

— [Our Issues](#) [Countries](#) [Policy Recommendations](#) [Explore the Map](#)

FREEDOM ON THE NET 2020

South Korea

66

PARTLY FREE

/100

A. <u>Obstacles to Access</u>	22 /25
B. <u>Limits on Content</u>	24 /35
C. <u>Violations of User Rights</u>	20 /40

LAST YEAR'S SCORE & STATUS

64 /100 **Partly Free**

Scores are based on a scale of 0 (least free) to 100 (most free)

Overview

South Korea saw a moderate improvement in internet freedom, attributed to an easing of systematic content manipulation and the decline in prosecutions and convictions related to pro-North Korean online content. However, the country has also been criticized for its inadequate response to newer, digitally mediated forms of violence against women, girls, and children. Moreover, the COVID-19 pandemic allowed authorities to tap into broad



On South Korea

See all data, scores & information on this country or territory.

surveillance powers, giving them access to sensitive personal information without robust safeguards.

South Korea's democratic system features regular rotations of power and dynamic political pluralism, with the two largest parties representing conservative and centrist liberal views. Personal freedoms are generally ensured, although the country struggles with protecting rights for marginalized communities and social integration. The criminalization of defamation has also been known to affect legitimate political expression.

Key Developments, June 1, 2019 - May 31, 2020

- Service providers continued restricting a substantial amount of online content, mainly on the orders of the Korea Communications Standards Commission (KCSC). In 2019, 160,803 websites or pages were blocked and 34,995 were deleted, according to the commission's official report (see B1, B2, and B3).
- Unlike in previous years, systematic online content manipulation has eased, although disinformation and hyperpartisan content remain serious concerns (see B5).
- While online defamation cases continued to increase, prosecutions related to pro-North Korean content decreased considerably. Meanwhile, in January 2020, News and Joy, a small-sized online news outlet, was ordered by court to pay a compensation of 30 million won (\$25,400) to anti-gay activist groups for having described them as "fake news spreaders" in articles from 2018 (see C3).

[See More >](#)

Country Facts

Global Freedom Score

83/100

Free

Internet Freedom Score

66/100

Partly Free

Freedom in the World Status

Free

Networks Restricted

No

Social Media Blocked

No

Websites Blocked

Yes

Pro-government Commentators

No

Users Arrested

Yes

In Other Reports

[Freedom in the World 2020](#)

- During the COVID-19 pandemic, the 2010 Infectious Disease Control and Prevention Act allowed authorities to access broad amounts of sensitive personal data from credit card records, phone location tracking, and security cameras, without judicial oversight (see C6).
- Online gender-based violence continues to undermine people's ability to use the internet safely and freely. Newer and larger-scale digital crimes were reported, especially online grooming and sex trafficking of young girls through Telegram and cryptocurrency (see C7).

Other Years

2019

A. Obstacles to Access

South Korea's rates of broadband and smartphone penetration are among the highest in the world. The internet service sector is relatively diverse and open to competition, while the mobile market is subject to more state influence. Broadcasting and telecommunications activities are regulated by the Korea Communications Commission (KCC), and the content and ethical standards of these sectors are monitored by the Korea Communications Standards Commission (KCSC). Both commissions are chaired by presidential appointees.

A1 0-6 pts

<p>Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?</p>	<p>6/6</p>
--	-------------------

South Korea is one of the most connected countries in the world, in terms of both usage and connection speeds. Smartphone penetration was approximately 98 percent as of December 2019, **1** surpassing other advanced economies in global surveys. **2** An estimated 99.5 percent

of households had internet access in 2018, according to the Ministry of Science and ICT (information and communication technology). The most common methods for access in those households were wireless LAN, or local area network (100 percent), and mobile internet (99.9 percent). **3** According to the Inclusive Internet Index 2020 report, South Korea ranks first out of 100 countries surveyed for availability. **4**

A2 0-3 pts

<p>Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?</p>	<p>3/3</p>
---	-------------------

High-speed internet is relatively affordable. The Inclusive Internet Index 2020 report ranks South Korea 15th for affordability, defined by cost of access relative to income and the level of competition in the internet service market.

5 There is no significant digital divide with respect to gender or income, although there is a need for further improvement in access for the elderly and rural populations.

6 Roughly 70 percent of South Koreans live in cities dominated by multistory apartment buildings that can easily be connected to fiber-optic cables. **7**

A3 0-6 pts

<p>Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?</p>	<p>6/6</p>
--	-------------------

The government does not intentionally restrict connectivity. The country's internet backbone market is dominated by a small number of companies, with Korea Telecom (KT) as the largest provider. KT was founded as a state-owned

enterprise in 1981 and was privatized in 2002.

