

# Italy

## C Violations of User Rights

*Violations of users' rights are uncommon in Italy, though cases of threats and legal intimidation against online journalists are occasionally reported. During the COVID-19 pandemic, the introduction of a contact-tracing mobile application sparked debate about privacy issues, as did the creation of a task force for harnessing data from telecommunications companies. High-profile cyberattacks of the sort that surrounded the 2018 elections were less common during the coverage period.*

C1 1.00-6.00 pts 0-6 pts

|  |                |
|--|----------------|
| Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence? | 4.004<br>6.006 |
|--|----------------|

Italy is a signatory to the European Convention on Human Rights and other relevant international treaties, and its constitutional guarantees regarding freedoms of speech and the press, as well as the confidentiality of correspondence,<sup>98</sup> are supported by an independent judiciary. Italy became the first European country to adopt a crowdsourced Declaration of Internet Rights in July 2015.<sup>99</sup> The nonbinding document includes provisions that promote net neutrality and establish internet access as a fundamental right. While generally seen as a positive development, the text has also raised some criticism for failing to outline adequate protections for anonymity, encryption, and data retention.<sup>100</sup>

Some restrictions on journalism, including online journalism, that are uncommon in other EU member states remain in place in Italy. Drawing on a 1948 law against the “clandestine press,” a regulation issued in 2001 holds that anyone providing a news service must be a “chartered” journalist with the Communication Workers’ Registry (ROC) and hold membership in the Italian National Press Federation.<sup>101</sup> With the exception of one case from the late 2000s, these rules have generally not been applied to bloggers, and in practice thousands of blogs are published in Italy without repercussions.

Italy approved a Freedom of Information Act (FOIA) only in 2016, recognizing the right to access data and documents from public administrations.<sup>102</sup> A March 2020 decree, passed during the COVID-19 pandemic, suspended FOIA requests until the end of May. A second decree issued in March suspended all nonurgent “administrative proceedings” until mid-April, encompassing FOIA requests. Journalists have lamented their impeded access to data about the spread of the pandemic on the local and regional level.<sup>103</sup>

## 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 |
|---|-------------|

Several laws present a threat to internet freedom in the country. A 2015 antiterrorism law expanded language in the criminal code on terrorist recruitment, as well as the endorsement or incitement of terrorism, to include online activities.<sup>104</sup> Critics argued that the law could be applied broadly and would sanction legitimate instances of free expression that fall within international norms on protected speech.<sup>105</sup>

Defamation is a criminal offense in Italy. According to the criminal code, “aggravated defamation” is punishable by prison terms ranging from six months to three years and a minimum fine of €516 (\$568). In cases of libel through the press, television, or other public means, there is no prescribed maximum fine.<sup>106</sup> Though these criminal provisions are rarely applied, civil libel suits against journalists, including by public officials and politicians, are a common occurrence, and the financial burden of lengthy legal proceedings may have chilling effects on reporters and their editors. In March 2017, the UN Human Rights Committee expressed renewed concerns that “forms of expression, including defamation, libel and blasphemy, remain criminal offences and can be punished with imprisonment and that article 13 of the press law and article 595 of the Criminal Code impose harsher punishments for defaming public officials, including the Head of State.”<sup>107</sup>

In early 2017, a widely criticized bill intended to tackle the spread of fake news and hate speech was presented for parliamentary discussion. According to this bill, online news organizations could be fined up to €5,000 (\$5,550) for publishing “false, exaggerated, or biased” news reports and failing to remove them within 24 hours. If fake news is deemed to damage the public interest or to seek to undermine the democratic process, publishers would face heavier fines and prison sentences.<sup>108</sup> The bill was officially presented in February 2017 but was not ultimately passed.<sup>109</sup>

## C3 1.00-6.00 pts0-6 pts

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

Defamation suits against journalists, including those operating online, remain common. Drawn-out legal proceedings, whatever their result, can entail serious financial costs for defendants. Ossigeno per l’Informazione, an organization that tracks threats to journalists in Italy, has reported hundreds of “frivolous defamation suits” against the media since 2011, including cases against online media.<sup>110</sup> According to a survey from the Italian National Institute of Statistics presented in October 2019, some 70 percent of all libel cases against journalists between 2011 and 2016 did not lead to a full investigation, a sign of the frivolous grounds of most of these complaints. However, overall convictions for defamation, whether or not the defendants were journalists, rose from 182 in 2014 to 435 in 2017, and the number of prison sentences, largely between three and six months, rose from 35 in 2014 to 64 in 2017.<sup>111</sup> In a representative incident reported in April 2019, the online news outlet Estense was presented with a €100,000 (\$110,000) lawsuit by a regional Lega politician after publishing a story in which interviewees accused the plaintiff of stopping suspected

immigrants and asking for their residency papers.[112](#)

