

LONDA 2025

DIGITAL RIGHTS & INCLUSION IN AFRICA REPORT

Sudan

Country Report



PARADIGM
INITIATIVE



LONDA 2025

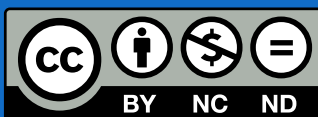
DIGITAL RIGHTS & INCLUSION IN AFRICA REPORT

Report produced and published by Paradigm Initiative
April 2026

This publication may be reproduced for non-commercial use in any form provided due credit is given to the publishers and the work is presented without any distortion.

Copyright ©2026 Paradigm Initiative

374 Borno Way, Yaba, Lagos, Nigeria.
media@paradigmhq.org
www.paradigmhq.org



Creative Commons Attribution-
NonCommercial-NoDerivatives
(CC BY-NC-ND) license

ISBN: 978-978-68-6631-4



Sudan

Anonymous

Executive Summary

This report examines the state of digital rights and digital inclusion in Sudan as of 2025. The report's methodology relies on desk research focusing on specific thematic areas for incidents in Sudan, in line with Paradigm Initiative's TheScore Index, aiming to assess the state of digital rights in focus countries, as well as insights from the author's practical experience of working on digital rights in Sudan. The report explores diverse digital rights thematic areas, including internet access, freedom of expression, data protection and priva-

cy, censorship and content moderation, access to information, AI and emerging technologies, and digital inclusion.

The year 2025 witnessed numerous instances of connectivity control by various actors. Also, freedom of expression faced significant legal barriers. The cybercrimes law was amended in October 2025, imposing stricter penalties, including mandatory fines and imprisonment, and has been used against journalists and activists criticising state leaders. Moreover, privacy violations were frequently reported in 2025, including the Rapid Support Forces (RSF) inspecting citizens' phone content in conflict zones. Despite these

challenges, the Government announced the establishment of new institutions in November 2025, including the Sudanese Cybersecurity Authority and the Sudanese Data and Artificial Intelligence Authority. Furthermore, the Universal Service Fund (USF) activities have recently resumed, supporting internet connectivity via Star-

link Wi-Fi stations in underserved areas.

The report provides recommendations to the Government, including the Sudanese Armed Forces (SAF), Rapid Support Forces (RSF), civil society, private sector, and the media.



Introduction

Sudan lies in northeastern Africa, bounded on the north by Egypt, on the east by the Red Sea, Eritrea, and Ethiopia, on the south by South Sudan, on the west by the Central African Republic and Chad, and on the northwest by Libya.¹ Following the ousting of the authoritarian regime of Al-Bashir, who ruled Sudan for 30 years, in 2019, the Sudanese people gained hope to build a democratic country after the last revolution.² However, the military took over as Sudan is now ruled by a military regime that has been in charge since October 25 2021. Lieutenant General Burhan led a military coup against his partners in the transitional government, just after the Sudan uprising. In 2025, the Sudanese people, especially in Kordufan and Darfur regions, were living in a crisis sit-

uation where a fierce war between the SAF and RSF was ongoing.³

As of 2025, Sudan's total population was 52.2 million.⁴ However, 14.6 million citizens use the Internet, with internet penetration at a rate of 28.7%.⁵ There were 21.6 million cellular mobile connections in Sudan at the start of 2025.⁶ There are four main internet service providers (ISPs) in Sudan, three of which are foreign-owned (Zain, MTN, and Canar), and the fourth is Sudatel, whose board of directors includes a member of the Transitional Sovereign Council, which represents the Head of State, and the Minister of Finance.⁷

1. Britannica, "Sudan", <https://www.britannica.com/place/Sudan>, (accessed on 29 November 2025).
2. BBC, "Omar al-Bashir: Sudan's ousted president", <https://www.bbc.com/news/world-africa-16010445>, (accessed on 29 November 2025).
3. BBC, "A simple guide to what is happening in Sudan", <https://www.bbc.com/news/articles/cjel2nn22z9o>, (accessed 20 January 2026)
4. Worldmeter, "Sudan Population", <https://www.worldometers.info/world-population/sudan-population/>, (accessed on 20 January 2026)
5. Data Portal, "DIGITAL 2025: SUDAN", <https://datareportal.com/reports/digital-2025-sudan>, (accessed on 9 November 2025).
6. Data Portal, "DIGITAL 2025: SUDAN", <https://datareportal.com/reports/digital-2025-sudan>, (accessed on 9 November 2025).
7. Mubasher, Sudatel, <https://english.mubasher.info/markets/adx/stocks/SUDATEL/profile>, (accessed on 9 November 2025).