The network infrastructure is connected to the international internet, predominantly from the southern cities of Busan and Keoje, through international submarine cables extending to Japan and China. For national security reasons, the police and the National Intelligence Service (NIS) have oversight of the access points, but the government is not known to implement politically motivated restrictions on internet or mobile access. **8**

A4 0-6 pts

<p>Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?</p>	<p>5/6</p>
--	-------------------

The internet service market is relatively diverse and open to competition, with 96 internet service providers (ISPs) operating as of January 2019. Nevertheless, it is dominated by three companies: KT (40.7 percent of the market share as of April 2020), SK Telecom (25.7 percent), and LG Telecom (19.8 percent). The same firms control the country’s mobile service market, with 26.6 percent, 41.9 percent, and 20.8 percent of market shares, respectively. **9** All three companies are publicly traded, but they are part of the country’s *chaebol* system—a pattern of ownership characterized by large, family-controlled conglomerates that are connected to the political elite, often through marriage.

10 This has given rise to speculation that favoritism was at play in the privatization process and in the selection of bidders for mobile phone licenses. **11**

In 2019, amendments were made to the Telecommunications Business Act, whereby new “facilities-based telecommunications businesses” would only have to register with the Ministry of Science and ICT instead of

applying for a license, as was the case previously. It remains to be seen whether the change would lower entry barriers for the mobile service market in practice. **12**

A5 0-4 pts

<p>Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?</p>	<p>2/4</p>
--	-------------------

The Korea Communications Commission (KCC) regulates the sectors of broadcasting and telecommunications, while the Korea Communications Standards Commission (KCSC) monitors content and ethical standards. Both commissions, whose members are responsible to the president, have been criticized for the politicized appointments of their members and their lack of transparency.

The conservative government of President Lee Myung-bak (2008–13) created the five-member KCC in 2008. **13** The president appoints two commissioners, including the chair, while the National Assembly chooses the remainder. The sixth and current chairman is Han Sang-hyuk, appointed in September 2019. **14**

The first KCC chairman, Choi See-joong, was a close associate of former president Lee. **15** Choi resigned in 2012 amid bribery scandals and was later sentenced to two and a half years in prison and a fine of 600 million won (\$507,500) for influence peddling. **16** Lee pardoned him just before the end of his presidency. **17** In 2013, then president Park Geun-hye (2013–17) also named a close aide, four-term lawmaker Lee Kyeong-jae, to head the KCC. **18** He was succeeded by former judge Choi Sung-joon, who completed his term in April 2017. Subsequently, however, upon the request of the KCC, prosecutors launched an investigation in March 2018 into Choi's alleged preferential treatment of LG's mobile

operator during his term. He was cleared of the allegation in January 2020. ¹⁹ Following Choi, emeritus communication professor Lee Hyo-seong was appointed as chairman in August 2017 by the current president Moon Jae-in, despite strong objections from opposition parties. ²⁰ Lee resigned prematurely in July 2019, ahead of a large cabinet reshuffle.

Founded in 2008, around the same time as the establishment of the KCC, the KCSC monitors internet content and issues censorship orders to content hosts and other service providers (see B3). The KCSC's nine members are appointed by the president and the National Assembly.

²¹ Park Hyo-chong, a key figure in the country's neoconservative movement, led an all-male commission from 2014 to 2017. Former journalism professor Kang Sang-hyun chairs the current commission, which was formed in January 2018. The KCSC includes four subcommissions tasked with reviewing broadcasting, advertising, internet communications, and digital sex crimes, respectively. The fourth one was newly set up in August 2019. The internet communications subcommission evaluates online content flagged by a team of in-house monitoring officers, according to a former member, ²² and it also considers censorship requests from other agencies and individuals. The redacted minutes of their deliberations are released regularly on the KCSC website. Observers have criticized the commission's vaguely defined standards and broad discretionary power to determine what information should be censored, arguing that these allow commissioners to make politically, socially, and culturally biased judgments that often lack a legal foundation. ²³

B. Limits on Content

Although the internet environment in South Korea features

vibrant creativity, there are a number of restrictions on the free circulation of information and opinions. Website blocking and administrative deletion of posts are routinely conducted on the grounds that they are necessary to ensure national security or social order. The number of items restricted reached record highs in 2018. In February 2019, the government expanded its technical capacity by instituting SNI-based filtering of HTTPS—or “hypertext transfer protocol secure”—websites, which allows for more precise blocking of individual webpages. Systematic content manipulation eased during the coverage period, although hyperpartisan disinformation continued to spread.

