

# Rwanda | Freedom House

## Overview

Internet freedom in Rwanda declined during the coverage period, as the government continued to limit space for online expression, including through a restrictive new cybersecurity law, the continued blocking of independent news sites, and surveillance of social media users. Self-censorship online remains common, particularly around politically sensitive periods such as the run-up to the 2018 parliamentary elections and the commemoration of the 25th anniversary of the genocide in April 2019.

Although two opposition candidates won seats in Parliament in the 2018 parliamentary elections, President Paul Kagame and the Rwandan Patriotic Front (RPF), which has ruled since 1994, maintain tight control over the political system. The government habitually suppresses political dissent through pervasive surveillance, intimidation, arrest, and suspected assassinations of dissidents, including across borders.

## Key Developments

### June 1, 2018 – May 31, 2019

- Press freedom advocates expressed concern that a new cybersecurity law passed in August 2018 could be used to target journalists and bloggers. Among the broad and vaguely worded provisions in the law, anyone who publishes “rumors” or “establishes, publishes, or uses a site of a terrorist group” could be subject to fine or imprisonment ([see C2](#))
- In April 2019, Rwanda's Supreme Court repealed a law that banned the publication of political cartoons, but upheld a law that makes defamation of the president punishable by at least five years in prison ([see C2](#)).
- During the coverage period, four journalists were arrested for allegedly spreading rumors and propaganda against President Kagame on YouTube. All those arrested and detained awaited trial at the end of the coverage period ([see C3](#)).
- New SIM card registration requirements instituted in July 2018 compelled individuals to present identification to receive a SIM card, while additional regulations rolled out in January 2019 prohibit mobile phone users from having more than three SIM cards on each network. Critics argued that the regulations were designed to enable greater government surveillance of mobile phone users ([see C4](#)).

## A Obstacles to Access

*Rwanda continued making strides in expanding internet access and improving affordability, but new information suggests that the internet service provider (ISP)*

*market is significantly less diverse than previously believed.*

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	36
--	----

Access to information and communication technologies (ICTs) in Rwanda has improved notably in recent years. The government has invested in building its internet infrastructure and other ICTs in its effort to develop a robust information economy.

According to a December 2018 report by the Rwanda Utilities Regulatory Agency (RURA), the sector regulator, internet penetration has reached 52 percent.<sup>1</sup> However, DataReportal reported a lower penetration rate of 44 percent in January 2019.<sup>2</sup> Most new users are accessing the internet on smartphones. Only 4.9 percent of the population is active on social media.

According to the government, over 90 percent of the population lives in areas covered by broadband networks. Government investments in broadband technology across the country continued to grow during the reporting period (see A2). The International Telecommunication Union (ITU) is collaborating with the Rwanda Utilities Regulatory Authority (RURA) to further expand broadband coverage (see A2).<sup>3</sup>

Improved access to electricity via hydropower and solar energy projects has helped increase internet connection speeds and decrease costs. However, according to the government, by June 2018, only 44 percent of the population had access to electricity, <sup>4</sup> which fell far short of the government's ambitious plan to achieve 70 percent electrification by 2018.<sup>5</sup>

According to Akamai's *State of the Internet* report, Rwanda's average internet connection speed was 7.7 Mbps in 2017, above the global average of 7.0 Mbps.<sup>6</sup> However, limited fixed-line infrastructure has negatively impacted internet access. Nevertheless, developments in the fixed-network market have improved connectivity and reliability. Operators have rolled out national fiber-optic backbone networks to connect to the international submarine fiber-optic cables on the east coast of Africa. The cables have provided the entire region with fiber-based international bandwidth for the first time, ending the dependency on satellites. During the reporting period, Liquid Telecom continued to expand its fiber to the premises (FTTP) services in Kigali and some small towns.<sup>7</sup>

In 2013, the government signed a deal with Korea Telecom Rwanda Network (KTRN) to provide internet service to 95 percent of the population.<sup>8</sup> KTRN is a wholesale provider of the universal mobile broadband network built on 4G LTE technology. National LTE coverage was reached in 2018.<sup>9</sup>