Internet access and disruptions

Network operations in Sudan are regulated under the Telecommunication and Post Regulation Authority Act (TPRA) of 2018⁸. The locally licensed internet in Sudan is available only in SAF-controlled areas, while people in other areas connect using satellite internet. The average internet speed in the third quarter was 22.2 Mbps, including Starlink's speed (36.7 Mbps)⁹. Moreover, the average price of 1 GB for mobile is SDG1,500 (US\$0.4), including VAT, while the Starlink services are provided by the hour, where an hour of connection costs SDG7,000 SDG (US\$2). It is worth noting that RSF collects Star-

link operating fees in its controlled areas. Moreover, the Minister of Finance issued an order to collect the telecommunication tax in advance.¹⁰

The TPRA law has many vague articles that were previously used to disrupt the internet¹¹. However, 2025 witnessed numerous cases of connectivity control, varying in duration, mechanism, impact, and actor. On January 21 2025, it was reported that the RSF confiscated Starlink devices from al-Hasahisa, al-Kamlin, and East al-Jazira without any justification.¹² On June 23 2025, it was reported that RSF dismantled Starlink devices in Kotom town in northern Darfur and installed its own.¹³ Moreover, on November 6 2025, the local authorities in Diling shut down the Starlink services for two days due to

8. TPRA, Laws, <https://tpra.gov.sd/wp-content/uploads/2025/02/THE-TELECOMMUNICATION-AND-POST-ORGANIZATION-Act2018-%D8%A7%D9%84%D9%85%D8%B9%D8%AA%D9%85%D8%AF%D8%A9.pdf>, (Accessed on 9 November 2025)
9. SpeedGeo, "Internet speed in Sudan", <https://www.speedgeo.net/statistics/sudan>, (Accessed on 9 November 2025)
10. Ministry of Finance, "A decision from the Ministry of Finance to collect telecommunication VAT in advance", <https://mof.gov.sd/%D9%82%D8%B1%D8%A7%D8%B1-%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%A7%D9%84%D9%8A%D8%A9-%D8%A8%D8%A7%D9%84%D8%AA%D8%AD%D8%B5%D9%8A%D9%84-%D8%A7%D9%84%D9%81%D9%88%D8%B1%D9%8A-%D9%84%D9%84%D8%B6%D8%B1%D9%8A/>, (accessed on 9 November 2025)
11. Global Voices, "In Sudan, the court stands on the side of unrestricted access to the internet", <https://advoc.globalvoices.org/2021/12/16/in-sudan-the-court-stands-on-the-side-of-unrestricted-access-to-the-internet/>, (Accessed on 9 November 2025)
12. Nabd Sudan, "RSF confiscates Starlink from 3 localities", <https://nabdsudan.net/?p=159983>, (Accessed on 9 November 2025)
13. Darfur 24, "Arrests and restrictions on internet use in North Darfur", <https://www.darfur24.com/2025/06/23/%D8%A7%D8%B9%D8%AA%D9%82%D8%A7%D9%84%D8%A7%D8%AA-%D9%88%D8%AA%D9%82%D9%8A%D9%8A%D8%AF-%D8%A7%D8%B3%D8%AA%D8%AE%D8%AF%D8%A7%D9%85-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%81%D9%8A-%D8%B4/>, (accessed on 9 November 2024)

bombing activities.¹⁴ In addition, the authorities ordered a daily internet shutdown between July 7-10 2025 for three hours each, justifying the order by saying the shutdown was to avoid cheating in the national exam.¹⁵ In addition, after controlling Al-Fashir city in late October 2025, the RSF isolated the city, prohibiting any means of communication.¹⁶