B1 0-6 pts

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

3/6

Service providers continued blocking content that was deemed to violate the law or social norms, including threats to national security and public morality, mainly on the orders of the KCSC. **24** Political content, such as that praising North Korea, can also be subjected to blocking, according to Article 7 of the 1948 National Security Act. **25**

In February 2019, the KCSC confirmed that it added to its technical repertoire a controversial new method to block illegal content, specifically pornography and pirated material, accessed through HTTPS websites. **26** The new scheme uses Server Name Indication–filtering (SNI), which entails monitoring the unencrypted SNI that shows which HTTPS sites a user is visiting. **27**

The KCSC does not publish a list of blocked sites, but it does release the number of websites blocked under different categories of banned content. In 2019, a reported 160,803 websites or pages were blocked and 34,995 were deleted,

indicating a small decrease in numbers compared with the previous year. **28** Among those blocked, 27,270 were targeted due to “prostitution and obscenity,” 48,355 for “encouraging gambling,” 34,975 for promoting “illegitimate food and medicine,” 25,957 for “violating others’ rights,” and 24,246 for “violating other laws and regulations.” The last category includes content related to identity fraud, forgery, and organ trades. North Korean websites and content are also blocked. The KCSC ordered immediate blocking of 78 websites in January 2020 as per requests from police and national intelligence. **29**

B2 0-4 pts

<p>Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?</p>	<p>2/4</p>
--	-------------------

In addition to blocking, some political and social content is subject to removal, mainly through the KCSC’s orders.

In 2019, the KCSC had 34,995 items deleted. Of these, 6,904 for promoting “illegitimate food and medicine,” 17,786 for “prostitution and obscenity,” 80 for “violating others’ rights,” 24 for “encouraging gambling,” and 10,201 were targeted for “violating other laws and regulations.” **30**

Since the outbreak of COVID-19, the KCSC has concentrated its resources on containing the spread of fraudulent information that might otherwise “undermine the country’s pandemic response.” Between January 30 and March 16, 2020, the KCSC identified 350 items of “disinformation,” out of which it ordered 30 items to be blocked and 125 to be deleted, on the grounds of “disturbing the social order.” On March 4, the internet communications subcommission held an emergency meeting, upon the request of the then

Central Disaster Management Headquarters (under the Ministry of the Interior and Safety), and agreed on correction orders for 13 online posts. On March 11, the subcommission also issued correction orders for 13 posts claiming that President Moon had saluted the flag with his left hand. On March 12, it ordered deletion of another post claiming that the First Lady had been spotted wearing a mask made in Japan. These corrections were all made on the grounds of causing social disorder. The national union of journalists, among others, expressed concerns over the ambiguous criteria used in these decisions and the potential for abuse. **31**

Service providers that do not comply with KCSC orders face up to two years of imprisonment or a fine of up to 20 million won (\$16,900), according to Article 73 of the Act on Promotion of Information and Communications Network Utilization and Information Protection (the Network Act). Individuals, the police, and other government agencies can also instruct content hosts to remove content. On receiving a takedown request from individual users, a company must immediately hide the content in question for 30 days and delete it if the content owner does not revise it or appeal within that time, on the basis of Article 44(2) of the Network Act.

Moreover, under Article 44(3) of the same law, online intermediaries are encouraged to monitor and carry out proactive 30-day takedowns of problematic content, even without being prompted by complaints. **32** Companies that can demonstrate proactive efforts to regulate content would be favorably considered by the courts, while those that do not may be liable for illegal content posted on their platforms. **33**

In October 2019, the ruling party announced that it would

pursue amendments to the Network Act to be able to fine platform operators and domestic and foreign companies up to 10 percent of their annual turnover if they fail to moderate “fake news.” Civil society groups have expressed concerns over this pursuit, warning about the potential misuse and abuse of criminal laws to regulate information.

34

Separately, in May 2019, Ha Tae-kyeung, a legislator of the center-right Bareun Mirae Party, proposed an amendment to the Network Act to expand the definition of “illegal content” so that websites containing “anti-social, hate speech” can be censored more. The proposal included that a website should be shut down and the site owner should be sanctioned if 20 percent of its content contains such antisocial material, a category not clearly defined. Currently the criterion for a site being shutdown is if 70 percent of its content is illegal. **35**

B3 0-4 pts

<p>Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?</p>	<p>2/4</p>
---	-------------------

An expansive legal and administrative framework enables the authorities to restrict a broad range of content.

