Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**511**
Land:	Sudan
Kilde:	Freedom House
Titel:	Freedom on the net 2020 - Sudan
Udgivet:	14. oktober 2020
Optaget på baggrundsmaterialet:	7. januar 2021

Freedom House

Sudan

FREEDOM ON THE NET 2020

30
/100

NOT FREE

A. Obstacles to Access	5 /25
B. Limits on Content	15 /35
C. Violations of User Rights	10 /40

LAST YEAR'S SCORE & STATUS
25 /100 Not Free

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

Overview

Internet freedom in Sudan has improved under the reforms of a technocratic cabinet led by Abdalla Hamdok, the first civilian prime

minister to serve since former president Omar al-Bashir came to power in a 1989 coup. The cabinet governs alongside the Transitional Sovereign Council (TSC), the civilian-military transitional government that assumed control from the Transitional Military Council (TMC), a short-lived military junta, in August 2019. The TSC's interim constitution, the Sudan Constitutional Charter, safeguards rights and freedoms, including freedom of expression, freedom of the press, and the right to access the internet, and the transitional government has signalled it will liberalize the regulatory environment. The practical extent of these reforms remains to be seen, as Sudanese internet users continue to face arrest, harassment, and intimidation for their online activities.

The military leaders and civilian protesters who ousted the repressive regime of former president al-Bashir and his National Congress Party (NCP) in April 2019 are uneasy partners in the transitional government that—if successful—will be replaced by an elected government in 2023. Civic space is slowly opening to individuals and opposition parties, but security personnel associated with the abuses of old regime remain influential, and their commitment to political freedoms and civil liberties is unclear.

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

- Multiple connectivity restrictions were reported, including a 36-day shutdown that followed the killing of 127 protesters in Khartoum by security forces in June 2019 (see A3).
- The transitional government made changes that may strengthen the autonomy of the country's telecommunications regulator, appointing a new head of the regulator in July 2019 and removing it from the defence ministry's purview that September (see A5).
- Troll armies affiliated with the ousted al-Bashir regime reportedly spread disinformation about the COVID-19 pandemic online, in an apparent effort to destabilize the transitional government (see B5).

- Social media platforms again served as spaces for protesters to mobilize during the coverage period, after the online environment was previously constrained by social media blocks and internet shutdowns (see B8).
- The transitional government's interim constitution, which enshrines freedom of expression as well as the right to access the internet, was published in August 2019 (see C1).
- Systemic state harassment of online activists subsided during the coverage period, though internet users faced continued intimidation and harassment from security forces and other ordinary users (see C7).

A. Obstacles to Access

The government imposed a 36-day internet shutdown in June and July 2019, after security forces killed 127 protesters in the capital city of Khartoum. A two-day shutdown was reported in the city of Kassala in May 2020 and Port Sudan in August 2019, both times following fatal clashes between Beni Amer and Nuba tribespeople. Electric infrastructural issues limited internet access even as Sudanese people increasingly worked online due to the COVID-19 pandemic.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**1** / 6

Internet penetration remains low, with 30.9 percent of individuals using the internet as of 2017, according to the International Telecommunication Union (ITU). [1] The ITU also reported that as of 2018, less than 1 percent of the population had a fixed-broadband subscription. [2] Meanwhile, the 2018 GSMA Mobile Connectivity Index reports that 39 percent of the population has a mobile broadband connection. [3] However, these figures are based on the total number of SIM cards, so the reported penetration rate may be inflated by individuals who have multiple SIM

cards. Nevertheless, the available data suggests that most internet users have mobile subscriptions.

An unreliable electricity supply limits internet service in Sudan, including in major cities that have been subject to periodic power rationing due to electricity price increases. Most rural areas have unsteady access to electricity or none at all. Power cuts usually peak in the summer when demand for electricity is highest, especially in Khartoum, where a growing population and severe weather have intensified demand. Khartoum accounts for approximately 70 percent of the country's electricity usage. [4]

Sudan encountered severe power rationing between February and April 2020 as maintenance on two power stations was performed. The country's dams, meanwhile, did not function at full capacity due to low water levels during the summer. [5] Most households and businesses experienced power outages, some lasting as along as 12 hours. [6] As many of Sudan's cell towers lack backup generators, these power cuts often limited internet access, particularly affecting those working remotely due to the COVID-19 pandemic. [7]

Blackouts previously occurred in January and February 2019, allegedly due to technical issues. [8] However, many observers suspect that the blackouts were intentional and meant to disrupt the protests against the regime. Another outage occurred in April 2019 (see A3).

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?	**0** / 3

Internet access is prohibitively expensive for many users, and the economic crisis increased relative prices further during the coverage period.

In a continuation of the economic deterioration that began in 2011, sustained petroleum scarcity led to inflation and higher prices in 2020. [1]

Sudan's inflation rate remained high, at just over 99 percent in May 2020. [2] The central bank imposed limits on cash withdrawals during the reporting period, [3] further limiting citizens' ability to pay for goods, including internet service.