On another note, the TPRA ordered the ISPs to restrict WhatsApp calls in June 2025, justifying this order under “national security”.¹⁷

Online Freedom of

Expression and Access

to Information

The authorities amended the Law Combating Cybercrimes of 2018 (Cybercrimes law) in October 2025, with stricter penalties and the mandatory imposition of both fines and imprisonment.¹⁸ The first case of using law against freedom of expression was against the journalist Azmy Abderazik, who criticised the Prime Minister.¹⁹ Moreover, even before the amendments, the law had been used against activists who criticised the “state leaders”. In February 2025, the Anti-Terrorism and

14. Darfur 24, “Internet shutdown lifted in Dilling, South Kordofan, after isolation imposed by bombing”, <https://www.darfur24.com/2025/11/08/%D8%B1%D9%81%D8%B9-%D8%AD%D8%B8%D8%B1-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%81%D9%8A-%D8%A7%D9%84%D8%AF%D9%84%D9%86-%D8%AC-%D8%A8%D8%AC%D9%86%D9%88%D8%A8-%D9%83%D8%B1%D8%AF%D9%81%D8%A7/>, (accessed on 9 November 2025)
15. Cloudflare, “Online outages: Q3 2025 Internet disruption summary”, <https://blog.cloudflare.com/q3-2025-internet-disruption-summary/#sudan>, (accessed on 9 November 2025)
16. Akhbar Sudan, “al-Fasher is experiencing complete digital isolation after communications equipment was confiscated by the RSF.”, <https://www.sudanakhbar.com/1715407>, (accessed on 9 November 2025)
17. Developing telecoms, “Sudan’s blocking of WhatsApp calls goes into effect”, <https://developingtelecoms.com/telecom-business/telecom-regulation/18836-sudan-s-blocking-of-whatsapp-calls-goes-into-effect.html>, (accessed on 19 November 2025)
18. Al Jazeera, “نادرسلاب تاييرحل دي يقيقتل تي نوناق تال يدعت لالغتسا نم فواخم” [Concerns that legal amendments could be exploited to restrict freedoms in Sudan]”, <https://www.ajnet.me/politics/2025/10/19/%D9%85%D8%AE%D8%A7%D9%88%D9%81-%D9%85%D9%86-%D8%A7%D8%B3%D8%AA%D8%BA%D9%84%D8%A7%D9%84-%D8%AA%D8%B9%D8%AF%D9%8A%D9%84%D8%A7%D8%AA-%D9%82%D8%A7%D9%86%D9%88%D9%86%D9%8A%D8%A9>, (accessed on 19 November 2025)
19. Akhbar Sudan, “سيريدي لمارك نع هلاقم دعب قزارل دبع يمزع يفحصلنا ىلع ضربق لابل اراق رصت فباينلا” [The prosecution issued an arrest warrant for journalist Azmi Abdel Razek following his article about Kamel Idris.]”, <https://www.sudanakhbar.com/1719589>, (accessed on 19 November 2025)

foreign policy. The law is not yet fully operational since its passage as it stated establishing information access commission but it wasn't established until the moment of writing this report, making the right to access information inaccessible. In addition, although it was enacted, the law classified some information that is banned from access by citizens, using the broad term "national security", which can be abused to stifle access to information. Even though the law affirmed the rights of persons with disabilities (PWDs), it did not specify the accessible communication means required to ensure the inclusion of PWDs.²⁶

Other laws used by authorities include the Telecommunication and Post Regulation Authority Law of 2018, the 2007 Amendment of the Law of the Sudanese Armed Forces, and the Emergency and Public Safety Law of 1997.