The process for ordinary users to appeal the KCSC’s censorship decisions is neither easy nor straightforward. Nevertheless, there have been cases in which orders are challenged in court. In 2017, the Seoul Administrative Court ruled in favor of British journalist Martyn Williams, who, with support from local nongovernmental organizations (NGOs), had appealed the KCSC’s blocking of his website, North Korea Tech, for allegedly violating Article 7 of the 1948

National Security Act. **36** The Seoul High Court later upheld the ruling. **37**

In addition to the Network Act, laws that can be invoked for content removal include the National Security Act, the Antiterrorism Act, the Public Official Election Act, and the Children and Youth Protection Act. Article 17 of the Children and Youth Protection Act places responsibility for removing child sexual abuse images on service providers, with possible penalties of up to three years of imprisonment or fines of up to 20 million won (\$16,900). In 2015, Lee Sir-goo, the then chief executive of the country's most popular mobile messaging application, KakaoTalk, was charged under this article with failing to take measures to stop the distribution of 745 videos featuring the sexual abuse of children and minors. Since holding a chief executive personally liable for user activity was unprecedented in South Korea, critics alleged that the charge was actually punishment for refusing to curb users' criticism of the government. **38** In June 2018, the Constitutional Court upheld Article 17, stating that service providers are legally obligated to prevent the circulation of child or juvenile sexual abuse images. **39** Nevertheless, the Suwon District Court acquitted Lee of the negligence charge in February 2019, even though it ruled that the technical measures put in place by KakaoTalk were indeed inadequate. **40**

B4 0-4 pts

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

3/4

Some users in South Korea self-censor to avoid reprisals for their speech, including criminal charges of defamation, which draws heavier penalties when committed online (see C2).

Resonating with the global #MeToo movement against sexual assault and harassment, survivors of such abuse in South Korea have used various social media platforms to reach a wider audience and advocate for social and legal changes. However, many survivors have self-censored to avoid being publicly shamed, fired from their jobs, or, most notably, sued for defamation (see also C7). **41**

B5 0-4 pts

<p>Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?</p>	<p>2/4</p>
--	-------------------

Score Change: The score improved from 1 to 2 due to less systematic manipulation of online content by the government, although hyperpartisan content and disinformation remains to be a cause for concern in the digital sphere.

While systematic online content manipulation has long been a concern for users in South Korea, such issues have eased in recent years. Hyperpartisan manipulation of content continues to be an issue.

The administration of former president Park, who was impeached on corruption charges in December 2016, was overshadowed from the beginning by investigations into the politicized manipulation of online comments by intelligence agents and military officials working to aid her victory in the 2012 election. Park denied ordering or benefiting from election manipulation. **42** In 2017, the High Court sentenced former director of the National Intelligence Service Won Sei-hoon to four years in prison for election interference. Won was first indicted in 2013, accused of authorizing agents to post thousands of online comments and 1.2 million

posts on Twitter characterizing members of the opposition as North Korea sympathizers. **43**

Similarly, in 2013, the Ministry of Defense’s cyber command unit, launched in 2010 to “combat psychological warfare in cyberspace,” stated that some officials had posted inappropriate political content online during the same period, but without the knowledge of the unit’s leaders. However, the ministry’s own investigation in the aftermath of Park’s impeachment confirmed that former minister of defense Kim Kwan-jin had mobilized the cyber command unit for smear campaigns against opposition candidates in the 2012 elections. **44** Kim was sentenced in February 2019 to two years and six months in prison for the manipulation operation. He has appealed to a higher court. **45**

Investigations surrounding the 2016 presidential corruption scandal revealed that online opinion manipulation was not limited to the 2012 election. Both Park’s administration and that of her predecessor, Lee Myung-bak, were found to have maintained a list of almost 10,000 artists, writers, and other cultural practitioners who satirized or criticized the two conservative governments. **46** Those on the list were defunded, professionally disadvantaged, or subjected to systematic online harassment. **47**

Current president Moon Jae-in, who took office in May 2017, lost an opportunity to distance himself from this decade-long history of online manipulation when a close ally, Kim Kyoung-soo, was accused of having worked with a group of bloggers to rig online support prior to the 2017 presidential election. **48** In January 2019, the Seoul Central District Court found Kim guilty of manipulating online comments, including using software to post over 99.7 million fraudulent “likes” and “dislikes” on social media content, to Moon’s advantage. **49** The case is being heard in an appellate court.

A report from the Oxford Internet Institute released in September 2019 confirmed previous revelations of content manipulation. The report identified South Korea as having previously actively coordinated “cyber troop” teams of less than 20 people to manipulate information on Facebook and YouTube on behalf of politicians and political parties. **50** The report found evidence that the teams had worked to support preferred messaging and attack the political opposition.

