

South Africa

C Violations of User Rights

State of disaster regulations enacted in response to the COVID-19 pandemic impose criminal penalties for online speech that misleads people about the pandemic or misrepresents information about the government's response. Several people were arrested under the regulations. A High Court ruled that South African law does not authorize the state to conduct bulk interception of private communications and found numerous provisions of the national security surveillance authority to be unconstitutional.

C1 1.00-6.00 pts0-6 pts

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

Score change: The score declined from 5 to 4 as the government enacted state of disaster regulations that limited freedom of expression online during the COVID-19 pandemic.

There are no specific legislative provisions to protect online modes of expression. However, the constitution provides for freedom of the press and freedom of expression, among other guarantees. It also includes constraints on “propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that constitutes incitement to cause harm.”¹¹³ The right of access to information held by the state, and in limited circumstances by private bodies, is also guaranteed by the constitution.¹¹⁴ These rights apply to all members of the public and to journalists equally, whether they operate online or offline. However, observers have expressed concern that, if signed into law, the Films and Publications Amendment Act will make online content vulnerable to censorship (see B3).

In March 2020, the government declared a three-month state of disaster under the Disaster Management Act of 2002 in response to the COVID-19 pandemic. The regulations issued under the state of disaster imposed a national lockdown, limiting freedom of expression, freedom of movement, and other rights that are derogable under the Constitution.¹¹⁵ The state of disaster remains in place as of September 2020 following numerous extensions by the government, amid numerous losses in the courts to legal challenges that contested the validity of the regulations.¹¹⁶

In a positive development for internet freedom, in July 2018, South Africa voted in favor of a UN Human Rights Council (UNHRC) resolution on “the promotion, protection, and enjoyment of human rights on the internet.”¹¹⁷ South Africa had previously voted against a 2016 version of the resolution, siding with repressive countries such as China, Russia, and Saudi Arabia.¹¹⁸

The judiciary is generally regarded as independent and in recent years has been seen as the branch of government that has been most dedicated to upholding the rule of law by constraining the executive and legislative branches from arbitrary actions.[119](#)

The police and other law enforcement agencies have been criticized for failing to adequately investigate and prosecute EFF supporters who have threatened and attacked journalists, contributing to an environment of impunity and threatening rights guaranteed in the constitution.[120](#)

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
---	----------------

A number of laws are vulnerable to being misused to prosecute online journalists and activists. The offense of *crimen injuria*, or insulting the dignity of a person, has been invoked to prosecute online harassment.[121](#)

The state of disaster regulations passed in March 2020 criminalize “any statement, through any medium, including social media, with the intention to deceive any other person about COVID-19; COVID-19 infection status of any person; or any measure taken by the Government to address COVID-19.” The penalty is a fine or imprisonment of up to six months, or both.[122](#)

Defamation is a criminal offense, though prosecutions are rare and, until recently, defamation charges were not brought against people for online activity. The ANC committed to scrapping criminal defamation in September 2015, but there have been no moves to introduce legislation to fulfill this promise.[123](#)

A draft Cybercrimes and Cybersecurity Bill, first introduced in 2015, was criticized by civil society activists for its ambiguous language, which they claim has the potential to infringe on freedom of expression.[124](#) In the second version of the bill, introduced in 2017, a chapter on “malicious communications” would penalize the dissemination of a “data message which is harmful,” the definition of which includes content that is “inherently false,” without further specifications.[125](#) The bill also contained a number of provisions that were vaguely worded, leading to concerns that it could be used to censor political speech online,[126](#) while other aspects of the bill would enhance the state’s surveillance powers (see C5).

In October 2018, a substantially revised third version of the bill was presented by the Department of Justice and Constitutional Development. The legislation, renamed the Cybercrimes Bill, no longer contained language on cybersecurity.[127](#) It also addressed the ambiguous definition of “unlawful,” bringing it in line with the Protection of Personal Information (POPI) Act of 2013, and dispensed with crimes related to “critical infrastructure.”[128](#) This version was passed by the National Assembly in November 2018. An amended version of the bill was adopted in July 2020, after the coverage period, and now awaits signature by the President.[129](#)

C3 1.00-6.00 pts0-6 pts

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

Score change: The score declined from 6 to 5 after several internet users were

arrested for spreading false information relating to the COVID-19 pandemic online.