A month of fixed-line internet service can cost nearly half the average monthly income in Sudan. [4] In August 2019, telecommunications companies reportedly raised internet subscription fees by 15 percent. [5]

According to a survey conducted by Afrobarometer in 2018, women in Sudan are nine percent less likely to access the internet regularly than men. In 2013, the same survey reported a five-percent gender gap. [6]

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**1** / 6

The government frequently exercises control over the internet infrastructure, and internet access was shut down for over a month as antigovernment protests were held in June and July 2019.

Mobile internet services were suspended for three days in May 2020 in the city of Kassala. Activists suggested that the Kassala state government restricted connectivity in order to maintain calm during a TSC delegation visit. A week before, clashes between Nuba and Beni Amer tribespeople left 11 people dead. Residents using mobile service providers Zain and MTN were chiefly affected, although the shutdown may have affected other providers. Fixed-line internet services were not affected. [1]

Internet connectivity was also restricted for several days in Port Sudan in August 2019. The city had been placed under curfew after dozens of people were injured and killed amid violent clashes between Beni Amer and Nuba tribespeople in the region. [2]

Sudan experienced a near-total network shutdown, lasting 36 days, between early June and July 2019. [3] In early June, security forces

attacked a peaceful protest in Khartoum, killing 127 people, injuring hundreds more, and sexually assaulting dozens. [4] The timing of the shutdown limited the spread of information about the massacre on the internet, including evidence of abuses perpetrated by security forces. [5] During the shutdown, internet services were intermittently available via some Canar Telecom and Sudan Telecom Company (Sudatel) ADSL fixed-line connections. [6] Canar Telecom and Sudatel services are often used by government offices, but because both providers rely on expensive fiber-optic infrastructure, very few individual users can afford their services. [7] Some Sudanese internet users reported that they sought to purchase fixed-line connections from Canar Telecom and Sudatel during the shutdown, but were told that the companies had run out of stock, possibly indicating that the authorities sought to limit internet access. [8]

In July 2019, after the internet shutdown, the Khartoum District Court ordered Zain to resume internet services. [9] That same month, a Zain executive disclosed that the company restricted internet services under orders from the Telecommunications and Post Regulatory Authority (TPRA), the Sudanese telecommunications regulator (see A5). [10] In September 2019, a court ruled that Sudatel and MTN could be sued by their subscribers for the June shutdown and ordered the companies to apologize to their subscribers. [11]

Internet service providers (ISPs) blocked [12] WhatsApp, Facebook, Twitter, Periscope, and Instagram [13] from December 2018 through February 2019, according to the digital rights organization NetBlocks. [14] The block was instituted less than a week into nationwide protests that began in December 2018. Users were able to access the blocked social media and messaging platforms through virtual private networks (VPNs), which users could generally only download with a strong wireless connection. NetBlocks stated in a study that Zain had the most “extensive blocking scheme” among providers. [15] Users reportedly lost internet connectivity a day after the mass protests erupted in Khartoum that December. [16] Multiple electricity outages in January and February 2019 coincided with the protests and social media block, raising concerns that the outages were intentional.

In early April 2019, a day after hundreds of thousands of protesters marched to the army's headquarters in Khartoum, social media platforms were again blocked, including Telegram, which is widely used by activists and remained accessible during the initial December-to-February block. [17] Several widely used VPN platforms such as Hotspot Shield, ExpressVPN, and others were reportedly blocked. Users struggled to find a VPN to download. [18] The block was lifted on April 11th, the day al-Bashir was ousted in a coup. [19]

A power outage on April 7th, 2019 coincided with mass protests and the social media block. NetBlocks reported that a few hours after the social media block was reported, 45 percent of telecommunications services were disabled by power outages that affected mobile service providers and fixed-line internet services. [20] The Ministry of Water Resources, Irrigation and Electricity did not provide an explanation for the blackout. [21]

Sudan is connected to the global internet through international gateways controlled by the partly state-owned Sudatel, Zain, and Canar Telecom, which are in turn connected to five submarine cables: Saudi Arabia-Sudan-1 (SAS-1), Saudi Arabia-Sudan-2 (SAS-2), Eastern Africa Submarine System (EASSy), FALCON, and Africa-1, the largest cable.

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**3** / 6

There are no legal or regulatory obstacles that restrict the diversity of service providers, but there are economic constraints. Canar Telecom, one of the four licensed telecommunications providers in Sudan (offering fixed phone and home internet service) was partially owned by the Emirati mobile service provider Etisalat. However, Etisalat sold its shares in the company to the Bank of Khartoum for $95 million in 2016. [1] The bank used its 3.7 percent share in Canar to block Zain's efforts to purchase it. [2] Observers believe that the government's move to increase its market share in the telecommunications industry will have a negative impact on internet freedom and reduce the dynamism in the market.