The government has signaled that it closely monitors so-called “fake news.” In October 2018, during a cabinet meeting, Prime Minister Lee Nak-yeon announced a crackdown on purportedly false news online, vowing to use the country’s criminal laws to curb what officials claim is “a threat to democracy.” **51** While there has been no evidence that legitimate content is being suppressed, critics are concerned that the “fake news” crackdown will limit free expression and make the government the arbiter of which online information is true or false. **52**

B6 0-3 pts

<p>Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?</p>	<p>3/3</p>
---	-------------------

There are no known economic or regulatory constraints that systematically hinder online content production and publication. However, small-sized publishers remain vulnerable to retaliatory lawsuits (see C3).

It was previously revealed that the Park Geun-hye and Lee Myung-bak administrations had secretly channeled funds to progovernment news outlets, civic groups, and websites. **53** No evidence of similar practices by the current government emerged during the coverage period.

Online platforms face general financial concerns to remain viable. Newstapa, a user-funded investigative journalism platform, has been faced with financial challenges under the current centrist-liberal government, as most of its donors are ardent supporters of President Moon and his Minjoo Party. Many have withdrawn their donations after the platform published reports critical of the government and the ruling party. **54**

In June 2020, after the coverage period, the government passed amendments to the Telecommunications Business Act, including a new Article 22(7) whereby, in short, service providers (both foreign and domestic) responsible for providing stable services. **55** A corresponding presidential decree clarifying how the amendments will be enforced was under consultation as of September 2020. Critics have raised concern that the changes create a “pay-to-play” regime that undermines net neutrality as content providers are likely to have the financial and technical burden to ensure quality data service over service providers. **56**

B7 0-4 pts

Does the online information landscape lack diversity?	3/4
---	-----

South Korea’s overall media environment is partly restricted yet relatively diverse. Alternative and activist media outlets have developed online in part to challenge existing restrictions. **57** The country is home to the first viable model of citizen journalism, OhmyNews, which has served as an inspiration to sites of a similar nature around the globe since 2000. **58** Newstapa has accumulated more than 30,000 regular donors and over 168 million views on its YouTube channel since its launch in 2012. **59** It was a leading source of information on the 2012 election manipulation

scandal, **60** and it was one of the first outlets to allege systemic corruption and negligence behind the sinking of the ferry Sewol in 2014, a disaster that resulted in 304 deaths.

B8 0-6 pts

<p>Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?</p>	<p>6/6</p>
---	-------------------

South Koreans have long embraced online technology for civic engagement and political mobilization, and online mobilization platforms and tools are freely available. The public's response to corruption allegations against then president Park Geun-hye between October 2016 and April 2017 was one of the country's most historic examples of digital mobilization. Hundreds of thousands of citizens participated in the campaign to pressure the government's legislative and judicial branches to bring the president and other suspects to justice. The will of citizens, expressed through social media and a sustained series of mass candlelight rallies, successfully led the more conservative mainstream media and legislators to endorse the removal of the president. **61**

South Korean women have continued to use the internet to foreground their experiences of gender-based discrimination and violence. From May to December 2018, thousands of women organized online and offline protests against “spycam porn,” or *molka* (meaning “hidden camera” in the Korean language). This epidemic problem involves small cameras that are hidden in various places—such as toilet stalls, subways, hospital changing rooms, and motels—to capture images of women without their consent. The images are then shared and consumed as entertainment and

pornography in various male-dominated online spaces (see C7). **62**

In response to the protests, the government and lawmakers amended Article 14 of the Act on Special Cases Concerning the Punishment of Sexual Crimes in November 2018, imposing harsher penalties for *molka* crimes on both those who collect the images and those who distribute copies (effective from December 2018).

Online petitions have also been used to raise awareness of other forms of gender violence. In February 2020, more than 100,000 people signed an e-petition for introducing a law to prevent online grooming and sex trafficking, committed through the secure messaging app Telegram and cryptocurrency. **63** Such petitions and campaigns across social media platforms led directly to a set of significant legal amendments for heavier punishment against digital sex crimes, especially ones involving minors, effective from June 2020. **64**

C. Violations of User Rights

Individual citizens have been charged with defamation or violation of other criminal laws for their online posts. During the coverage period, survivors of gender-based crimes continued to come forward and share their experiences, but they often faced negative repercussions in both their personal and professional lives. The privacy of countless women has also been violated through the epidemic practices of cyberstalking, nonconsensual sharing of intimate images, face-swap porn, and spy-camera porn, in which voyeuristic images of random victims are recorded and exploited. The COVID-19 pandemic allowed authorities

to tap into broad surveillance powers, giving them access to sensitive personal information without judicial oversight.

C1 0-6 pts

<p>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?</p>	<p>3/6</p>
--	-------------------

The constitution guarantees the freedoms of speech, the press, assembly, and association to all citizens, but it also enables restrictions, stating that “neither speech nor the press may violate the honor or rights of other persons nor undermine public morals or social ethics.” South Korea has an independent judiciary and a national human rights commission that have made decisions upholding freedom of expression. Nevertheless, the prosecution of individuals for online activities has a chilling effect and generates international criticism. Several laws restrict freedom of expression in traditional media as well as online (see C2).