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	13
---	----

Internet access is concentrated primarily in Kigali and remains beyond the reach of many citizens, particularly those in rural areas who are limited by low income and

low levels of ICT awareness.<sup>10</sup> However, there have been efforts to reduce costs and expand service to underserved communities. Poverty continues to be the primary impediment to internet access, with the majority of the population engaged in subsistence agriculture. Despite these challenges, the Alliance for Affordable Internet ranked Rwanda as the 28th most affordable internet environment among 60 low- and middle-income countries in 2018.<sup>11</sup>

In October 2018, KTRN announced a reduction in 4G internet prices to as low as 1,000 Rwandan francs (\$1) per day and 3,000 francs (\$3) per month, in an effort to lessen economic barriers to internet access.<sup>12</sup> However, in March 2019, Expatistan, an online index that measures the cost of living across countries, estimated that the price of internet service at 8 Mbps in Kigali was nearly 23,000 francs (\$23) per month, which is prohibitively expensive for the majority of residents.<sup>13</sup>

Only 11 percent of Rwandans are ICT literate,<sup>14</sup> and over 70 percent of the population speaks only Kinyarwanda, making internet content in English inaccessible to the majority of Rwandans.<sup>15</sup>

The joint ITU and RURA broadband expansion project aims to increase connectivity in rural areas and improve access to government services and information. According to the ITU, the project also aims to provide free or low-cost internet access to schools, hospitals, and underserved populations.<sup>16</sup> In February 2019, OneWeb, a UK-based company, launched a satellite that brings internet access to schools in remote areas.<sup>17</sup>

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	56
--	----

There were no restrictions on connectivity reported in Rwanda during the coverage period, though Article 52 of the 2001 Law Governing Telecommunications gives the government powers over telecommunications networks in the name of preserving “national integrity.” These powers include the ability to “suspend a telecommunications service for an indeterminate period, either generally or for certain communications.”<sup>18</sup>

The local internet exchange point (IXP), the Rwanda Internet Exchange (RINEX),<sup>19</sup> is managed by the Rwanda Information & Communications Technology Association, a nonprofit comprised of ICT institutions and professionals.<sup>20</sup>

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	36
--	----

RURA is not transparent in its oversight of ISPs. As of March 2019, more than 30 ISPs were licensed. However, an anonymous source from the legal department at RURA said in 2019 that the majority of ISPs are no longer operational due to the dominance of MTN and Airtel. According to the source, the hegemony of these two companies is in the state’s interest because centralization allows RURA to more easily monitor users.<sup>21</sup> According to local sources, government officials and agencies have shares in some telecommunications companies, which may enable the state to interfere in their operations.

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	14
--	----

There are no legal guarantees for the autonomy of RURA. RURA reports directly to the office of the prime minister. The government audits RURA's budget, while the president nominates its seven board members, supervisory board, and director general, limiting its autonomy in practice.[22](#)

Recent appointments to RURA have raised concerns about the influence of the military and intelligence services on the regulation of the ICT sector.[23](#) Patrick Nyirishema, a senior military officer,[24](#) was appointed director general of RURA in 2014.[25](#) A former head of Rwanda Interpol and the Criminal Investigation Department, Anthony Kulamba, serves as the head of media regulation and consumer affairs at RURA.[26](#)

There are no mechanisms for ISPs or other companies regulated by RURA to appeal its decisions.[27](#) Furthermore, no self-regulatory mechanism available for the ISPs.[28](#)

## B Limits on Content

*Censorship of online content remained common, with a number of independent online media outlets still blocked in the country. Self-censorship also remains prevalent, particularly related to controversial issues. The 2018 parliamentary elections and 2019 genocide commemoration were particularly sensitive subjects during the reporting period. President Kagame has threatened members of the diaspora who speak out against the government online. These threats are considered credible, given the regime's history of targeting dissidents.*

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	36
---	----

The government restricts the types of online content that users can access, particularly material that strays from the government's official line. In 2018 and 2019, numerous independent news outlets and opposition blogs that have been blocked for years reportedly remained inaccessible,[29](#) including the website of the *Rwandan* newspaper, as well as the online publications Inyenyeri News and Le Prophete.[30](#) The websites for independent regional news outlets such as *Great Lakes Voice* and websites of the Rwandan diaspora such as Rugali are also blocked and only accessible via web proxy. The BBC Kinyarwanda/Kirundi website has remained inaccessible since 2014. However, most international news sources, some of which are critical of the Rwandan government, are available online. These websites most likely remain unblocked because the majority of Rwandans engage with content in the local language, Kinyarwanda.