Three other licensed telecommunications providers operate in Sudan: Zain, MTN, and Sudatel. MTN and Zain are primarily foreign owned. [3] The government owns more than a 20-percent share in Sudatel [4] and reportedly has significant sway over the company's board of directors. [5]

Zain also has some apparent links to the government. According to a local source, Zain Sudan appointed Osama Kahin as its new general manager in April 2019. Kahin is seen as an independent figure, unlike his predecessor, Al-Fatih Erwa, who is a former security officer. Erwa remained in the company, but due to his former positions in the security apparatus, his profile will be much lower.

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?	**0** / 4

The regulatory bodies that oversee service providers historically lacked independence, though recent changes may indicate movement toward autonomy. The TPRA, which replaced the National Telecommunications Corporation (NTC) in 2018, [1] is tasked with regulating internet use and telecommunications licensing, facilitating competition, producing telecommunications statistics, and developing the telecommunications and information technology industries. [2] It is also responsible for determining what content is accessible on the internet (see B3). [3]

In July 2019, the TMC appointed Major General Sadiq Jamal al-Deen al-Sadig as the head of the TPRA, [4] replacing Mustafa Abdel Hafeez, who was appointed director of the NTC in December 2018. [5] In September 2019, the TSC separated the TPRA from the Ministry of Defense and brought it under its direct administration; previously, the TPRA was under the Ministry of Information.

The decisions to place the TPRA under the purview of the Ministry of Defense, and then the TSC itself, were met with criticism, as the body has the power to engage in surveillance and shut internet access. The telecommunications sector generates significant revenue for the

government, as well; in 2015, the NTC collected $560 million in taxes imposed on the industry. [6]

B. Limits on Content

Social media platforms remained unblocked during the coverage period and pornographic websites reportedly became accessible for the first time in years. Activists returned to social media in the aftermath of the December 2018 social media blocks and June 2019 internet shutdown, which left some people hesitant to mobilize online. Troll armies affiliated with the al-Bashir regime are reportedly active in disinformation campaigns surrounding COVID-19 with the goal of destabilizing the transitional government.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	**5** / 6

Score Change: The score improved from 3 to 5 because the extensive social media blocks imposed in December 2018 were not repeated during the coverage period.

The government did not block social media platforms during the current coverage period, while the extent of content blocking under the transitional government is unclear.

The now-ousted al-Bashir regime openly acknowledged blocking and filtering websites that it considers “immoral” and “blasphemous.” Political or social content was blocked in 2012, when the online news outlet SudaneseOnline and Facebook were intermittently inaccessible, and the “Innocence of Muslims” YouTube video was blocked. Pornographic websites reportedly became accessible in Sudan in 2019; the authorities previously blocked most pornographic content.

Previously, social media blocks enacted in December 2018 (see A3) curtailed the sharing of political and social content during the mass

protests that began that month. Social media was instrumental in organizing demonstrations against the al-Bashir regime and the TMC (see B8). Blocking social media platforms was intended to disrupt the ability to access information related to the protests.

Many internet users were able to access social media through VPNs. Many users without VPNs on their phones paid specialists at technology shops throughout Sudan to install them. In April 2019, a number of free VPNs, such as Hotspot Shield, became inaccessible, which forced some users to again pay for the installation of VPNs that remained available. [1]

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?	**2** / 4

The Sudanese government does not systematically use legal or administrative means to force publishers and content hosts to delete legitimate content. Instead, the authorities use intimidation to coerce internet users to delete content (see C7). This practice became more common after the protests began in December 2018 and continued into June 2019, though the practice then reportedly subsided.

However, in May 2020, security forces threatened and intimated journalists Lana Awad and Aida Abel Qader (see C7). The journalists published reports, including on Facebook, [1] about high death rates among elderly people in North Darfur hospitals as the COVID-19 pandemic took hold. [2] The General Intelligence Service (GIS) and individuals affiliated with the government harassed and intimidated users to delete content they objected to from Facebook groups. [3]

Prepublication censorship has been prevalent in previous years. In early 2019, *Al-Jareeda*, one of Sudan's few independent newspapers, was repeatedly confiscated or banned from publishing. Although the newspaper continued to publish on its website and Facebook page, authorities also threatened to shut down its online presence. The paper continued to publish online despite those threats. [4]

B3 0-4 pts

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

The TPRA still has not disclosed details about the 2018 social media blocks and network shutdowns. In December 2018, National Intelligence and Security Service (NISS) head Salah Abdallah admitted that the government was responsible for blocking social media platforms, but the NTC did not provide further information about the decision. [1]

Under the al-Bashir regime, the TPRA managed online censorship through its internet service control unit. The regulator previously acknowledged that 95 percent of blocked material is related to pornography, [2] though it also acknowledged that it has not succeeded in blocking all "negative" sites in Sudan. [3] The TPRA additionally requires cybercafé owners to download blocking and filtering software. [4]

The authority's website gives users the opportunity to submit requests to unblock websites "that are deemed to not contain pornography," [5] but it does not specify whether the blocking of political websites can be appealed. Users attempting to access a blocked site were met with a page stating, "This site has been blocked by the National Telecommunications Corporation," which included links to further information and a contact email address. [6] In addition to the TPRA, the general prosecutor has the power to block any site that threatens national security or violates social mores. [7]

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Government threats against online journalists and internet users have led to growing self-censorship in recent years. Ordinary internet users have become more inclined to self-censor to avoid government surveillance

and arbitrary legal penalties. They also rely on anonymous communication to speak candidly. WhatsApp, for example, is particularly popular in Sudan due to the platform's privacy and anonymity features. [1] Telegram was also widely used during antigovernment protests in early 2019. [2]

Many journalists writing for online platforms also publish anonymously to avoid prosecution.

