# Colombia

## C Violations of User Rights

*During the coverage period, a journalist served a 10-day prison sentence for refusing to remove articles from his news site and personal website. Two investigations revealed that the military used both open-source and more sophisticated surveillance technology and monitored at least 130 people, including 30 journalists. Amid a legal environment that obliges service providers to collaborate with intelligence agencies and retain subscriber data for five years, the government authorized mobile providers to share users' personal data with public authorities responding to the COVID-19 pandemic. Several cyberattacks targeted news sites that reported on sensitive topics.*

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? | 3.003 6.006 |

Article 20 of the constitution guarantees freedom of information and expression and prohibits prior restraint. Article 73 further provides for the protection of "the liberty and professional independence" of "journalistic activity." Although there are no specific provisions protecting freedom of expression online, bloggers have the same liberties and protections as print or broadcast journalists.[83] The Constitutional Court confirmed the application of such protections to the internet in a 2012 ruling.[84]

Impunity for perpetrators of violence is a pervasive problem in Colombia's judicial system and represents a grave threat to freedom of expression, according to rights advocates.[85]

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 |

Colombia maintains criminal penalties for defamation. According to the Colombian penal code, individuals accused of insult can face up to six years in jail and a fine, while individuals accused of libel can face between fifteen months and four-and-a-half years in jail, also with possible fines.[86] Cases pertaining to online defamation have occasionally been brought before the court with varying outcomes.

The penal code includes a concerning provision regarding online publication or reproduction of insults. According to Article 222, "whoever publishes, reproduces, or repeats insult or libel" may also be subject to punishment. This article raises concerns as it leaves open the possibility for charges of indirect insult and libel. The penal code also establishes the use of "social mediums of communication or of other collective divulgence" as an aggravating circumstance that can increase the penalty for insult or libel.87 However, courts have not held intermediaries responsible for defamatory content created or shared by third parties.

Between 2018 and 2019, two bills, PL 60/18 (on strengthening citizens' security) and PL 74/18 (on combatting cybercrimes), which would establish worrisome restrictions for online expression, were presented and debated. The bills, which were later combined, aimed to prohibit the nonconsensual dissemination of sexual content. However, the proposal was criticized for being overly broad; it originally focused on "intimate" content, and makes no exceptions for other content that can be considered "sexual."88 The legislation was not yet approved as of June 2020.

Another bill proposed in 2019 would restrict online expression. PL 176/19, which aims to regulate social networks, seeks to prohibit citizens from publishing any type of data, information, files, photographs, or videos of another person without their express written consent, while prohibiting the creation of profiles "that do not represent a real person." It would apply, for example, to accounts for pets or for parody. It also seeks to prohibit the publication of insults, prohibit people from "overexposing" their own privacy, oblige them to be "discreet" in their publications, and prohibit users from disclosing "sensitive" personal information, such as financial information, contact details, or "sentimental information." In addition, users would be prohibited from accessing "inappropriate content," though how that content would be defined is not clear.89

Colombia has harsh penalties for copyright violations and lacks flexible fair use standards employed in many countries. In a prominent case, in 2014, student Diego Gómez was charged with violating copyright violations for uploading an academic thesis onto Scribd.90 Digital rights groups heavily criticized the decision to prosecute, especially when he did not claim to have authored the thesis and did not profit by sharing it.91 He was finally cleared of criminal charges in 2017.92

C3 1.00-6.00 pts0-6 pts

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

Prosecution, imprisonment, or detention for ICT activities is quite rare in Colombia, and writers, commentators, and bloggers are not systematically subject to imprisonment or fines for posting material on the internet.