The websites of several Ugandan news outlets were blocked in the wake of rising diplomatic tensions between the two countries in recent years. Each government, through state-sponsored media houses and social media platforms, has accused the other of espionage and intent to undermine state security. The website of SoftPower

News, a Ugandan digital media company, remained blocked in Rwanda as of May 2019. After the coverage period, in August 2019, Rwanda reportedly blocked additional Ugandan websites<sup>31</sup> in retaliation for Uganda blocking Rwanda's *New Times* website.

Social networking sites and communications apps such as YouTube, Facebook, Twitter, and WhatsApp are freely available.

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?	24
--	----

The extent to which the government forces websites or digital platforms to delete content is unknown, though anecdotal evidence in recent years suggest that the practice is common. According to journalists who have spoken on condition of anonymity, authorities often pressure editors of news sites to delete content that is critical of the government, threatening to block sites that do not comply.<sup>32</sup> Local journalists refer to the practice as “kunyonga,” which means “shooting down anonymously.”

Credible sources claim that the Office of the Government Spokesperson (OGS), an official propaganda entity, has administrative access to the websites of some nominally independent newspapers. Government employees reportedly remove stories deemed critical of the Kagame administration on a routine basis.

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	14
---	----

RURA generally does not provide explanations when local and international news sites are blocked. Website owners have no avenue of appeal when their sites are blocked.

In May 2019, the Rwandan government announced it intends to start regulating social media content, arguing that it was necessary to protect citizens from misinformation and that social media platforms were being used to rally people to disrupt society. Specific regulations have not been announced, but critics say the move targets government critics and independent journalists.<sup>33</sup>

According to a 2010 law relating to electronic messages, signatures, and transactions, intermediaries and service providers are not held liable for content transmitted through their networks.<sup>34</sup> Nonetheless, service providers are required to remove content when handed a takedown notice, and there are no mechanisms for appeal.

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	04
---	----

While Rwandans are active on Facebook and Twitter, self-censorship has become

more pervasive among both online journalists and ordinary users in recent years due to increasing government repression, social pressure to support the government, and fear of reprisals for those who criticize the authorities. The hostile environment for journalists, who risk prosecution and imprisonment for critical, independent reporting, contributes to self-censorship. The disappearance and murder of numerous opposition members similarly reinforces self-censorship ([see C7](#)). [35](#) Internet users typically avoid topics that can be construed as critical of the government or disruptive to national unity and reconciliation.[36](#)

President Kagame has frequently threatened his critics and accused them of destabilizing the country, further entrenching self-censorship. In a speech in May 2019, Kagame warned opponents of his government in the diaspora when he said, "Those making noise on the internet do so because they're far from the fire. If they dare get close to it, they'll face its heat."[37](#) Observers argued that Kagame's threats were genuine, in light of the fact that a number of Rwandan dissidents abroad have been killed or disappeared.

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	14
--	----

Online information is manipulated by the government through editorial influence and coordinated social media campaigns.

Security officials and other government authorities frequently interfere with editors at online outlets to prevent the publication of stories on certain topics and alter content that criticizes the government.[38](#) Journalists say that editorial decisions are heavily influenced by government forces—including police officers, army officers, and powerful political leaders—whose demands are colloquially known as "I say this." For example, two anonymous sources confirmed that during the 2017 presidential campaign, editors of Igihe, an online news outlet, were not allowed to publish articles on candidates that were challenging President Kagame. According to journalists interviewed anonymously, security officials often review journalists' stories and photos before they are published. One respondent said that authorities have tightened their control of the media by ensuring that each news organization employs a government representative to monitor editorial content.

Social media accounts with government affiliations regularly debate and harass individuals who post online comments considered critical of the government.[39](#) Progovernment accounts also mobilize to retweet and post positive comments in response to President Kagame's tweets, to project an image of widespread support. Through Itorero, a state-run traditional school of values, the government has mobilized social media users to counter the views of individuals deemed to be "enemies of the state." The so-called "Twitter Army" has systematically attacked and discredited individuals and media outlets that criticize the government. According to local sources, these social media users are rewarded for their attacks with access to jobs at government institutions and private companies that have ties to the ruling party. One source said that intelligence services monitor and report social media users who engage constructively with government critics.