With the transitional government's formation, journalists and commentators who were blocked from appearing on television or in newspapers by the al-Bashir regime, and who were exclusively working online since, have returned to other forms of media.

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?	**0** / 4

While Sudan has a vibrant online media landscape, the government has frequently manipulated internet content to advance its agenda, spreading disinformation and manipulating social media discussion through a so-called cyberjihadist unit. [1] This unit was established under the NISS's purview in 2011, and proactively monitored content posted on blogs, social media platforms, and online news forums. The unit collected information about dissidents and reportedly orchestrated technical attacks against independent websites, especially during political events (see C8). In 2019, the unit was especially active on Facebook and Twitter, using human-run accounts to target opposition figures and protesters through harassment. [2] As part of its work, it also sought to report target accounts for violating community standards of social media platforms, which sometimes lead to their closure or suspension. The unit also sought to sway public opinion by flooding platforms with coordinated posts, hashtags, and messages. [3]

The unit also spread "fake news" to muddle debate and discredit independent news outlets and analysts who unknowingly circulated false

stories. In January 2019, reports surfaced that three people were killed when police used live ammunition to disperse a protest in Khartoum. However, an image purportedly showing the aftermath was actually taken in Brazil; Sudanese activists asserted that the story was planted in an effort to discredit organizations that disseminated it, [4] including the Central Committee of Sudan Doctors and Sudan Change Now. Similar tactics were used in an effort to thwart the 2018 "bread protests," which were prompted by the government's handling of the economy and proposed tax increases. During these protests, cyberjihadists spread misinformation that the protests were meant to destabilize Sudan.

After the al-Bashir regime's ouster, the Khartoum Electronic Media Center, which housed the unit, closed its website and social media pages. The unit reportedly maintains offices in Khartoum as well as a presence in countries including Turkey and Qatar. [5] Fraudulent pictures, videos, and stories were notably circulated on social media platforms during the coverage period. [6]

The cyberjihadist unit has engaged in disinformation campaigns surrounding COVID-19, reportedly sharing stories claiming that the virus has not reached Sudan and that the transitional government was using the pandemic lockdown to stifle dissent. The unit reportedly sought to mobilize people to protest the lockdown. [7]

Campaigns originating in Russia have also targeted Sudanese internet users. In October 2019, Facebook reported that it removed a network of Facebook accounts, pages, and groups, along with Instagram accounts, that focused primarily on Sudan. The Russia-based network distributed content, including false and misleading information, about events in Sudan and Russia, occasionally criticizing Sudanese protesters. Over 450,000 Facebook accounts and about 3,000 Instagram accounts followed pages and groups within the network, which was active as early as mid-2018. [8] A July 2019 report from the Carnegie Endowment found that Russian disinformation campaigns sought to shape perceptions of Sudan's democratic transition, particularly through state-affiliated media targeting Sudanese audiences with content critical of prodemocracy protesters. [9]

During the COVID-19 pandemic, false information about the virus spread online, including myths about immunization through traditional remedies. Health authorities reported that people who incorrectly believed they were immune because of such myths made containment strategies less effective. [10]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**0** / 3

There are a number of economic and regulatory constraints that negatively affect users' ability to publish content online. Tight government control of the media environment has prevented independent online news outlets and journalists from becoming economically viable. Polarization further constrains the development of sustainable independent journalism. [1]

In February 2020, the government appointed Lukman Ahmed, a former BBC journalist, as director of the Sudanese General Corporation for Radio and Television Transmission. [2] The corporation primarily regulates broadcast media, which are also an important source of news in the online media space. Ahmed and other officials indicated that they would seek to liberalize the media environment and reduce state control of broadcasters. [3]

In January 2020, the TSC closed two newspapers, *Al-Sudani* and *Al-Rai al-Am*, and two satellite channels, Al-Shorouk and Taiba TV, citing a need to recover state funds and alleging corruption. The four outlets purportedly received funding from the al-Bashir regime. [4] Al-Shorouk began broadcasting again in April 2020. [5] *Al-Sudani* and Al-Shorouk had popular digital media platforms; Al-Shorouk in particular served as an archive of decisions by the government and extensively covered digital media and cybercrimes.

