Technica*, November 20, 2015, <http://bit.ly/1XeWKf1>

80 Jean-Baptiste Jacquin, “Etat d’urgence : le Conseil constitutionnel censure les saisies informatiques lors des perquisitions” [State of emergency : Constitutional Council censors IT seizures during searches], *Le Monde*, February 19, 2016, <http://bit.ly/2eB8z1u>

this provision was reintroduced in July 2016 however, adding certain judicial guarantees.<sup>81</sup>

A new law related to the fight against organized crime and terrorism, adopted by parliament in May 2016 and enacted in June 2016, has also elicited strong reactions from the public.<sup>82</sup> The law notably expands special investigation methods to prosecutors and investigating judges, which were previously reserved for intelligence services. This includes bugging private locations, using phone eavesdropping devices such as IMSI catchers, and night-time searches.<sup>83</sup> These “new techniques” were used as part of investigations during this period of coverage, in particular to prevent an attack targeting Disneyland Paris Park. Five Islamic State militants were arrested on November 20, 2016 in relation to this planned terrorist attack.<sup>84</sup>

Other recent regulations on electronic surveillance were passed in December 2013 and came into force in January 2015, as part of a routine military spending bill (the Military Programming Law, or LPM). Article 20 of the LPM significantly expanded electronic surveillance of French residents and businesses by requiring ISPs to hand over data such as phone conversations, emails, internet activity, personal location data, and other electronic communication data to public authorities. The powers relate to the General Directorate for Internal Security (DCRI), three intelligence agencies under the Ministry of Defense, as well as anti-money-laundering and customs agencies. Under the law, these agencies can conduct surveillance without prior court approval for purposes of “national security,” the protection of France’s “scientific and economical potential,” and the prevention of “terrorism” or “criminality.”<sup>85</sup> The office of the prime minister authorizes surveillance and the National Commission for Security Interception (*Commission nationale de contrôle des interceptions de sécurité*, CNCIS) must be informed within 48 hours in order to ensure its approval.<sup>86</sup> Critics have pointed out that the CNCIS lacks appropriate control mechanisms and independence from political interference, given that the CNCIS is composed of only three politicians.<sup>87</sup> On the other hand, the government argued that the law provides an improved legal framework for practices that have already been in place for years.<sup>88</sup>

Article 23 of LOPPSI 2, adopted in 2011, grants the police with the authority to install malware—such as keystroke logging software and Trojan horses—on a suspect’s computer in the course of counterterrorism investigations, although authorization must come from a court order.<sup>89</sup>

---

81 Alexandre Boudet, “La version 4 de l’état d’urgence est la plus musclée depuis novembre 2015” [Version 4 of the state of emergency : the most beefed up version since November 2015], *Huffington Post*, July 27, 2016, <http://huff.to/2e1B8Uz>

82 Law 2016-731 of June 3, 2016, <http://bit.ly/2c7knag>; See also : Jean-Baptiste Jacquin, “La France se dote de la loi antiterroriste la plus sévère d’Europe” [France gets the strictest antiterrorist law in Europe], *Le Monde*, May 12, 2016, <http://bit.ly/2eB2jqA>; Donald Hebert, “Ce qui fait polémique dans le projet de loi Urvoas contre le terrorisme” [What is generating controversy with the Urvoas bill against terrorism], *Nouvel Obs*, March 3, 2016, <http://bit.ly/2dB1uLL>

83 “No Government has done more to counter terrorism to date,” *gouvernement.fr*, July 17, 2016, <http://bit.ly/2eB98bw>; Laetitia Vally, “Lutte contre le terrorisme : les 3 nouveautés à ne pas manquer !” [Fight against terrorism: three novelties not to miss!], *Net-Iris*, June 13, 2016, <http://bit.ly/2evOIEA>

84 Noémie Bisserbe and Sam Schechner, “French Authorities Deploy New Surveillance Powers to Thwart Attack”, November 25, 2016, <https://www.wsj.com/articles/french-authorities-deploy-new-surveillance-powers-to-thwart-attack-1480083370>

85 Alexandre Enraygues, “France—New ‘Patriot Act’ imposes surveillance obligations,” *Linklaters*, January 31, 2014 <http://bit.ly/1LOD6X5>

86 Kim Willsher, “French officials can monitor Internet users in real time under new law,” *The Guardian*, December 11, 2013, <http://bit.ly/18mtHm0>

87 Guillaume Champeau, “La DGSI investi du pouvoir de surveiller les communications sur internet” [The DGSI granted surveillance powers over the internet], *Numerama*, May 2, 2014, <http://bit.ly/2extbqS>

88 Scott Sayare, “France broadens its surveillance power,” *The New York Times*, December 14, 2013, <http://nyti.ms/1MBpsFD>