The 2020 bylaw on Content Filtering and Website Blockage on the internet created a list containing 13 categories that must be filtered and blocked in Sudan.²⁷ These categories include child pornography, weapons, gambling, and betting. Some vague categories, including "calling for atheism" in Article 16-E of the bylaw, open a wide door for abuse against religious freedom. Also, the same list stipulates in Article 16-I that Virtual Private Networks (VPN) must be blocked, indicating an intention of blocking the circumvention tools.²⁸

Data Protection and Privacy

Sudan currently lacks a comprehensive data protection law.²⁹ Despite this absence, Article 20-1 of the 2013 Regulation

26. Global Voices, "The case for reforming the Sudanese Access to Information Act", <https://globalvoices.org/2019/08/28/the-case-for-reforming-the-sudanese-access-to-information-act/>, (accessed on 7 November 2025)

27. TPRA, "List of filtering and blocking pages and websites on the Internet for the year 2020", <https://tpra.gov.sd/wp-content/uploads/2023/12//%D9%84%D8%A7%D8%A6%D8%AD%D8%A9-%D8%AA%D8%B1%D8%B4%D9%8A%D8%AD-%D9%88%D8%AD%D8%AC%D8%A8-%D8%A7%D9%84%D9%85%D9%88%D8%A7%D9%82%D8%B9-%D9%88%D8%A7%D9%84%D8%B5%D9%81%D8%AD%D8%A7%D8%AA-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D8%B9%D9%84%D9%89-%D8%B4%D8%A8%D9%83%D8%A9-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%84%D8%B3%D9%86%D8%A9-2020%D9%85.pdf>, (accessed on 9 January 2025)

28. Global Voices, "How the government in Sudan legalized internet categorizing and content filtering", <https://advoc.globalvoices.org/2022/08/02/how-the-government-in-sudan-legalized-internet-categorizing-and-content-filtering/>, (accessed on 8 November 2025)

29. Data protection Africa, "Sudan", <https://dataprotection.africa/sudan/>, (accessed on 3 November 2024)

for Organizing Payment Systems mentioned that payment service providers must take necessary measures to protect and preserve user data.³⁰

The practice of surveillance and privacy violations in Sudan is problematic, as the authorities have used different technologies from several vendors during various eras.

Several privacy violation cases were reported during 2025. It was reported that the RSF inspected the citizens' phones' content in Niyala city.³¹ Moreover, some citizens reported that the RSF was inspecting the content of their phones at Starlink points in Khartoum before clashing with SAF.³² These cases have implications for safe and encrypted communications.

Censorship and

Content Removal

The year 2024 saw significant changes in content moderation efforts in Sudan. In October 2024, X followed Meta in suspending some RSF accounts, including the official account of the RSF, in addition to the account of the RSF commander, Mohamed Hamdan Daglo.³³ This step came after a public relations campaign led by a pro-SAF activist called Mohamed Kambal.³⁴ However, on November 27 2025, the same person, Kambal, revealed that X removed the accounts of the so-called "Tasees government" which is connected to the RSF.³⁵