However, in March 2020, journalist Edison Lucio Torres served a 10-day prison sentence in the Los Caracoles police station after being sentenced by a criminal court in the city of Cartagena; the court also handed down a $2,600 fine.93 The decision came after Torres did not comply with an order to remove articles from his news site Vox Populi, as well as his personal website. The articles centered on 2016 reports about a religious leader who allegedly used church donations for personal expenses; the subject and his wife subsequently filed a complaint in November 2019, resulting

in the removal order.94 The judicial process was criticized for numerous flaws.95

The case demonstrates a small but persistent trend in which, as the public debate is being adjudicated, imprisonment is demanded as a form of rectification. Similarly, in August 2018, Juvenal Bolívar, a journalist at news outlet *Corillos*, and Sofía Ortíz Delgado, a former staff member there, served a 10-day sentence that was arbitrarily imposed by a civil court in the city of Bucaramanga. The sentence was issued after Bolívar refused to comply with a ruling ordering him to withdraw an investigation into a city official from his website, after a process plagued by procedural irregularities.96

In June 2020, after the coverage period, three contributors to ab zurdo, a photography account on Instagram, were detained in Medellín while covering a demonstration against the government's COVID-19 response. They were fined for violating the city's lockdown.97

C4 1.00-4.00 pts0-4 pts

| | |
|---|---|
| Does the government place restrictions on anonymous communication or encryption? | 3.003 4.004 |

Colombia has no general restrictions against anonymous communication, and there are no registration requirements for bloggers or cybercafé owners, though users must register to obtain telecommunication services. Police have access to a database that must be maintained by telecommunication service providers. This database contains user data, such as name, identification number, place and residence address, mobile phone number, and service activation date.98 Users must provide accurate information under penalty of perjury, which is punishable by a minimum of six years in prison.99

In April 2017, the prosecutor general announced a proposal to force WhatsApp and other internet intermediaries to decrypt users' communications for law enforcement purposes.100 Even though the proposal was never enacted, the announcement raised concerns about the state's surveillance ambitions, as well as officials' lack of understanding regarding technology like encryption.101 (Providers that encrypt communications end-to-end cannot decrypt them.)

Since 1993, Colombian law has banned the use of "communication devices that use the electromagnetic spectrum" to send "encrypted messages or messages in unintelligible language."102 In response to an information request, the ICT ministry explained that those provisions apply only "to the content of the communications, not the encryption of the medium." Despite the ambiguous wording of the law, the ICT ministry further claimed that these provisions only apply to radio-like devices and not to the internet.103 The Intelligence and Counterintelligence Act stipulates that telecommunications service providers may only offer encrypted voice services to intelligence agencies and "high government" officials.104

C5 1.00-6.00 pts0-6 pts

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

Intercepting personal communications in Colombia is authorized only for criminal investigation purposes and legally requires a judicial order.105 Colombian law allows intelligence agencies to monitor devices that use the electromagnetic spectrum to transmit wireless communication without a judicial order.106

Episodes of extralegal surveillance carried out by intelligence agencies, the army, and the police have constituted an ongoing scandal in Colombia in recent years. Some steps have been taken to punish perpetrators of illegal surveillance, although it seems unlikely that these efforts have changed the overall environment, as intelligence agencies continue to operate with minimal oversight. Concerns about illegal surveillance by certain sectors of the government and military persist. Several Colombian civil society organizations have criticized the excessive and apparently uncontrolled use of surveillance tools in the country, which they argue has been facilitated by "weak legislation" on intelligence matters.107

In January 2020, the magazine *Semana* published an investigation revealing the military's use of open-source intelligence and sophisticated equipment. During 2019, technology provided by the United States to address drug trafficking and the fight against guerrillas was used to spy on politicians, magistrates, generals, social leaders, activists, and journalists. According to IFEX, files on each target included "excerpts of their conversations on social media and messaging apps, photographs, videos, network of contacts, and maps tracing their movements." Most of the information was obtained through open source. However, other technology, including International Mobile Subscriber Identity (IMSI) catcher equipment and a malware system called Invisible Man was also employed, as was the artificial intelligence tool Voyager, which was created by an Israeli company.108

*Semana* published the results of another investigation in May 2020, which noted that 130 people were targeted for surveillance, including 30 journalists from outlets including the *New York Times*, *Wall Street Journal*, *Semana*, and La Liga Contra El Silencio. The regional head of Human Rights Watch (HRW) was also surveilled.109 The *New York Times* identified journalist Nicholas Casey, who reported on Major General Nicacio Martínez Espinel's orders to increase the number of killed militants and criminals in May 2019, as a surveillance target.110 (Major General Martínez was relieved of his post that December.) Also targeted were social leaders and human rights defenders from the Inter-Ecclesial Commission for Justice and Peace.111