No individual was prosecuted, detained, or sanctioned by the state for protected political, social, or religious speech online during the coverage period. However, at least eight individuals were arrested during the coverage period for spreading false information related to COVID-19. The arrests were made pursuant to the state of disaster regulations, which prohibit the intentional dissemination of false information relating to the virus.¹³⁰ One of those detained, Stephen Birch, was arrested for circulating misleading information about test kits online and charged under the March 2020 emergency regulations.¹³¹ Celebrity Somizi Mhlongo was charged with violating the regulations for suggesting during an Instagram Live stream that Transport Minister Fikile Mbalula told him that the state of disaster lockdown would be extended; Mhlongo turned himself into the police and was released on bail.¹³²

C4 1.00-4.00 pts 0-4 pts

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

South Africa has few restrictions on anonymous communication or encryption. There are no laws requiring internet users, website owners, or bloggers in South Africa to register with the government or any of its agencies to operate. Users are also not required to use their real names when posting comments on the internet, including on social media platforms.

The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) of 2002, however, compromises users' rights to anonymous communication by requiring mobile subscribers to provide national identification numbers, copies of national identification documents, and proof of physical address to service providers.¹³³ An identification number is legally required for any SIM card purchase, and registration requires proof of residence and an identity document.¹³⁴ Beyond privacy concerns, the RICA requirements can be an obstacle to mobile phone usage for the many South Africans who live in informal settlements with no recognized address.

Users are not explicitly prohibited from using encryption to safeguard their communications. However, RICA empowers a judge to force the disclosure of decryption keys or to require assistance in decryption in specified circumstances, upon approval of a request made by the police, military, intelligence, or other law enforcement agencies.¹³⁵

C5 1.00-6.00 pts 0-6 pts

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

Strong concerns about potentially unchecked government surveillance powers over online activity remain, but some legal safeguards related to surveillance do exist. RICA does not permit the blanket collection of telecommunications metadata but provides for a stringent process for the targeted collection of metadata, the interception of communications, and the decryption of private communications, all

of which require a court order.[136](#)

In September 2019, a High Court ruled that numerous provisions of RICA were unconstitutional.[137](#) The Amabhungane Centre for Investigative Journalism had filed a case in April 2017 challenging the constitutionality of RICA on several fronts. The High Court ruled that the bulk surveillance conducted by the National Communication Centre (NCC) is unlawful because there is no legislation that authorizes the state to conduct such interception of private communications. The ruling postponed the resulting invalidation of RICA for two years to permit parliament to pass legislation amending the unconstitutional provisions and imposed interim changes to the law. The interim changes include requiring the NCC to notify individuals who have their communications intercepted within 90 days after the surveillance has been terminated and to disclose in its application when the target of surveillance is a journalist or lawyer.

Under RICA, the threshold for granting a court order is low, oversight is insufficient, and in the past users did not have to be informed that their communications had been intercepted.[138](#) A loophole allows communications to be intercepted under the Criminal Procedure Act, which lacks certain safeguards and has been abused by law enforcement agencies.[139](#) Up to 95 percent of court orders involving the interception of communications are not approved by a RICA judge; most of the court orders outside of RICA are for metadata. The metadata of between 70,000 and 195,000 mobile users is collected every year.[140](#) Telecommunications service providers are also required to store the metadata of all customers for three to five years, a provision that concerns privacy advocates.[141](#)

South Africa has the technical capacity to undertake bulk and targeted surveillance, and it has been acknowledged that bulk surveillance is being undertaken by various government agencies.[142](#) This is particularly concerning because RICA's oversight applies only to domestic signal interception and not to the interception of foreign signals (which originate outside South Africa but pass through or terminate in the country), which include communications such as emails.[143](#) The NCC is responsible for intercepting foreign signals and does so without oversight. According to reporting from Privacy International, published in August 2019, South African security agencies claim that while bulk surveillance is meant to focus on foreign communications, their surveillance system is unable to discern between international and domestic communications and therefore collects both.[144](#)

The South African police possess international mobile subscriber identity (IMSI) catcher technology, also known as "stingrays," which permit the bulk interception of mobile phone traffic, although the extent of its use is uncertain.[145](#) The Ministry of State Security does not believe that IMSI catchers are governed by RICA, and use is therefore unregulated.[146](#) The government has claimed that the technology is used only for national security matters.[147](#) Nonetheless, consistent weaknesses in oversight mechanisms within the state security departments leave surveillance open to abuse; in addition, the interception of communications that originate outside South Africa are essentially unregulated.[148](#) In light of the September 2019 court ruling on RICA, the state's use of IMSI catchers is illegal unless new legislation is passed to regulate such use for bulk surveillance.