C2 0-4 pts

<p>Are there laws that assign criminal penalties or civil liability for online activities?</p>	<p>2/4</p>
---	-------------------

A number of laws criminalize online activities. The 1948 National Security Act allows prison sentences of up to seven years for praising or expressing sympathy with the North Korean regime. The act applies both online and offline.

Defamation, including written libel and spoken slander, is a criminal offense in South Korea, punishable by up to five years of imprisonment or a fine of up to 10 million won (\$8,500), regardless of the truth of the contested

statement. Insult charges, which unlike defamation cases must be initiated directly by a complainant, are punishable by a maximum fine of two million won (\$1,700) or a prison sentence of up to one year. Defamation committed via ICTs draws even heavier penalties—seven years in prison or fines of up to 50 million won (\$42,300)—under the 2005 Network Act, which cites the faster speed and wider audience of online communications as a basis for the harsher sentencing. **65**

C3 0-6 pts

Are individuals penalized for online activities?	3/6
--	-----

Score Change: The score improved from 2 to 3 due to fewer prosecutions and convictions for violation of the National Security Act, although there remains thousands of cases for online defamation.

Criminal cases related to North Korean online content have reduced significantly in recent years, although thousands of people continue to be arrested for online defamation. The number of online defamation and insult cases increased from 13,348 in 2017 to 15,926 in 2018. **66** In 2019, between January and August, 12,432 cases were filed, out of which 8,653 led to arrests. **67**

Where cases involve politicians, the coverage period saw some positive developments for freedom of expression. In August 2019, congresswoman Na Kyung-won of the conservative United Future Party (UFP) filed online insult cases against 170 user accounts. The public prosecutors' offices did not indict in most cases, although some were still pending at the end of the coverage period. **68**

Similarly, in September 2019, a 35-year-old man named Cho

was cleared of an insult charge brought against him in 2017 for posting on a blog that Shim Jae-chul from the UFP was a “mental patient.” Cho was initially indicted by public prosecutors and fined one million won (\$850). **69**

A positive development has been that the current government has significantly reduced National Security Act-related prosecutions. **70** In 2018, only 1 percent of cases, both online and offline, led to prosecutions—a significant decrease from the 42.7 percent rate in 2014. The rate of prosecution has notably declined in contrast to the rising number of online posts blocked or deleted for violation of the National Security Act; from 1,137 in 2014 to 1,939 in 2018 (see B1 and B2).

During the COVID-19 pandemic, an increasing number of cases were reported and tried for spreading false information through social media. In June 2020, for example, the Daegu District Court sentenced an unnamed 33-year-old man to a suspended eight-month jail term with a two-year probation period and 80 hours of community service for “obstruction of business.” He shared in a group chatroom in February 2020 that a hospital in Gyeongbuk was going to have to close its emergency room because it was visited by a confirmed COVID-19 patient. **71**

Small-sized publishers remain vulnerable to retaliatory lawsuits. In January 2020, an online news outlet News and Joy was ordered by the Seoul Central District Court to pay compensation for damages after describing several anti-gay activist groups as “fake news spreaders” in their articles from 2018. The court did not dispute the facts in the articles, but it found the expression “fake news spreaders” to have damaged the claimants’ personality rights. The news outlet was ordered to pay 30 million won (\$25,400) as well as to retract the articles in question. **72**

The ruling against News and Joy was contradicted a month later. The far-right Christian organization Esther Prayer Movement filed a civil lawsuit in 2018 against *Hankyoreh*, a major center-left newspaper established in 1988, for describing the organization as a “fake news factory” in online stories. In February 2020, the Seoul Western District Court ruled in favor of *Hankyoreh*, stating that the defining characteristics of fake news are whether the information is based on actual facts and whether its propagators have certain intentions. The court concluded that the newspaper’s description was within reason. **73**

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	2/4
--	-----

There are some limits on anonymous communication, although a problematic real-name system was largely dismantled in 2012. First adopted through a 2004 amendment to the Public Official Election Act, **74** the system required users to submit their Resident Registration Numbers (RRNs) in order to join and contribute to major websites. The RRN is a 13-digit number uniquely assigned to each South Korean citizen at birth. In 2007, the system was applied to any website with more than 100,000 visitors per day under Article 44(5) of the Network Act. The Constitutional Court ruled Article 44(5) unconstitutional in 2012, because it renders individuals vulnerable to cyberattacks, among other factors. **75** Under 2013 amendments to the Personal Information Protection Act, website administrators are prohibited from collecting RRNs, and failure to protect an individual’s RRN is punishable by fines of up to 500 million won (\$422,900). **76**