Ahead of the May 2020 report's publication, at least 11 army officials were fired and one resigned.112 While the military carried out an investigation,113 the general prosecutor's office opened its own, though no progress on that effort was publicized at the end of the coverage period.114

Data sharing, including through apps, has been initiated as part of Colombia's COVID-19 pandemic response (see C6), but concerns have been raised about the privacy rights of users and the effectiveness of the apps. Privacy International warned that the government's COVID-19 app, Coronapp, will not function without the user providing information including their name, sex, ethnicity, and email address, and provides no clarity on how that data will be used or protected. Coronapp notably asks users if they participated in mass protests within the last eight days.115

In 2015, documents leaked from the technology company Hacking Team, which is known to provide spyware to governments, suggested that the Colombian government had contracts with the company. Leaked emails referenced the National Police Office's (OPN) purchase of Hacking Team's Remote Control System (RCS) product, Galileo, which is capable of accessing and hijacking target devices' keyboards, microphones, and cameras. Police would only acknowledge having contractual ties with a Colombian company called Robotec, which distributes Hacking Team's services,116 though the leaked documents indicate that the national police contacted Hacking Team directly to activate spyware.117 Another leaked email suggested that the US Drug Enforcement Agency (DEA) may be conducting surveillance in Colombia.118

That same year, police reportedly said that they would start testing a centralized platform for monitoring and analysis known as PUMA. They said telephone lines would be subject to monitoring, but not social networks and chats.119 The prosecutor general's office previously ordered police to stop developing PUMA because of a lack of transparency and insufficient guarantees to ensure its lawful use. Journalists initially reported that the government was investing over $100 million in a monitoring platform in 2013. The system was intended to provide the government with the capacity to intercept telephone and internet communications, including private messages, in real time.120

Also in 2015, Privacy International found that the Bogotá police bought technology from the companies NICE (sold to Elbit Systems the same year) and Verint that could intercept phone calls in order to monitor government opponents. According to a 2018 investigation by Israeli newspaper *Haaretz*, Colombia has continued to purchase technology from Verint.121

Courts have sought to rein in illegal surveillance, sentencing former public officials involved in wiretapping scandals. In September 2018, the general attorney's office filed criminal charges against a former high-ranking police official, retired general Humberto Guatibonza, along with a hacker and three former army members for alleged illicit association, abusive access to an IT system, personal data violation, malicious software use, and illegal interceptions. The individuals were placed under house arrest.122 The investigation was still ongoing at the end of the coverage period.

Several former heads of the now-dismantled government Administrative Security Department (DAS), notably Fernando Tabares, Jorge Noguera, and María del Pilar Hurtado, were convicted for illegal wiretapping in 2015. Bernardo Moreno, former secretary of the president's office, also received an eight-year prison sentence on charges of illegally intercepting private communications of journalists, politicians, and civil society groups.123 Noguera was called to trial again, and was sentenced to 94 months in prison in 2017 for his part in illegal interception activities against human rights defenders, journalists, and civil society organizations.124 Military officials were fired in early 2015 following a high-profile wiretapping scandal.125

C6 1.00-6.00 pts0-6 pts

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

*Score Change: The score declined from 4 to 3 because the government authorized mobile providers to share users' personal data with public authorities as part of its COVID-19 response, amid a legal environment that obliges service providers to collaborate with intelligence agencies and retain subscriber data for five years.*

While some constitutional and legal protections regulate the government's use of data, service providers in Colombia are obligated to share data with the intelligence community with limited judicial review; providers are also obligated to capture and store user data for use in criminal investigations.