C4 1.00-4.00 pts0-4 pts

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

The government places few restrictions on anonymous communication or encryption. Italian law does require mobile service providers to obtain customers' personal and identification data in order to register a SIM card, citing counterterrorism purposes.[113](#)

In October 2019, Parliament member Luigi Marattin indicated on Twitter that he would work on legislation to effectively ban anonymous social media accounts in Italy.[114](#) According to Marattin's statements, the proposal would require all Italians to provide identity cards when registering an account on social media. The idea was framed as a means of combating hate speech and the spread of fake news. Despite sparking widespread media coverage and a debate about its propriety,[115](#) the idea was never formally presented as draft legislation.

In May 2019, lawmaker Andrea Ruggieri had advanced a similar measure to fight anonymous trolling on social media. The proposal would have required social media companies to record users' identity cards and personal tax codes upon registration.[116](#) The concept was harshly criticized by experts in the field, who highlighted the potential for civil rights violations.[117](#) It did not appear to have advanced by the end of the coverage period.

C5 1.00-6.00 pts0-6 pts

|   |             |
|---|-------------|
| Does state surveillance of internet activities infringe on users' right to privacy? | 3.003 6.006 |
|---|-------------|

Italian courts and lawmakers have sought in recent years to better define the legal boundaries of state surveillance, whether for law enforcement, intelligence, or public health purposes.

During the COVID-19 pandemic, officials introduced a contact-tracing mobile app, known as Immuni (the immune ones), that was selected after a March 2020 open call coordinated by the ministers of health and innovation and the National Institute of Health (ISS).[118](#) The app was developed by the private company Bending Spoons and is open-source.[119](#) Use of the app, set to be formally released at the end of May, is voluntary, and the program is technically compatible with Apple and Google's more privacy-oriented framework. Immuni uses Bluetooth technology, allowing nearby devices to exchange contact information with each other, and the data are stored on each person's smartphone for no more than 14 days, theoretically maintaining both decentralization and privacy.[120](#) The launch of the app followed a wide debate about privacy, surveillance, and digital rights in the country;[121](#) after originally planning to have the app store information externally in a government-managed database, Bending Spoons later switched to a decentralized model, but there was also a lack of clarity as to whether the app would be mandatory.[122](#) The government-led process for selecting the app was frequently criticized for a lack of transparency.[123](#)

An anticorruption law approved in February 2020 included provisions and a further decree that extended the authorized use of trojans, a type of malicious software, to investigations of crimes against the public administration committed by public officials, if the crimes are punishable with at least five years of imprisonment. In addition, the changes allow for the interception to take place at “the target’s private home,” even if a crime is not occurring at the moment, as long as it has been authorized.<sup>124</sup>

Despite former US intelligence contractor Edward Snowden’s 2013 revelation of intrusive surveillance practices by the US government and its European and other allies, Italy has not engaged in a thorough public debate on surveillance. Authorities are widely perceived to be engaged in regular wiretapping, and the news media often publicizes wiretap information that is leaked to them. In 2017, it was revealed that Lorenzo Tondo, an Italian journalist at the *Guardian*, was secretly wiretapped by prosecutors while investigating Medhanie Yehdego Mered, a reputed human trafficker. Tondo condemned the wiretapping as “a clear violation of my rights as a professional journalist.”<sup>125</sup>

The use of hacking by Italian law enforcement agencies has been documented, and in May 2017, the UN Human Rights Committee raised concerns that “intelligence agencies are intercepting personal communications and employing hacking techniques without explicit statutory authorization or clearly defined safeguards from abuse.”<sup>126</sup> In July 2016, however, the Supreme Court had ruled that hacking by law enforcement authorities under certain circumstances was constitutional and in accordance with human rights law.<sup>127</sup>

Lawmakers have made several attempts to regulate hacking in recent years.<sup>128</sup> A criminal justice reform law approved in June 2017 calls on the government to regulate hacking for the purpose of criminal investigations.<sup>129</sup> Organizations such as Privacy International have contended that the law fails to meet the standard of legality, necessity, and proportionality, and does not establish sufficient minimization procedures, effective oversight, or safeguards from abuse.<sup>130</sup> Another proposal known as the Trojan Bill sought to establish a more robust system for authorizing remote and covert hacking.<sup>131</sup> The bill was ultimately withdrawn in the aftermath of the March 2018 general elections.