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	13
---	----

Compared to their state-run counterparts, which receive income from government advertisements and direct subsidies, independent media outlets often struggle financially.<sup>40</sup> Large businesses generally only advertise with state-owned or progovernment media outlets, based on an unspoken rule.

B7 0-4 pts

Does the online information landscape lack diversity?	14
---	----

Government repression of the media greatly limits the diversity of the information landscape, both online and offline. Critical and independent online journalism produced by opposition supporters overseas—mainly in Europe, the United States, and South Africa—is blocked in Rwanda. Proxy servers can be used to access blocked content, but few Rwandans are aware of the extent of blocking or the means to circumvent it.<sup>41</sup>

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	36
---	----

Digital activism on political and social issues is uncommon, despite the widespread availability of mobilization tools. SIM card registration requirements have made users fearful of using digital tools for political activism that challenges the government (see C4).

## C Violations of User Rights

*In August 2018, the president signed into law a revised penal code, which prescribes prison sentences of five to seven years for defamation against the president and criminalizes “humiliating” state officials, although it decriminalizes defamation against private individuals. The Supreme Court struck down part of the law, but upheld criminal defamation against the president. A new cybersecurity law, also passed in August 2018, was expected to further restrict online expression.*

C1 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?	16
--	----

Rwanda's legal framework is used to restrict fundamental rights to freedom of expression, including online, despite constitutional protections. The Rwandan judiciary is not independent, and many journalists who publish material online view the threat of imprisonment as a key constraint on their work.

While a 2013 law provides for public access to government information,

implementation has been weak. Data published on Sobanukirwa, a website created by the government to ease the process of requesting access to documents, suggest that only a small fraction of requests result in positive and timely responses.

In April 2019, Rwanda's supreme court repealed a law that banned the publication of political cartoons, but upheld criminal defamation against the president ([see C2](#)). The decision draws an explicit distinction between the head of state and other public officials,[42](#) and was viewed as evidence of the judiciary's deference to the executive.

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	14
---	----

A number of laws restrict free expression and impose criminal and civil penalties for legitimate online activities.

A new cybersecurity law passed in August 2018 imposes up to five years imprisonment and a fine between 1 million francs (\$1,000) and 3 million francs (\$3,000) for publishing “rumors that may incite fear, insurrection or violence...or that may make a person lose their credibility.”[43](#) Additionally, anyone who “establishes, publishes, or uses a site of a terrorist group” faces imprisonment of 15 to 20 years and a fine between 20 million (\$20,000) and 50 million francs (\$50,000).[44](#) The government considers many exiled opposition organizations “terrorist groups,” which has contributed to concerns that the law will be used to further crack down on opposition activities.[45](#)

Defamation of the president is a criminal offense in Rwanda. Revisions to the penal code signed into law in August 2018 impose penalties of five to seven years in prison for defaming the president.[46](#) However, defamation against private individuals was decriminalized under the revised code. A provision in the code that criminalized the “humiliation of national authorities,” including through cartoons, was overturned by the Supreme Court in April 2019 ([see C1](#)).[47](#) Many other provisions in the revised penal code, often vaguely worded, contain undue restrictions on freedom of expression that can be applied to online activities. Notably, the spread of “false information or harmful propaganda with intent to cause a hostile international opinion against [the] Rwanda government” carries penalties of between seven and ten years in prison in peacetime and life imprisonment during wartime.[48](#)

An ICT law enacted in 2016 created a new legal and regulatory framework for the ICT sector and codified specific restrictions on internet activities that are antithetical to internet freedom.[49](#) Most notably, provisions in the law prohibit the dissemination of “grossly offensive” or “indecent” messages as well as the use of ICTs to cause “annoyance, inconvenience, or needless anxiety.” [50](#)

The law against “genocide ideology”—amended in October 2013—also threatens freedom of expression both online and off, prescribing heavy prison sentences of up to nine years and fines for any offender “who disseminates genocide ideology in public through documents, speeches, pictures, media, or any other means.”[51](#)

C3 0-6 pts

Are individuals penalized for online activities?	26
--	----

Citizens and journalists are periodically arrested for online activities in Rwanda, though the high degree of self-censorship practiced by online journalists and ordinary users alike has resulted in fewer arrests in recent years. Cases may also be underreported, given the government's strict control of the media.