Mobile service providers still require users to submit their

RRNs, and some other registration requirements remain in place. In 2015, the Constitutional Court upheld clauses of the Public Official Election Act that require people to verify their real names before commenting online during election periods (23 days before a presidential election and 14 days before a general election). **77** Other laws, such as the Children and Youth Protection Act, the Game Industry Promotion Act, and the Telecommunications Business Act, separately require internet users to verify their identities. **78**

C5 0-6 pts

<p>Does state surveillance of internet activities infringe on users' right to privacy?</p>	<p>2/6</p>
---	-------------------

Government surveillance of online activity has been a concern in South Korea. When visiting the country in July 2019, the UN special rapporteur on the right to privacy, Joseph Cannataci, confirmed allegations of state surveillance from 2016. He noted improvements among state agencies since 2017, but called on the government to establish an independent oversight body to minimize additional surveillance abuses. **79**

Some cases in recent years have raised questions about how the authorities gain access to personal data. According to the 2019 Korea Internet Transparency Report by the Clinical Legal Education Center (CLEC) at Korea University, police and other investigative agencies searched more than 8.3 million Naver or KakaoTalk accounts in 2018. The report noted that affected users were often not notified until after the search, and the notification could even be further delayed at the discretion of the director of the investigation. **80**

80

During a state audit in October 2019, it was revealed that

approximately 5,000 police officers had been accessing the database of Duplication Information (DI) without warrants over the previous ten years. A unique identifier of an individual online user, DIs have been used by service providers to prevent duplicate registrations since the introduction of a ban on collecting users' RRN (see C4). **81**

The National Intelligence Service (NIS), the country's main spy agency, has been at the center of major surveillance scandals in recent years, including the use of surveillance software—purchased from the controversial Italian company Hacking Team—on domestic mobile devices and KakaoTalk under the previous government. **82** For example, the NIS, the police, and the Defense Security Command monitored the families of victims of the 2014 Sewol ferry disaster. **83**

A 2016 antiterrorism law enables the NIS to access individuals' travel records, financial records, private communications, location data, and any other personal information for terrorism investigations, based on suspicion alone and without judicial oversight. **84**

C6 0-6 pts

<p>Are service providers and other technology companies required to aid the government in monitoring the communications of their users?</p>	<p>3/6</p>
--	-------------------

Court-issued warrants are required to access the content of private communications, but the NIS, police, public prosecutors' offices, and other investigative agencies may request users' metadata from service providers without a warrant under Article 83(3) of the Telecommunications Business Act. The government publishes the number of times data was provided to investigative agencies based on these requests, but digital rights advocates say the figures

may be misleading, since one request can affect many individuals over a long period of time. **85** According to an official press release, in 2019, service providers fulfilled 6,024,977 requests for metadata (a 1.9 percent decrease compared with the previous year) and 448,352 requests to access the logs of private communications (a 19.2 percent decrease). **86** Metadata in this context includes the user's name, RRN, postal address, telephone number, user identification, and dates of joining or leaving the service, while logs document who the user spoke with and for how long. Unlike in previous coverage periods, there were no reports of government critics being targeted.

There is limited transparency surrounding official requests for communications data, and courts have reinforced this lack of openness. Service providers have a legal duty to inform the targets, but they have been criticized for failing to do so. **87** Open Net Korea, an NGO that advocates for a free and open internet, filed a tort claim against the government in 2016 over warrantless access to citizens' personal information, but the claim was rejected by a court in December 2018. **88**

In the context of the government's COVID-19 response, the 2010 Infectious Disease Control and Prevention Act (IDCPA) **89** provides authorities with broad surveillance powers. Officials have accessed personal data from credit card records, phone location tracking, and security cameras all without court orders. They have paired the data with personal interviews for rapid contact-tracing and monitoring of actual and potential infections. Importantly, IDCPA requires information collected to "be destroyed without delay when the relevant tasks have been completed," **90** but criticisms have been raised over excessive data collection. In some cases, officials have publicized online the gender, age range, and movements of

patients, fueling online ridicule, scrutiny, and social stigma.

In January 2020, amendments to the country’s three major data privacy laws (Personal Information Protection Act, the Network Act, and the Credit Information Use and Protection Act) were passed so as to reduce the scope of protected personal data. The amendments allow for more third parties to better access users’ private information. The government claims the amendments seek to encourage more “research and innovation,” in the broadest senses of the terms. ⁹¹ Civil liberties organizations have raised strong concerns over the potential privacy violations of the amendments, ⁹² which came into effect in August 2020, after the coverage period.