Amendments to the Media Law passed in 2018 (see C2) require online news outlets to register with the Journalism Council, which has the power

to suspend publications and prevent online journalists from posting content it objects to. [6] As registered outlets, online publications are required to have a physical office, which many news sites previously avoided due to security and financial concerns. [7]

According to a local source, numerous news sites were financed by the al-Bashir government, such as Al-Nileen. As of June 2020, several news sites are now funded by businesspeople and donors. In 2017, a news site called Bajnews became the first online publication founded and funded by a businessperson in Sudan.

B7 0-4 pts

Does the online information landscape lack diversity?	**2** / 4

Compared to the highly restrictive space in the traditional media sphere, which is characterized by prepublication censorship, confiscations of entire press runs of newspapers, [1] and warnings from GIS agents against reporting on certain taboo topics, [2] the internet remains a relatively open space for freedom of expression. Many voices express discontent with the government on various online platforms. Online news outlets such as Al Tareeq, [3] Al Taghyeer, [4] Radio Dabanga, [5] Hurriyat, and Al Rakoba cover controversial topics such as corruption and human rights violations.

Facing heavy censorship, many print newspapers have shifted to digital formats, circulating censored or banned material on their websites and social media pages; as a result, residents increasingly rely on online outlets and social media for uncensored information. [6]

Blogging is also popular, allowing journalists and other writers to publish commentary free from the restrictions leveled on print newspapers while providing women and ethnic and religious minorities a platform to express themselves. The more active Sudanese bloggers write in English.

However, the economic crisis and associated rise in the cost of internet access has negatively impacted the quality of content available, mainly

because users are less likely to access higher-quality content, or do not access online content at all due to the high cost of data (see A2). Many people share information on WhatsApp, which uses less data than other platforms.

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**3** / 6

Score Change: The score improved from 2 to 3 as activists returned to social media, though the December 2018 social media blocks and June 2019 internet shutdown left some people hesitant to use the internet to organize protests.

The internet is an increasingly important tool for mobilization, though internet shutdowns and social media blocks designed to impede online organizing have harmed the online environment. Activists relied on Facebook and Twitter to mobilize protests before the June 2019 internet shutdown. During the shutdown, organizers mobilized protests through short-message service (SMS). [1] When internet services were restored in July 2019, people took to social media to circulate images and footage from the June 3rd attack in Khartoum, call for accountability, and organize protests. [2]

Social media and communications platforms were critical in organizing protests in early 2018, as well as the protests that began in December 2018 and ultimately led to al-Bashir's ouster. [3] However, the government's blocks of social media platforms and disruptions to network coverage limited the ability of activists to organize the protests (see A3). Ordinary users worked around the blocks by utilizing free VPNs and circulating instructions on downloading VPNs, which allowed many users continued access to social media platforms (see A3).

The government's blocking and network disruption scheme was clearly intended to disrupt mobilization efforts, as evidenced by the armed NISS and Rapid Support Forces (RSF) agents who stopped protesters and

searched their phones for videos, posts, or pictures about the December 2018 demonstrations. One eyewitness and his friend were stopped on Nile Street in Khartoum by an agent who requested their phones. Both individuals anticipated such an encounter and hid their phones in their car. “Everyone who had pictures and videos on the protests was arrested in front of us,” said the eyewitness in an interview. [4]

Another eyewitness reported that her colleague was stopped and searched, and that security agents did not believe that she only had a basic mobile phone, which led them to search for a smartphone in her car. [5]

After accounts of such practices by security agents spread online, protesters sought to protect themselves by deleting social media apps and information received on WhatsApp and other platforms. Some demonstrators bought a separate phone to use at protests or when they perceived a threat from security forces. [6] Protesters also used functions available on some phones that allow users to switch to a guest account that would have fewer apps available, and therefore less incriminating information. [7]

Between December 2017 and February 2018, mass protests broke out against the government’s handling of the poor economy and proposed tax increases. [8] The “bread protests” were largely organized through Facebook, Twitter, and WhatsApp, and led to the participation of an unprecedented number of ordinary citizens. Some government officials threatened WhatsApp, blaming it for the spread of rumors and leaked information, among other issues. For example, local sources report that during the height of fuel shortages in April 2017, the finance minister told the press that he held WhatsApp responsible for the fuel crisis by spreading false information and panic about fuel prices.

The cyber jihad unit attempted to shut down Facebook pages that disseminated information about the protests, by reporting them en masse (see B5). Social media was the main source of news about the protest movement.

C. Violations of User Rights

The transitional government's interim constitution safeguards freedom of expression, freedom of the press, and access to the internet. The systemic offline harassment by security forces of protesters and activists for their online activity has largely ceased. However, security forces continue to arrest, intimidate, and harass people for their online activities, particularly people expressing critical opinions.

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?	**1** / 6

Score Change: The score improved from 0 to 1 because Sudan's interim constitution, which protects rights and freedoms including freedom of expression, freedom of the press, and access to the internet, was published during the coverage period.