A November 2018 ruling by the Supreme Court was expected to effectively place limits on authorities’ ability to conduct hacking as part of a criminal investigation. The case involved the installation of malware on a suspect’s mobile phone; the Supreme Court instructed a lower court to reexamine whether police practices were consistent with articles of the European Convention of Human Rights and the Italian constitution that protect the freedom and confidentiality of correspondence and other forms of communication.<sup>132</sup> According to Privacy International, the ruling “points to the need for Italy and other states to thoroughly review their practices of hacking for surveillance purposes and stop these activities until and unless they can be demonstrated to be in full compliance with applicable international human rights law.”<sup>133</sup>

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 |
|--|----------------|

Service providers are required to comply with law enforcement requests for users' activity records, known as metadata, under a variety of circumstances, including in the course of a criminal investigation or "for the purpose of preventing crimes by criminal associations and international terrorism organizations."<sup>134</sup>

Although the CJEU struck down the 2006 EU directive on the retention of data, Italy has extended the period for which ISPs must keep users' metadata. In November 2017, Parliament swiftly approved a regulation on data retention that requires telecommunications companies to store telephone and internet data for up to six years. Despite civil society protests, there was virtually no public or parliamentary debate on the measure, which had been added to unrelated legislation following a European Council directive before passage.<sup>135</sup> The DPA expressed its objection to the bill, citing its incompatibility with EU law and case law.<sup>136</sup> European Data Protection Supervisor Giovanni Buttarelli commented that the new regulation did not reflect the European approach to data retention: "The European Court of Justice has said that we can no longer collect anything that concerns us all just to have it 'in case.' This is a type of approach that is not part of the European legal system."<sup>137</sup>

In March 2020, in response to COVID-19, a Ministry of Innovation task force collaborated with the University of Pavia to create a program that compiles and analyzes anonymized data drawn from Facebook and telecommunications firms such as TIM, Vodafone, Wind Tre, and Fastweb. According to *Wired Italy*, the datasets "aggregate users' movements to help with contact tracing or other forms of monitoring."<sup>138</sup> The system is apparently used by health researchers and nonprofit organizations that have signed licensing agreements with Facebook. The president of the Italian Privacy Institute warned that while EU regulators allow for a loosening of data protection rules in a public emergency, the Italian program lacked provisions for the restoration of ordinary safeguards and the deletion of the data after the crisis has passed.<sup>139</sup>

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 |
|---|----------------|

While cases of intimidation or physical violence in response to online activity are reported only sporadically, individuals who expose organized crime activities in some parts of the country may be especially at risk of reprisals. For example, in May 2019, journalist Gaetano Scariolo's car was set on fire by unknown assailants. Scariolo, who covers criminal justice and whose work appears online, said, "I am sure that the intimidation has to do with my professional activity."<sup>140</sup>

Ossigeno per l'Informazione documented 433 cases of threats and intimidation against journalists and bloggers during 2019.<sup>141</sup> The previous year, the organization found that 11 percent of all threats against journalists were issued online.<sup>142</sup>

Hate speech remains an endemic problem on the Italian internet.<sup>143</sup> Women journalists and politicians in particular are subject to virulent online harassment. In the summer of 2018, journalist Annalisa Camilli received derogatory and

threatening anonymous emails after publishing an online story about a migrant rescued at sea by the nongovernmental organization Open Arms.[144](#) Other female journalists have reported experiencing similar harassment, frequently for their coverage of the migration crisis.[145](#) Independent lawmaker Laura Boldrini was harassed throughout the coverage period, including by Salvini, whose posts about her elicited death and rape threats from his online supporters.[146](#)

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<br>3.003 |
|---|----------------|

*Score Change: The score improved from 1 to 2 because there was no repetition of the high-profile cyberattacks that surrounded the 2018 elections during the previous coverage period.*

Cyberattacks have constituted a problem in Italy in recent years, though the defacement of or distributed denial-of-service (DDoS) attacks against the websites of political figures were less common during the latest coverage period. Hacks of public and private institutions continued to occur.