C7 0-5 pts

<p>Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?</p>	<p>3/5</p>
---	-------------------

During the coverage period, gender-based discrimination and harassment continued, and women were targeted after sharing, subscribing to, following, or even “liking” feminist messages and images on social media. ⁹³

Women developers and artists in the gaming industry have been particularly vulnerable to such discrimination. According to a June 2018 *Hankyoreh* report, at least 10 women in the gaming industry were fired between March and April 2018 for their alleged affinity with Megalia, an online feminist community that no longer existed. ⁹⁴ In November 2019, a freelance illustrator was fired from her work with a mobile game company for having supported on social media—in 2016—voice actress Kim Jayeon after Kim was fired for her feminist post on Twitter. ⁹⁵

South Korean women have also experienced widespread violations of their rights to privacy, safety, and dignity. The coverage period was marked by new and more dramatic revelations about the epidemic phenomenon of “spycam porn” (see B8) and digitally mediated sex trafficking. ⁹⁶ In March 2019, it was reported that about 1,600 guests in motel rooms in 10 South Korean cities had been filmed by hidden cameras. The videos were live streamed on a pay-per-view porn site. ⁹⁷ In the spring of 2019, several showbiz celebrities were arrested for sharing *molka* videos and conspiring to commit date rape in KakaoTalk chatrooms. ⁹⁸ There has also been a proliferation online of pornographic images that were created using face-swapping tools. The composite images are meant to humiliate everyday women.

99

There have been arrests and prosecutions resulting from such egregious online gender-based violence. In March 2020, Cho Ju-bin was arrested and charged for violating the Child Protection Act, the Privacy Act, and the Sexual Abuse Act. He allegedly created and ran multiple large Telegram chatrooms to blackmail women and illegally produce, trade, and buy sexually dehumanizing footage of 74 people, including 16 underage girls. ¹⁰⁰ At least 10,000 people used the chatrooms, with some paying up to \$1,200 in bitcoin for access. ¹⁰¹ Over 2 million people signed an online petition to disclose all the suspects’ identities, largely out of frustration, especially among women, that digital sex crimes carry disproportionately light penalties. ¹⁰² In March 2018, Son Jong Woo was arrested in March 2018 for running “the world’s largest darknet marketplace” for child sexual abuse imagery, according to a US federal grand jury’s indictment. ¹⁰³ He was sentenced in May 2019 in Korea to 18 months in prison.

C8 0-3 pts

<p>Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?</p>	<p>2/3</p>
---	-------------------

According to statistics provided by the National Police Agency's Cyber Bureau, businesses and NGOs have reported a rise in the number of cyberattacks, from 175 cases in 2014 to 418 in 2019. ¹⁰⁴ Reported violations of electronic personal data tripled between 2010 and 2013, from 54,832 incidents to 177,736. However, in 2019 the number decreased to 159,255. ¹⁰⁵

South Korean officials had previously alleged that the North Korean government was responsible for cyberattacks on major banks and broadcasting stations in 2013, ¹⁰⁶ attacks on nuclear power plants in 2014, ¹⁰⁷ and an attack that seized control of a large university hospital network for eight months in 2015, ¹⁰⁸ among many other incidents. In December 2018, the personal information of nearly 1,000 North Korean defectors in South Korea was stolen through a computer infected with malicious software. The Ministry of Unification launched an investigation to determine who perpetrated the breach, declining to comment on whether North Korea was behind it. ¹⁰⁹ The intrusions have highlighted vulnerabilities in the country's ICT infrastructure.

¹¹⁰

Footnotes

- 1 "Number of smartphone subscribers" [Korean,] IT Statistics of Korea, accessed December 2019, <http://www.itstat.go.kr/m/stat.it?no=1149>.
- 2 Kyle Taylor & Laura Silver, "Smartphone ownership is growing rapidly around the world, but not always equally," Pew

Research Center, February 5, 2019,
<https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-g...>

“2018 survey on the internet usage: Summary report”
[Korean,] Ministry of Science and ICT, February 24, 2019,
https://www.kisa.or.kr/eng/usefulreport/surveyReport_View.jsp?cPage=1&p...

“Availability rank: South Korea,” The Inclusive Internet, The
Economist Intelligence Unit, January 2020,
<https://theinclusiveinternet.eiu.com/explore/countries/KR/?category=ava...>

**Be the first to
know what’s
happening.**

“Availability rank: South Korea,” The Inclusive Internet, The
Economist Intelligence Unit, January 2020,
<https://theinclusiveinternet.eiu.com/explore/countries/KR/?category=aff...>

Join the Freedom House
monthly newsletter
More footnotes

Email

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org

@2020 FreedomHouse