South Africa's intelligence services are also reported to be using a social media analytics and monitoring tool called Media Sonar, which allows for the searching and analyzing of social media content of users within a defined geolocation and the use of keyword searches.[149](#)

Journalists have been frequently targeted for surveillance by the state, usually as a means of identifying confidential sources.¹⁵⁰ For example, in May 2018, it emerged that the telephone conversations of investigative journalist Jacques Pauw had been intercepted while he was reporting on state capture during the Zuma administration.¹⁵¹ Nonstate actors have also targeted journalists for surveillance purposes. In March 2018, the *Mail & Guardian* disclosed that the telephone records of journalist Athandiwe Saba, who had reported critically on the Railway Safety Regulator, were obtained by a private investigator hired by the regulator, likely with the assistance of the police or National Prosecuting Authority.¹⁵²

In a 2018 report by Citizen Lab, a Canadian internet watchdog, South Africa is listed as one of 45 countries worldwide using Pegasus, a targeted spyware software developed by the Israeli technology firm NSO. Pegasus is known to be used by governments to spy on journalists, human rights defenders, and the opposition.¹⁵³

Concerns over the potentially unchecked government surveillance powers over online activity remain, but they were somewhat addressed when Dr. Setlhomamaru Isaac Dintwe was appointed as the inspector general of intelligence (IGI) in 2017, after the position had been vacant for an extended period.¹⁵⁴ As an independent actor accountable to parliament, the IGI was expected to strengthen oversight mechanisms for intelligence agencies and determine their compliance with the legislative framework and constitution.¹⁵⁵ However, upon assuming office, Dintwe had difficulty fulfilling his mandate as a result of interference by leadership in the intelligence community. In April 2018, he filed an urgent court application to prohibit Arthur Fraser, the director general of the State Security Agency (SSA), from intervening in the execution of his mandate.¹⁵⁶ Fraser was subsequently transferred out of the SSA.¹⁵⁷

Beyond RICA, the POPI Act serves as South Africa's legal framework protecting the constitutional right to privacy. POPI includes provisions to protect users' online security, privacy, and data, and allows an individual to bring civil claims against those who contravene the law (see C6).¹⁵⁸

In February 2019, a private company, Vumacam, commenced the installation of 15,000 CCTV cameras in a number of Johannesburg suburbs,¹⁵⁹ as part of an effort to address rising crime. Vumacam sells its footage to security companies operating in neighborhoods within its coverage area. Analysts expressed concern that the CCTV network is potentially a tool for unchecked mass surveillance and racialized profiling of black and brown people in public spaces.¹⁶⁰ Vumacam denied that its cameras are enabled with facial recognition technology and stated that it is not building a database on the movements of private citizens or engaging in racial profiling.¹⁶¹ Concerns have also been raised that Vumacam is not registered with the Private Security Industry Regulatory Authority.¹⁶²

Provisions in the Cybercrimes and Cybersecurity Bill that could have enhanced the state's interception powers were removed in October 2018 (see C2).

C6 1.00-6.00 pts 0-6 pts

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

The Protection of Personal Information Act of 2013, South Africa's data protection

framework, entered fully into force on July 1, 2020, after the coverage period. RICA provides for a legal process for the interception of communications, and service providers are, under certain circumstances, required to aid the government in surveillance (see C5).

POPI entered fully into force following a presidential proclamation in June 2020. A few elements of POPI had entered into force by presidential proclamation in 2014, including the establishment of the South African Information Regulator, which was not able to act in the six-year interim. The deadline for implementation of POPI is July 1, 2021.[163](#)

POPI establishes safeguards for the processing of personal data, including requirements for consent, retention limitations, and notice and limitations on automated processing and cross-border data transfers. POPI defines personal data broadly, covering information about individuals, their beliefs, and their legal identity, and also establishes more extensive safeguards for especially sensitive personal data. The law includes a standard set of exceptions, including national security and criminal matters. Penalties for contravening the law are stiff, including prison terms and fines of up to 10 million South African rands (\$650,000).[164](#)

According to RICA, service providers, including ISPs, are required to use systems with the technical capacity for communications to be intercepted; they are also required to retain customer metadata for three to five years.[165](#) RICA specifically requires service providers to intercept and provide the communications of their customers upon a judge's directive.[166](#) In practice, however, the bulk of requests for information are not made through RICA and are thus not transparent or subject to appeal (see C5). However, neither RICA nor POPI impose data localization requirements.