30. Central Bank of Sudan, "Regulation for Organizing Payment Systems", https://web.archive.org/web/20230501153605/https://cbos.gov.sd/sites/default/files/ps_business_organization.pdf, (accessed on 29 November 2025)
31. Sudan Independent, "سودان مستقل، 'حملة لفتح هواتف المدنيين في نيالا، جنوب دارفور' [A campaign to search the phones of civilians in Nyala, South Darfur]", (accessed on 29 November 2025)
32. Facebook, Mohsin Alneemah, https://www.facebook.com/story.php?story_fbid=10233655448826580&id=1190028496&rdid=QIQTUcf6lwFLEDeA#, (accessed on 29 November 2025)
33. Business & Human Rights Resource Centre, "Sudan: X has suspended the accounts of Hemedti and RSF", <https://www.business-humanrights.org/en/latest-news/sudan-x-suspends-accounts-of-hemedti-and-rsf/>, (accessed on 29 November 2025)
34. Aljazeera, "الجزيرة، 'معدلة تائباسح تناصنم ففاق ي دعب نادوسلا يف لدج' [Controversy in Sudan after suspending Rapid Support Forces accounts]", <https://www.ajnet.me/news/2024/10/22/%D8%AC%D8%AF%D9%84-%D9%81%D9%8A-%D8%A7%D9%84%D8%B3%D9%88%D8%AF%D8%A7%D9%86-%D8%A8%D8%B9%D8%AF-%D8%A5%D9%8A%D9%82%D8%A7%D9%81-%D9%85%D9%86%D8%B5%D8%A7%D8%AA-%D8%AD%D8%B3%D8%A7%D8%A8%D8%A7%D8%AA>, (accessed on 29 November 2025)
35. Facebook, Mohamed Kambal, [https://www.facebook.com/permalink.php?story_fbid=pfbid02Vz6Amw3R8JU-cAv9f5hVXeu81XRE56zyxf6v9vHM5sYw6mTnvokbuRnLCXXBSsjMDI&id=100069487239242&_cft__\[0\]=AZXHAK-mhXosehZGKgfI56QuHT31qD7OXPSXHOU4Ag5u9XG7rYa6EstZ4hQEIZvdD9mGXoyG4TvqJASuoWfFPBtOAsOK-mkBpLxV6c7C0swo8Pi_WhzzTqV5TJq3KimVvQv8fnWLLJk8uFxAiHwWEdXCRQwaYLVQ-PcwavaBjNl4NbFzt_u6O-QPCku2MDMGptGFw&__tn__=%2CO%2CP-R](https://www.facebook.com/permalink.php?story_fbid=pfbid02Vz6Amw3R8JU-cAv9f5hVXeu81XRE56zyxf6v9vHM5sYw6mTnvokbuRnLCXXBSsjMDI&id=100069487239242&_cft__[0]=AZXHAK-mhXosehZGKgfI56QuHT31qD7OXPSXHOU4Ag5u9XG7rYa6EstZ4hQEIZvdD9mGXoyG4TvqJASuoWfFPBtOAsOK-mkBpLxV6c7C0swo8Pi_WhzzTqV5TJq3KimVvQv8fnWLLJk8uFxAiHwWEdXCRQwaYLVQ-PcwavaBjNl4NbFzt_u6O-QPCku2MDMGptGFw&__tn__=%2CO%2CP-R), (accessed on 29 November 2025)

Moreover, the Meta transparency center highlighted³⁶ that it did not receive any removal requests from the Sudanese government. In addition, the transparency centre of TikTok has not issued updates on the data of content removal requests this year. Also, Google’s transparency report does not include Sudan on the list of countries, representing a gap in the sources of information related to Sudan with regard to content moderation.³⁷

Digital Inclusion

In November 2025, the Sudanese Minister of Telecommunication and Digital Transformation announced the establishment of three new institutions, including the Digital Transformation Authority, the Sudanese Cybersecurity Authority, and the Computer Professions Regulatory Council. He also mentioned that the name of the National Information Centre has been

updated to be the Sudanese Data and Artificial Intelligence Authority.³⁸ Despite these developments, the governance and legal framework of these institutions have not been published.

Two ICT practitioners claimed that they created facial recognition software that is trained to recognise the soldiers of the RSF at borders.³⁹ While it is not yet confirmed whether it was used by authorities or not, the software’s accuracy raises many questions about its potential impact on citizens’ freedoms and rights.

Article 35 of the Cybercrimes law explicitly criminalises acts such as threatening or deceiving a child through digital means, aiming to safeguard minors from online bad behaviour. Unfortunately, despite this positive provision, there is a clear absence of proactive engagement, leaving children vulnerable to cyber threats without timely intervention.

36. <https://www.google.com/url?q=https://transparency.meta.com/reports/government-data-requests/country/SD/&sa=D&source=docs&ust=1771768464868635&usg=AOvVaw3AcPAdSA4tqWEbMYxNICQF>

37. Google transparency report, “Government requests to remove content”, <https://transparencyreport.google.com/government-removals/government-requests?hl=en>, (accessed on 5 November 2025)

38. LinkedIn, Ahmed Dirdiri Ghandour, https://www.linkedin.com/posts/ahmedghandour_sudan-digitaltransformation-artificialintelligence-activity-7391916669910265856-UQdn?utm_source=social_share_send&utm_medium=member_desktop_web&rcm=ACoAACH4BX0BFFQpZj9F_NHDZ6xgvoj0mB0RkBM, (accessed on 29 November 2025)