In March 2019, Rwandan authorities arrested and detained a local journalist, Olivier Habimana for allegedly spreading rumors and propaganda against President Kagame through YouTube.<sup>52</sup> Habimana was still awaiting trial at the end of the coverage period. On similar charges, the authorities arrested in October 2018 Damascene Mutuyimana, Jean Baptiste Nshimiyimana, and Shadrack Niyonsenga, who are all journalists for Iwacu TV, a Kinyarwanda-language news broadcaster on YouTube.<sup>53</sup> They were still detained and awaiting trial at the end of the coverage period, though the trial will reportedly not start until 2022.<sup>54</sup>

In March 2018, a court sentenced blogger Joseph Nkusi to ten years in prison for incitement to civil disobedience and the spread of rumors. In 2016, Nkusi, who had lived in Norway since 2009, was deported following the rejection of his asylum application. Upon his return to Rwanda, he was immediately arrested and questioned about his political activities and blog postings, which were known for their sharp criticism of the Rwandan government. Nkusi had also reportedly founded a radical opposition group while living in exile in Norway and made false claims about the 1994 genocide, which is illegal under Rwanda's law against "genocide ideology."<sup>55</sup> He had written that both Hutus and Tutsis were targeted in a "double genocide."<sup>56</sup>

The authorities have used private conversations on mobile chat apps as evidence in prosecutions of dissidents, heightening concerns about the government's ability to intercept communications on social media platforms. In 2017, a few months after announcing her presidential election bid, Diane Rwigara was arrested, along with her mother Adeline and sister Anne (who was quickly released), for alleged tax evasion and incitement against the government.<sup>57</sup> Rwigara had been disqualified from running in the election, with the government claiming that signatures on her petition were forged.<sup>58</sup> At a pretrial hearing in October 2017, prosecutors presented WhatsApp audio messages allegedly taken from the mobile phones of Diane and Adeline as evidence against them.<sup>59</sup> The defendants had asked the judge to disregard the WhatsApp audio files as evidence, citing that they were obtained through phone interceptions.<sup>60</sup> The judges in the case acquitted the accused in December 2018 amid increased international scrutiny of the case, as well as a social media campaign for their release, which included a #FreeDianeRwigara campaign on Twitter.<sup>61</sup>

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	34
--	----

The ability to communicate anonymously is compromised by mandatory SIM card registration requirements in place since 2013.<sup>62</sup> Under the law, RURA has unfettered access to SIM card databases managed by operators, while other "authorized" individuals or institutions may also be granted access.<sup>63</sup>

In July 2018, RURA revised its regulations on SIM card registration, ostensibly to tackle fraud, including SIM boxing, identity theft, and phishing.<sup>64</sup> The revised regulations required individuals to present identification to receive a SIM card. In January, 2019, RURA announced that mobile phone users could not use more than

three SIM cards on each network. The new regulations required users to register each SIM card with their national identification by the end of the month. Foreigners can now use only one SIM card. RURA justified the regulations on security grounds, arguing that the proliferation of SIM cards had made it more difficult to track criminal activity.<sup>65</sup> Critics argue that the SIM card registration regulations are meant to collect users' data, since many people have evaded state monitoring by buying and registering SIM cards with false identities. The various legal provisions that enable surveillance and limit anonymity are particularly troubling in the absence of a comprehensive data protection law. A data protection provision is included in the ICT law passed in 2016, but it is limited by provisions that provide for broad national security exceptions.<sup>66</sup>

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	26
---	----

The extent of the authorities' surveillance capabilities is unknown, but there is a strong sense among observers that surveillance is pervasive. The government closely monitors social media discussions, as evidenced by the prevalence of progovernment commenters that frequently appear on social media platforms (see B5). Exiled dissidents have been attacked and murdered, despite their efforts to protect their identities, following threats from individuals inside or associated with the government.<sup>67</sup> In September 2018, the Citizen Lab, a Canadian internet freedom watchdog, reported that Rwanda is one of the 45 countries worldwide using Pegasus, a surveillance software developed by the Israeli technology firm NSO. Pegasus is frequently used by governments to surveil journalists, human rights defenders, and the opposition.<sup>68</sup>

In July 2018, the government passed a law that extended surveillance powers to a civilian institution, the Office of the Ombudsman, to investigate corruption-related crimes.<sup>69</sup> The law came into effect as part of the new penal code in September 2018.<sup>70</sup> Previously, interception powers were only held by security agencies such as the police, military, and intelligence services. The legislation was vague about whose communications could be intercepted. Press freedom advocates believe that the law could further threaten independent journalism (see C2). The interception of communications without the prior authorization of a judge is still legally permissible.