Service providers are required to collaborate with intelligence agencies by providing access, when feasible, to the communications history, location data, or technical data of any specific user without a warrant; intelligence agencies conducting an authorized operation only need to request the data. However, Colombian intelligence and counterintelligence agencies are also subject to Statutory Law 1621 of 2013, which binds agencies to respect "rights to honor, good name, personal and family privacy, and due process." Article 4 restricts the discriminatory use of intelligence data, including on the basis of gender, race, or origin (see C5).126

Service providers are also obliged to retain subscriber data for the purposes of criminal investigations and intelligence activities for a period of five years.127 An additional threat to user privacy comes in the form of Article 2 of Decree 1704 (2012), which requires that ISPs create access points that capture communications traffic on their networks for criminal investigation purposes—which can be used under the prosecutor general's authorization. A service provider that does not comply with these obligations faces fines and could lose its operating license.128

In March 2020, the Superintendence of Industry and Commerce (SIC), a consumer protection agency that operates under the purview of Colombia's trade ministry, released a circular that authorized telecommunications firms to share user data with public authorities as part of the country's COVID-19 response. While public entities are obliged to secure data and respect its confidentiality,129 the decision opens users to risks including discrimination, undue surveillance, invasion of privacy, and the revelation of journalistic sources. The circular does not specify what data should be collected and imposes no time limit.130

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? | 3.003<br>5.005 |

Corruption, longstanding armed conflict and associated surveillance, and the war against drugs are the greatest threats to freedom of expression in Colombia, although online journalists have not been attacked as often as print journalists. According to FLIP, at least 22 journalists have been murdered and many more have been threatened since 2005.131 There is no broad trend of retaliation specifically for online content, but the high level of intimidation towards media and human rights defenders creates a climate of fear that also affects online journalists.

In April 2020, Eder Narváez Sierra, the creator and editor of news site NP Noticias and a television correspondent,

received death threats over WhatsApp from an individual claiming to lead the Los Caparrapos armed group, which is linked to drug trafficking. Narváez speculated that an article he wrote covering two homicides, which also identified the victims, may have brought the threat about. The individual who wrote to Narváez claimed that they were responsible for the murders.[132]

During the coverage period, FLIP observed a number of cases demonstrating a continued trend of extralegal intimidation against online journalists as a consequence of their work. For example, in August 2019, journalist Vicky Dávila received several tweets threatening both her and her family after a discussion on Twitter with Senator Gustavo Petro. The conversation was spurred by Dávila's sharing of a video that showed Magdalena gubernatorial candidate Carlos Caicedo, a Petro ally, being attacked by eggs.[133] During the previous month, journalist Gabriel Angarita, of the digital television channel Tvcucuta, reported receiving a death threat through WhatsApp and another threat on Facebook.[134]

Also during the coverage period, Bogotá-based CNN correspondent Asdrúbal García was threatened on Facebook after he denounced another threat made against documentary filmmaker Jonathan Palacios on his profile. Palacios was investigating irregularities in the administration of the mayor of the municipality of Anolaima. Asdrúbal received a message from a person identified as "José Medina," who told him to "shut his mouth so flies would not enter."[135]

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? | 1.001<br>3.003 |

In 2019 and 2020, FLIP recorded at least 18 cyberattacks against websites.[136]

In early March 2020, online news outlet La Oreja Roja (the Red Ear) published an article discussing late drug trafficker José Guillermo "Añe" Hernández's suspected involvement in a vote-buying campaign during the 2018 presidential election. The website was made inaccessible the weekend after the article was published.[137]

In November 2019, the website of newsmagazine *Cartel Urbano* was attacked, and was inaccessible for several hours. The technical attack took place after the outlet published a note denouncing a police search of their office. The newsmagazine's social media accounts were also hacked, and social media comments were posted by outside individuals.[138]

Also in November 2019, the website of Cerosetenta, a digital media initiative sponsored by the University of the Andes, suffered a distributed denial-of-service (DDoS) attack. The attack came after the outlet reported that the police attempted to restrict an article from another outlet, which informed readers how to protect themselves while participating in protests.[139]

According to an editor of newsmagazine *Don Jumento*, the outlet has been unable to administer its own website since

February 2020 due to an apparent password change initiated by someone other than a staff member. Meanwhile, Mario Cepeda, the director of digital news site Página10, informed FLIP that the he could no longer administer the outlet's Facebook page in September 2019. A systems engineer found that Cepeda's inability to manage the site was the result of a hack, apparently performed by an expert. While the page remained online, Cepeda was unable to share content to it.