39. Alzaawia, “بي عن اتصال الفذلا” ب ربا عملما يف عير-سلا م-عدلا يبوسنم يلع فرعتي يلا ماظن رالفتبا” [Developing an AI-powered system to identify rapid response personnel at border crossings.], <https://alzaawia.net/92148>, (accessed on 29 November 2025)

The Universal Service

Fund (USF)

The government established the Universal Service Fund (USF) project in Sudan three times, starting in 2003, after forming the Information Technology Development Council. Then, in 2005, the Council was changed to a 'Fund', and finally, the current Universal Service Fund was established under the new name in the year 2018, according to the Telecommunication and Post Regulation Act (TPRA).⁴⁰

The regulator, TPRA, conducts annual surveys as part of its comprehensive service project. The last publicly available information was in 2018, when a survey was conducted targeting 55 areas that were not covered by communication networks in the first phase, to collect accurate data and then classify them by economic feasibility for profit and loss, for operators and ISPs. The survey team identified 17

feasible areas and 38 non-feasible areas. Starting in 2018, the TPRA specified that the USF mission is to be responsible for supporting the economically unfeasible areas, while the telecommunications companies should include the economically feasible areas in their annual plan for implementation.⁴¹

However, this research did not find any online information about any projects that the USF supported in 2025. However, the Londa 2023 report mentioned that the USF did not have any plans or resources due to the war.⁴² However, the year 2025 witnessed the return of the USF as the TPRA Director, Dr. Alsadig Gamal, stated that they supported internet connectivity via Starlink in some areas that were not covered by ISPs. He added, "We installed Wi-Fi stations connected with Starlink and offered connectivity for a supported price."⁴³

40. TPRA, "Universal Service Fund", <https://web.archive.org/web/20190422055334/https://tpra.gov.sd/wp-content/uploads/2018/06/Universal-Service-Fund.pdf>, (accessed on 29 November 2025).

41. TPRA, "Universal Service Fund", <https://web.archive.org/web/20220625164326/https://tpra.gov.sd/regulation-issues/%d8%a7%d9%84%d9%85%d8%b4%d8%a7%d8%b1%d9%8a%d8%b9/universal-service/>, (accessed Theon 10 November 2023).

42. Paradigm Initiative, "Londa Sudan 2023", https://paradigmhq.org/sdm_downloads/londa-23-sudan-en/, (accessed on 29 November 2025)

43. Interview with the TPRA director, 29 November 2025

Conclusion

Sudan's digital environment is connected to the ongoing conflict, resulting in limited internet access and severe restrictions on digital rights. The TPRA Act and recent legal amendments have provided a framework for authorities and warring parties to actively disrupt communication, censor expression, and violate privacy. While there are efforts to modernise ICT insti-

tutions, these developments are undermined by the secrecy surrounding new legislation and the active enforcement of restrictive laws against citizens and journalists. The general environment demonstrates a significant gap between the stated goal of digital transformation and the reality of censorship, surveillance, and suppression of dissent.

Recommendations

The Government should:

- Immediately stop using vague Articles (6-j) in the TPRA law to disrupt internet access or impose restrictions, such as the order to restrict WhatsApp calls under “national security”.
- Amend the laws of Combating Cybercrimes (Articles 24, 25, 26)⁴⁴, Press and Press Publications of 2009 (Articles 5, 33, 35)⁴⁵,

44. Law of Combating Cybercrimes, <https://tpra.gov.sd/wp-content/uploads/2024/12/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9.pdf>, (Accessed on 2 February 2026)

45. Law of Press and Press Publications of 2009, Mena Rights, <https://menarights.org/sites/default/files/2016-11/The%20press%20and%20printed%20press%20material%20act%202009%20%28AR%29.pdf>, (Accessed on 2 February 2025)

Telecommunication and Post Regulation Authority 2018 and National Security Act of 2010 (Article 25(a))⁴⁶, which contain vague terms and impose harsh and disproportionate punishments on the state workers to discard vague provisions and criminalisation of false news and sedition.