While the ECTA does not require ISPs to actively monitor content or to seek information on unlawful activity, the minister of communications may, under certain circumstances, require ISPs to provide information on illegal activities of their users or information that facilitates the identification of users.[167](#)

C7 1.00-5.00 pts0-5 pts

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

Cases of extralegal intimidation or violence reported against bloggers, journalists, and online users declined sharply after the May 2019 elections. Women and LGBTQ+ people routinely experience online harassment in South Africa.

In March 2020, Azarrah Karim, a journalist for the online newspaper News24, was fired at by police officers while covering police dispersing crowds with rubber bullets in Johannesburg during the first day of the lockdown, even after she identified herself as press.[168](#) Karim was later mocked by officers when she filed a statement at the local police station.[169](#)

Members of the EFF, including leader Julius Malema, have attacked and encouraged attacks against journalists online on several occasions. In March 2019, for example, veteran journalist Karima Brown mistakenly posted a message directed

to her staff on a WhatsApp Group that included EFF members. In response, Malema posted a screenshot of the message that contained Brown's mobile number on Twitter. Brown then received a barrage of abusive and threatening messages from EFF supporters.¹⁷⁰ Several other journalists, including Adriaan Basson of News24¹⁷¹ and Pauli van Wyk of the Daily Maverick, have also faced online attacks by Malema and supporters of the EFF.

Although the EFF has threatened online journalists more prominently and apparently with more frequency than other political actors, supporters of the ANC have also been known to threaten and harass online critics. In September 2018, a prominent ANC member allegedly sent *Sunday Times* journalist Qaanitah Hunter an image of a gun in a text message, in response to an article she wrote about former president Zuma.¹⁷²

The South African National Editors' Forum (SANEF) took the EFF to court over allegedly enabling the intimidation and harassment of journalists. The case was dismissed for technical reasons relating to the legislative provisions that SANEF attempted to rely on, which the court ruled were not applicable. ¹⁷³

Online harassment on the basis of gender and sexuality is rampant in South Africa, and racist language is common. Almost one-quarter of South African women report experiencing online gender-based violence, according to an August 2020 report by Pollicy, a technology consulting firm, that surveyed 536 South African women.¹⁷⁴ In a 2018 report by Gender Links, 30 percent of women journalists surveyed reported experiencing some form of online violence.¹⁷⁵ A survey of LGBTQ+ youth released in April 2020 found that 82 percent reported experiencing harassment online because of their identity.¹⁷⁶ A report from PeaceTech Lab and Media Monitoring Africa found a sharp increase in racist and racially discriminatory terminology online during the May 2019 elections.¹⁷⁷

C8 1.00-3.00 pts 0-3 pts

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

South Africa is highly vulnerable to cybersecurity threats on many fronts, though independent news outlets and opposition voices were not subject to targeted technical attacks during the coverage period.

In February 2020, Nedbank announced that one of its third-party service providers had been hacked, leading to the theft of the personal data of 1.7 million customers including their names, ID numbers, telephone numbers, physical addresses, and email addresses.¹⁷⁸ In October 2019, several major South African banks were targeted by a distributed denial-of-service (DDoS) attack that was aimed at extracting ransom payments from them.¹⁷⁹ The City of Johannesburg also reported a breach of its network in October 2019 after its systems were attacked by a group calling themselves the Shadow Kill Hackers who demanded payment in Bitcoin and threatened to publish the data online if they were not paid.¹⁸⁰ The city was forced to shut down its website and billing services in an effort to contain the attack.

Government websites are often hacked. Most of the hacks are perpetrated by amateur hackers with no apparent political motivations other than to advertise their

skills. The government website of the National Cybersecurity Hub, whose objective is to protect South African citizens and businesses online, was hacked in August 2018.¹⁸¹ These attacks are usually short-lived, with the websites restored within a few days.¹⁸²

The ECTA contains provisions that protect against cyberattack by criminalizing access or interception of an individual's data without permission; interference with an individual's data without permission; unlawful production, sale, procurement, design, distribution, or possession of a device used to overcome security measures or the protection of data; the use of such a device to unlawfully overcome security measures for the protection of data; and interference with an information system that protects data.¹⁸³