On April 1, 2020, the National Social Security Institute (INPS) was forced to shut down its website due to a data breach. Initially attributed to a series of cyberattacks, the incident occurred on the first day that self-employed Italians could apply for a coronavirus relief package announced by the government in mid-March. Early login attempts reportedly led to several cases in which other users' information was displayed; the information was published by the hackers to reveal that they had obtained such data and would publish it all if a technical problem with the website was not fixed and users were not notified.[147](#) The following day, by which time the site had become accessible again,[148](#) the head of the DPA announced that it had started an audit of the INPS's recovery measures in order to identify any further interventions that might be needed to protect personal data.[149](#)

It was reported in May 2020 that, two months earlier, hacktivist groups Anonymous Italia and LulzSec Italia had hacked the intranet of a major Milan hospital, San Raffaele. The email addresses and passwords of 2,400 hospital employees and the personal data (including name, date of birth, nationality, and social security number) of at least 600 patients were allegedly stolen. The hackers stated that the hospital administration, under the GDPR, should have alerted both the DPA and the individuals whose data were exposed, which they said never happened, and they threatened to publish the data online. The hospital denied that the data breach occurred.[150](#)

In May 2019, Anonymous and LulzSec Italia breached the database of Rome's Bar Association, exposing the email accounts of 30,000 registered lawyers. The breach allegedly included the account of the mayor of Rome, a registered lawyer.[151](#)

In a major data breach reported in April 2019, roughly 1.4 million users' information was stolen from the Italian email services provider Italiaonline. Popular services Libero Mail and Virgilio Mail were also affected. A 24-year-old hacker

was arrested and charged for the attack that month, but not before selling the data to an unidentified party. The hacker entered Italiaonline's network by cracking its Wi-Fi network from a bar near the company's headquarters.[152](#)

In March 2019, *Vice* reported that hackers working for an Italian surveillance company had infected hundreds of people's devices with several malicious mobile apps that were hosted on the official Google Play store for months.[153](#) Experts said that the operation may have ensnared innocent victims, as the spyware appears to have been faulty and poorly targeted. The DPA announced an investigation into the matter, with the head of the authority declaring that such tools posed a serious risk to citizens' freedoms if deployed without the necessary safeguards. Prosecutors in turn launched an investigation into eSurv,[154](#) the company that made the spyware, seizing its computers and shutting down the program's infrastructure.

In its annual report, the Italian Association on Cybersecurity (CLUSIT) called 2018 the "worst year ever" with respect to the evolution of cybercrimes and attacks, both quantitatively and qualitatively.[155](#) The 2018 general election campaign in particular was characterized by several high-profile hacks. In February 2018, the Florence section of the Democratic Party was hacked, and personal information, including former prime minister Matteo Renzi's mobile phone number, was posted on Twitter by the hackers.[156](#) In the same week, two of Salvini's campaign websites were hacked, and some internal Lega party data were subsequently released on Twitter by the hackers. The AnonPlus collective claimed responsibility for both attacks.[157](#) Separately, in November 2018, LulzSec Italia and another collective, AntiSec Italia, conducted attacks targeting the websites of the Ministry of Economic Development, the State Police, the Brothers of Italy party, and some local branches of other political parties.[158](#)

During the summer of 2017, the Five Star Movement was hacked by an attacker using the handle @r0gue\_0. The perpetrator infiltrated Rousseau, the party's online organizing platform, and leaked internal data, including a password used by staff to access the platform.[159](#) The same hacker allegedly infiltrated the platform again in 2018, leaking phone numbers of two Five Star Movement ministers.[160](#) In September 2018, the DPA opened an investigation into the platform's security flaws and those of various websites connected to the Five Star Movement,[161](#) and in April 2019 it fined Rousseau €50,000 (\$55,000) for various data protection failures.[162](#)

Awareness of Italian involvement in the international cyber-weapons market has grown, and Italian companies have faced increased scrutiny over sales of surveillance software to government agencies and repressive regimes. In July 2015, a leak of internal documents from the Milan-based surveillance technology firm Hacking Team revealed details about some of the company's clients around the world, including in countries with poor human rights records.[163](#) The company had been criticized in the past for cooperating with undemocratic regimes and lacking sufficient consideration of users' privacy.[164](#) In April 2016, the Italian government suspended Hacking Team's "global" authorization to export its software, requiring it to obtain individual licenses from Italian authorities to serve countries outside of the EU.[165](#)

According to a study from Privacy International in August 2016, three other companies based in Italy market intrusion technology.[166](#) In 2017, the Italian Coalition for Civil Liberties and Rights, Privacy International, and the Hermes Center for Transparency and Digital Human Rights wrote a public letter asking the Ministry of Economic

Development to reconsider the export authorization for the Italian company AREA, which had been investigated after selling its products in Syria and Egypt.<sup>167</sup> The ministry issued a press release stating that the company's export authorization for Egypt had been suspended and would be revoked.<sup>168</sup> However, civil society organizations have continued to demand greater transparency on export licensing and the countries involved.<sup>169</sup>