- Enact a data protection law.
- Make the legislation related to newly established institutions publicly available to ensure accountability and prevent abuse.
- Implement the Access to Information Act to increase access to information, which will reduce the spread and impact of disinformation and empower citizens

to access the right information from their sources.

- Reduce the telecommunications tax to ensure affordable internet access.
- Support the operationalisation of the Universal Service Fund and proactively disclose the use of the funds.
- Not target citizens, journalists, and activists based on their online activities.
- Stop arbitrarily seizing and inspecting citizens' phones and other electronic devices, violating encryption, and breaching the right to privacy.
- Publish the legal frameworks of the Cybersecurity Authority and the Data and Artificial Intelligence Authority.

Rapid Support Forces (RSF) should:



- Not target citizens, journalists, and activists based on their online

activities through actions such as illegally seizing and inspecting or

46. National Security Law, Mena Rights, <https://menarights.org/sites/default/files/2016-11/Sudan%20National%20Security%20Act%202010%20%28EN%29.pdf>, (Accessed on 2 February 2026)

- stealing citizens' phones and other electronic devices.

Civil Society Organisations should:

- Actively monitor and document cases where the amended cyber-crimes law is abused to prosecute activists and journalists, and lobby for their repeal or reform.
- Civil society should advocate against internet shutdowns in conflict zones through mobilising strategic litigation and technical network monitoring to hold armed actors accountable for using internet shutdowns as a tool of information warfare and digital repression.
- Civil society must raise awareness of digital rights among the Sudanese people through training and media campaigns.
- Civil society should provide digital safety training to the targeted people with spyware or other forms of digital surveillance.
- Civil society should advocate for the immediate release of the legislation governing the new ICT and AI authorities announced by the Minister of Telecommunication and Digital Transformation.
- Civil society should monitor and document digital rights violations..

The Media:

- Enhance their capacity in fact-checking and anti-disinformation skills.
- Provide digital safety training to its members.
- Collaborate with international partners to pressure major technology platforms to improve transparency by including Sudan data in their content removal and transparency reports.
- Report on digital access inequality.







The private sector should:






- Update their transparency reports periodically. In addition, Google and X should add Sudan to their report.
- Uphold data protection standards.
- The Internet Service Providers should resist shutdown orders and notify their users when they receive such orders







The Score Index



Sudan, 2025

1 = Totally non-compliant; 2 = Mildly compliant; 3 = Moderately compliant;
4 = Considerably compliant; 5 = Fully compliant

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Internet Shutdowns	P38(2)	 2	 1	The government shut down the internet during exams and blocked WhatsApp calls.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	 2	 3	The USF supported the internet in some underserved areas.
False News Criminalisation	P22(2)	 2	 2	The Cybercrimes law criminalised false news.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Sedition Legislation	P22(2)			The Cybercrimes law criminalised Sedition.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)			Several arrests and media harassment cases by the authorities and RSF have been reported.
Data Protection Legislation.	P42			While some laws have articles related to data protection, there is no data protection legislation
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)			While there is no information for this year, last year witnessed numerous cases of governmental interference.
Invasion of Privacy of	P41			The RSF areas witnessed phone inspections.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)			While the government used to announce information using the official news agency and the Spokesperson platform, there is missing information that couldn't be found without media reports. Moreover, the legislation related to newly established institutions was not published. Also, the amendment of the Cybercrimes law was not published. Sudan passed the 'Right to Access Act' in 2015. The law contains a list of 12 types of classified information that are restricted from citizens, using vague terms in describing these categories which are used as a justification for non-disclosure.
AI and Emerging Technologies national strategies	P39(6)			The government established a new AI institution, but no clear activities have been announced yet.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)			Article 35 of the Cybercrimes Law punished the criminals who threaten or deceive a child. However, there is no on-ground pro-active application.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Digital Inclusion	P37(3)	 2	 2	There is no public information about the USF. However, we got information that the USF supported the internet in some underserved areas.
Total (out of 60):	2024: 21	2025 20		



374 Borno Way, Yaba 101245, Lagos, Nigeria.
www.paradigmhq.org