In August 2019, the TMC, the military junta that overthrew al-Bashir, and the Forces of Freedom and Change (FFC), a coalition of civilian organizations and rebel forces, signed an interim constitution, the Draft Constitutional Charter for the 2019 Transitional Period, to serve as Sudan's legal framework until a new constitution is drafted. [1] The interim document focuses on several priorities during the 2019–22 transitional period, including the reformation of existing laws that impinge upon freedoms under the transitional government's leadership.

The interim constitution includes a Rights and Freedoms Charter, which focuses on human rights, including those already specified in international agreements ratified by Sudan. The charter also enshrines the freedom of expression, freedom of the press, and access to the internet. [2] In addition, the interim constitution restructures Sudan's national judiciary and mandates that the transitional government ensures the judiciary's independence. [3]

Civil society organizations raised concerns that the charter does not contain benchmarks for the prescribed reforms or consequences if the transitional government fails to implement reforms. [4]

The constitution allows the cabinet and the TSC to declare a state of emergency, allowing the cabinet to take emergency measures that do not otherwise contradict the document. In extreme circumstances, the cabinet may ask the TSC to suspend the rights enumerated in the Rights and Freedoms Charter, with some exceptions. [5] In October 2019, the TSC announced a three-month state of emergency; [6] after it expired, the TSC "postponed" consideration of whether to extend the state of emergency in January 2020. [7] The TSC declared a health emergency in March 2020 in response to the COVID-19 pandemic, barring noncommercial travel and closing schools. [8]

When the army ousted al-Bashir in April 2019 following four months of popular protests, the TMC announced the suspension of the constitution, a state of emergency, and a curfew, which threatened the rights of online journalists and activists. [9] That February, al-Bashir declared a state of emergency, which also undermined basic constitutional rights. [10]

In July 2019, following the previous month's internet shutdown, the Khartoum District Court ordered Zain to resume internet services. [11] In September 2019, a court ruled that Sudatel and MTN could be sued by their subscribers for the June shutdown and ordered the companies to apologize to their subscribers. [12]

In the past, the Constitutional Court has ruled in favor of prepublication censorship if it is deemed in the interest of national security.

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	**1** / 4

Sudanese law can be used to penalize online activists, journalists, and ordinary users in retaliation for legitimate content. The justice minister is reportedly expected to repeal these laws as part of the transitional

government's plan for legal reforms, though little was shared with the media on what this reform will look like.

In July 2020, after the coverage period, Prime Minister Abdalla Hamdok signed amendments to the Law on Combating Cybercrimes of 2018, which introduced criminal penalties for the spread of fake news online in June 2018 [1] and is based on the Informatic Offenses (Combating) Act of 2007. [2] The July 2020 amendments increase the penalties for many activities specified in the original law, including online defamation, online extortion, hacking of government websites, and sharing false information on social media. [3] Also in July, military officials announced that a new cybercrime commissioner would monitor and prosecute "insults" about the army. [4]

According to the Social Media Exchange (SMEX), a digital rights organization, Article 23 of the 2018 law imposes sanctions such as "imprisonment for less than one year, flogging, or paying a fine" for "anyone who uses the internet, or any means of communications, information or applications to disseminate any news, rumor or report, knowing it's fake, to cause public fear or panic, threaten public safety and offend the reputation of the state." [5]

Amendments to the highly restrictive Media Law passed in 2016 include specific clauses that address online journalism. The amendments extend onerous restrictions long placed on the traditional press to the online sphere, [6] such as provisions that assign fines to journalists and publications found to undermine public order or national security and hold editors in chief criminally responsible for all content published by their outlets. [7]

The Informatic Offenses (Combating) Act of 2007, which provides the basis for the cybercrimes law, criminalizes the establishment of websites that publish defamatory material and content that disturbs public morality or public order. [8] Those found in violation of the law face fines and prison sentences of between two and five years.

National security imperatives have also opened journalists up to arrest. The 2010 National Security Act gave the NISS immunity from prosecution

and the ability to arrest, detain, and censor journalists under the pretext of national security. [9]

C3 0-6 pts

Are individuals penalized for online activities?	2 / 6

Arrests, prosecutions, and interrogations for online activities continued during the coverage period, particularly as heavy-handed censorship of the print and broadcast sectors led journalists to migrate online to disseminate news. Internet users continued to fear arrest for online dissent under the transition government, particularly after the June 2019 massacre.