The 2013 Law Relating to the Interception of Communications expanded the government's surveillance powers, authorizing high-ranking security officials to tap the communications, including online activity, of individuals considered potential threats to "public security."<sup>71</sup> While the law requires government officials to apply for an interception warrant, warrants are issued by the national prosecutor, who is appointed by the justice minister. The national prosecutor can also issue warrants verbally in urgent security investigations, to be followed by a written warrant within 24 hours. The law also provides for the appointment of "inspectors" to ensure that authorized interceptions are carried out in accordance with the law, though the inspectors are appointed by the president and lack independence.<sup>72</sup> There is no requirement to justify surveillance as necessary and proportionate to a legitimate aim.<sup>73</sup>

In 2015, email leaks from the Italian surveillance firm Hacking Team revealed that the government attempted to purchase sophisticated spyware known as Remote

Control System (RCS) in 2012.[74](#) While the leaked emails did not confirm that a sale took place, they illustrate the government's interest in acquiring technology that can monitor and intercept user communications.

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	26
--	----

Under the 2013 Law Relating to the Interception of Communications ([see C5](#)), communications service providers are required to ensure that their systems have the technical capability to intercept communications upon demand. Security officials also have the power to “intercept communications using equipment that is not facilitated by communication service providers,” which de facto allows the authorities to hack into a telecommunications network without a provider's knowledge or assistance.[75](#)

In 2018, interviews with anonymous local sources confirmed that government representatives are systematically embedded within the operations of telecommunications companies for the purposes of surveillance. Telecommunications technicians also routinely intercept communications on behalf of the military.

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	35
---	----

Independent journalists frequently face violence and harassment when attempting to cover news stories. As a result, many journalists have fled the country.[76](#) Progovernment trolls regularly harass journalists and ordinary users on social media for posts that are critical of the authorities.

In May 2019, Fred Muvunyi, former chairperson of the Rwanda Media Commission, was subjected to online attacks by members of the ruling RPF following the publication of editorials in the *Washington Post* and Deutsche Welle that questioned Rwanda's Supreme Court decision to uphold the law on defaming the president.[77](#) Muvunyi's family in Rwanda has reportedly been harassed and intimidated by state operatives. The state-owned newspaper, the *New Times*, also published an editorial in May aimed at discrediting Muvunyi. [78](#)

In 2017, when Diane Rwigara announced her intention to run as an independent presidential candidate, photoshopped nude pictures of her were circulated online. Observers suspect that state agents were responsible for distributing the photographs in an effort to discredit Rwigara and discourage her from continuing her campaign against President Kagame.[79](#)

Extralegal violence against dissidents, including journalists and other government critics, creates an atmosphere of intimidation. In March 2019, opposition politician Anselme Mutuyimana was found murdered in a forest in northwestern Rwanda. The Rwanda Investigation Bureau (RIB) had not updated the public on the status of the investigation by the end of the reporting period. In October 2018, another opposition figure Boniface Twagirimana disappeared from his prison cell in Mpanga in Southern Rwanda. His whereabouts remain unknown up to date.[80](#)

## C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	23
---	----

Although some incidents of hacking and cyberattacks occur, the problem is not widespread. The cybersecurity law passed in August 2018 includes provisions that address hacking and other threats to online security ([see C2](#)). The law was passed during a period when hacking had increased. According to authorities, hackers most commonly target financial institutions. In 2018, the Central Bank recorded 22 separate hacking incidents.[81](#)

There were no reported technical attacks against online news outlets during the period under study. The last reported attack occurred in April 2014, when the investigative news site Ireme faced a seemingly targeted cyberattack from an unknown source