89 Emilien Ercolani, “Loppsi : qui pourra installer les mouchards informatiques?” [Loppsi: Who could install spywares?], *L’informaticien*, November 7 2011, <http://bit.ly/1MBpDkh>

The Digital Republic Act adopted in October 2016 seeks to enhance individuals' rights to decide and control the use of their personal data. Companies will face hefty fines if they fail to comply: once the EU's General Data Protection Regulation comes into force in 2018, CNIL will be able to fine up to 4 percent of total worldwide annual turnover for any data protection violations.<sup>90</sup>

A French order in February 2016 from the European Data Protection Authority ruled that Facebook was not allowed to track non-users in France or transfer personal data to U.S. servers. Facebook tracks the online movements of its users via its tracking cookies and plugins on third party websites, even if they are logged out. As part of a wider European investigation, CNIL fined Facebook 150,000 euros (approximately US\$170,000) in May 2017.<sup>91</sup>

## Intimidation and Violence

While there were no reported physical attacks against bloggers or online journalists in France, outlets such as *Canard Enchaîné* and media site *Mediapart* reported receiving death threats in the lead-up to 2017 presidential elections.<sup>92</sup>

Under the state of emergency, human rights groups have documented abusive searches and house arrests based on suspected terrorist-related activity.<sup>93</sup> Regional media have reported on a number of raids and seizures specifically targeting suspects of online activism and propaganda.<sup>94</sup>

## Technical Attacks

Just hours before campaigning closed ahead of the presidential runoff on May 7, 2017, thousands of leaked e-mails and documents from Emmanuel Macron's campaign team were dumped on the internet in a last minute effort to destabilize the race (see Media, Diversity and Content Manipulation). According to a press release by Macron's team on May 5, the campaign was the "victim of a massive and coordinated hacking attack" and that "those circulating these documents add many false documents to sow doubt and misinformation."<sup>95</sup> The Macron campaign team had previously confirmed being the target of phishing operations by a group of hackers and denounced "interference."<sup>96</sup>

According to the Global State of Information Security Survey 2016, the number of recorded

---

90 LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique, <https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=14>

91 Rakesh Krishnan, "French Orders Facebook to Stop Tracking Non-Users or Face Fines," *The Hacker News*, February 9, 2016, <http://bit.ly/2dN6KPL>; "Facebook fined 150,000 euros by French data watchdog," Reuters, May 16, 2017, <http://uk.reuters.com/article/us-facebook-france/facebook-fined-150000-euros-by-french-data-watchdog-idUKKCN18C10C>

92 Jane Whyatt, "France: Petition demands reforms to media law after pre-election death threats," April 14, 2017, <https://ecpmf.eu/news/threats/france-petition-demands-reforms-to-media-law-after-pre-election-death-threats>

93 Human Rights Watch, "France: Abuses under State of Emergency," February 3, 2016, <http://bit.ly/1SZmwpH>; Amnesty International, "France: Upturned lives: The disproportionate impact of France's state of emergency," February 4, 2016, <http://bit.ly/1ZFUeJ>

94 See for example: "Perquisition à Hérouville : «Activisme et propagande sur Internet»" [Raid in Hérouville : Activism and propaganda on the internet], *Ouest-france.fr*, November 20, 2015, <http://bit.ly/2e1vAcm>

95 "Communiqué de presse - En Marche a été victime d'une action de piratage massive et coordonnée," En Marche! Press release, May 5, 2017, <https://en-marche.fr/articles/communiqués/communiqué-presse-piratage>

96 "Macron team confirms being targeted by cyber attacks," Reuters, April 26, 2017, <http://fr.reuters.com/article/topNews/idFRKBN17S150-OFRTIP>; Nicole Perlroth, "Russian Hackers Who Targeted Clinton Appear to Attack France's Macron," *New York Times*, April 24, 2017, <https://www.nytimes.com/2017/04/24/world/europe/macron-russian-hacking.html>

cyberattacks in France has grown by 51 percent in 2015 – which translates to approximately 21 attacks per day – compared to 38 percent globally.<sup>97</sup> In response, French cybersecurity budgets have increased by an average of 29 percent, compared to 24 percent globally, commensurate with the financial loss caused by the incidents (EUR 3.7 million on average per company).<sup>98</sup>

---

97 Philippe Trouchaud, "The Global State of Information Security, Survey 2016 - Turnaround and Transformation in cybersecurity," PriceWaterhouse Coopers France, October 2015, accessed February 16, 2016, <http://pwc.to/1NLowjA>

98 Elodie Gaillard, "Press Release in 2015," PriceWaterhouse Coopers France, October 15, 2015, <http://pwc.to/1Phurem>