In early April 2020, Edriss Elbur, a store owner and activist, was arrested and detained for two days by the RSF. During Elbur's detention, RSF officers interrogated him about Facebook posts he made criticizing the RSF and warned him not to make similar posts. [1] Later that month, Elbur was arrested a second time, allegedly after making a complaint against the officers who originally arrested him. [2]

In December 2019, the government issued an arrest warrant for journalist Abdel-Moneim Suleiman. The warrant alleged that Suleiman, who also faced travel restrictions, spread false information, including on his Facebook page, about conservative cleric Abdulhay Yousif. [3] Suleiman reported that he was not in Sudan at the time the warrant was issued. [4]

At least 79 journalists were arrested [5] as protests escalated between December 2018 and February 2019, during the previous coverage period, and several were held in detention for weeks. A number of journalists and bloggers were penalized for content published online. For example, in January 2018, Faisal Mohamed Saleh, an online journalist for Al Araby and Al Taghyeer, was arrested and interrogated for his coverage of the protests. Online journalist Ghurashi Awad was arrested on the same day and was also interrogated for his coverage of the protests. [6] Awad was reportedly detained for over a month. [7]

In January 2019, the Sudania 24 television network reported that the State Security Prosecution had produced arrest warrants for 38 journalists and activists, including those who publish online, for incitement and publishing fake news. [8] According to reports, 28 of the 38 people targeted by the warrants were living outside Sudan. Their names were not revealed, which instilled fear among journalists and activists. The government has reportedly explored using Interpol to pursue those living abroad. Authorities have pursued online activists based outside Sudan before, particularly those who live in Saudi Arabia. For example, Hisham Ali, [9] an online activist and blogger based in Saudi Arabia, was arrested by Saudi authorities in late 2017 and transferred to Sudan in May 2018. [10] He was detained until his release in April 2019. [11]

A number of people near protest sites were reportedly stopped by security forces, who searched their phones for digital content related to the demonstrations. If protest-related content was found on their phones, including pictures, videos, and online posts, they were arrested (see B8).

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**3** / 4

The government does not directly restrict encryption, but SIM card registration requirements limit anonymous communication. Social media blockings in past years drove users toward VPNs and facilitated the use of encrypted communication tools like Signal and Telegram.

Article 9 of the NTC's General Regulations 2012, based on the 2001 Communications Act, obligates mobile service providers to keep a complete record of their customers' data, and authorities began enforcing mandatory SIM card registration in late 2017. Subscribers were given a deadline of December 31, 2017 to register their phone numbers using their national identity cards, which include detailed personal information such as home address and birthplace. These requirements enable the government to access mobile user information, limiting anonymity.

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

Unchecked surveillance of information and communication technologies (ICTs) is a grave concern in Sudan, where the government is known to actively monitor communications on social media platforms and surveil online activists and journalists during politically sensitive periods. The NISS regularly intercepted private email messages with the aid of sophisticated surveillance technologies.

According to 2013 research published by Citizen Lab, a Canadian digital rights organization, Sudan possesses high-tech surveillance equipment produced by the American technology company Blue Coat Systems, which manufactures monitoring and filtering devices. The surveillance system was initially traced to three networks inside Sudan, including the networks of private telecommunications provider Canar Telecom. [1] In 2017, NISS agents reportedly planted Blue Coat surveillance software in the phones and laptops of at least 11 activists during an out-of-country meeting and training. According to a local expert, the software was installed through the Wi-Fi modem shared by the group and enabled the comprehensive monitoring of their online activities. [2]

The Sudanese government reportedly purchased software that can remotely infect an electronic device to monitor communications and steal files, known as the Remote Control System, from the Italian technology company Hacking Team in 2012. As of November 2014, Hacking Team has suspended service to Sudan. [3]

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	**0** / 6

Service providers are required to aid the government in the surveillance of their users, though no such incidents were publicly reported during the

coverage period. The SIM card registration process links phone numbers to users' personal data, which enables government surveillance (see C4). Mobile service providers are obligated to keep records of their customers' data, including full names, full addresses, other phone numbers, and place of employment.

An activist who was summoned for questioning in early 2018 [1] noted that an NISS officer told him that because authorities have access to the national ID system and the user information stored by telecommunications companies, they could collect extensive information about mobile users with just their phone numbers.

Telecommunications providers can be compelled to aid the government in monitoring the communications of their users, but authorities reportedly have a tighter grip on Zain and Sudatel than MTN. The NISS allegedly maintained significant involvement in telecommunications providers' hiring processes, and NISS agents were apparently sometimes embedded within the companies.

Between July and December 2019, Facebook received 52 requests for data covering 76 user accounts from the Sudanese government. Facebook produced no data in response to these requests. [2]

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?	**2** / 5

Score Change: The score improved from 1 to 2 as systemic offline harassment by security forces of protesters and activists for their online activity has largely subsided, though online and offline harassment remains common, particularly for women.

Online journalists and activists often face extralegal intimidation, harassment, and violence in retaliation for their online activities. The frequency of such incidents decreased during the coverage period, in comparison to the many protesters who reported harassment from

security agents after posting on social media around the mass demonstrations in early 2019.

In May 2020, security forces threatened and intimated journalists Lana Awad and Aida Abel Qader for their coverage of hospital deaths that were likely related to the COVID-19 pandemic in North Darfur. [1] Both women reported that individuals who identified themselves as military intelligence officers requested that they attend an interview at their headquarters, and threated to compel them to do so, over the course of three days in El Fasher. [2]

As internet services resumed in July 2019, protesters shared dozens of videos documenting the June massacre in Khartoum on social media. Lieutenant General Mohamed Hamdan Dagalo, then deputy chair of the TMC, reportedly accused one internet user of killing the protesters, contributing to the climate of intimidation online. [3]

Though security forces have not systematically harassed protesters for their online activity during the coverage period, activists and protesters reported that the authorities did make attempts to restrict their online activities. Demonstrators reported that security forces who violently repressed an April 2020 protest confiscated the phones of activists and journalists. [4] In December 2019, a group of social media activists reported that they were harassed.

Activists and protesters detained during the coverage period often experienced long pretrial detentions and torture by the authorities. Nine young people arrested in the aftermath of the Khartoum massacre were reportedly detained for more than three months, [5] while a prominent activist was sentenced to four months' detention for criticizing a police officer. [6] Activists reported numerous cases of violent arrest by security forces and torture while in custody. [7]

Social media influencers and minority groups such as the LGBT+ community are frequent targets of online harassment. Female activists are often subjected to threats and smear campaigns on social media. For instance, in July 2020, after the coverage period, high school student Ludan Tariq experienced bullying and harassment online, including

criticism that she was not covering her hair, after a video of Tariq criticizing the military went viral.

In September 2019, sexual videos of “Kholoud,” a young woman, were shared online without her consent. Social media users began harassing her online, causing Kholoud to stop leaving her home; she later left Sudan. [8]

In another prominent example from recent years, over 15 female activists were doxxed on the fake “Sudanese Women against the Hijab” Facebook group, where their private pictures were posted without their consent alongside fabricated quotes about their supposed opposition to the veil and Islam. Some of the targeted individuals feared for their lives in the face of threats of violence from religious fundamentalists. Two of the women reported the page to the cybercrimes prosecution office, which took no action. Instead, one woman was shamed and scolded for posting her picture online. The page was only shut down in 2017 after international human rights groups brought attention to the issue.

In several instances in past years, Sudanese nationals living outside of the country were subjected to online harassment. In February 2019, a Sudanese individual living abroad posted information about a Sudanese man living in Turkey, who reportedly facilitated the purchase of tear gas for the Sudanese government, to Monbrshat, a woman’s Facebook group. Her post was subsequently reported to Facebook, and she received extensive harassment on social media, along with threatening phone calls. A photo of the woman and her husband were later posted to social media, along with their full names; the woman’s sister also received a threatening phone call. [9] Monbrshat continued to endure online attacks as it posted pictures and information about NISS and other government officials.

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**0** / 3

Individual users faced cyberattacks and nonconsensual dissemination of intimate material during the coverage period. Media outlets regularly defend against cyberattacks, while a local source also indicates that government websites are regularly targeted by hackers.

In the aftermath of al-Bashir's ouster, videos and pictures of women previously deemed "immoral" became more common online, and have become a subject of debate. Supporters of al-Bashir blamed the prevalence of this material on the transitional government, while the TSC's supporters called their opponents' arguments a distraction meant to tarnish the new government. In a September 2019 example of this trend, "Kholoud" was subjected to the nonconsensual sharing of intimate material. That material resulted in an online campaign against her; she felt unsafe leaving her home, and later left the country altogether. [1]

Government and news websites often face hacking and other forms of cyberattack. A news article published in January 2019 cited the National Information Center when reporting that government websites were targeted by 200 daily hacking attempts. However, this figure could not be corroborated. [2]

In January 2019, hackers reportedly made some content housed on the website of the government-run Sudan News Agency (SUNA) inaccessible. [3] In June 2020, after the coverage period, hackers defaced the websites of two universities and other websites to commemorate the Khartoum massacre. [4] That same month, the Sudanese Ministry of Religious Affairs and Endowments experienced a cyberattack where pornography was posted on its website. [5]

In late 2018, Anonymous responded to the government's social media blocks by hacking government websites. In total, 260 websites were hacked and became inaccessible, including the sites of two progovernment television networks. [6]

Independent news sites are frequently subjected to technical attacks, which many believe are perpetrated by the cyber jihad unit. Attacks usually intensify around significant political events and unrest, while some prominent news sites ward off daily distributed denial-of-service (DDoS)

attacks. Several online outlets reported technical attacks against their websites in past years, but they were able to respond by increasing their cybersecurity capabilities.

Throughout 2017, a Facebook page created by Sudanese women to post screenshots of sexual harassment incidents faced several hacking attempts following strong condemnation from numerous male users. The women also have a private group with over 7,300 members on social media called “Inbox messages,” where they share sexually inappropriate and aggressive messages from men on social media with one another.

On Sudan

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

See More ›

Country Facts

Global Freedom Score

12 /100 **Not Free**

Internet Freedom Score

30 /100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

Yes

Social Media Blocked

No

Websites Blocked

No

Pro-government Commentators
Yes

Users Arrested
Yes

In Other Reports

Freedom in the World 2020

Other Years

2019

ADDRESS

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

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org