LONDA 2025

DIGITAL RIGHTS & INCLUSION IN AFRICA REPORT

Using The Score Index for evaluation, this report details key findings and recommendations to advance digital rights and inclusion in Africa.



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: 978-978-789-359-3

TABLE OF CONTENTS

Angola 00	Benin 00	Botswana 00	Cameroon 00	Central African Republic 00
Cote d'Ivoire 00	Democratic Republic of Congo 00	Egypt 00	Ethiopia 00	Gambia 00
Ghana 00	Kenya 00	Lesotho 00	Malawi 00	Mozam-bique 00
Namibia 00	Nigeria 00	Rwanda 00	Senegal 00	Sierra Leone 00
Somalia 00	South Africa 00	Sudan 00	Tanzania 00	Togo 00
Tunisia 00	Uganda 00	Zambia 00	Zimbabwe 00	

Acknowledgements

The Londa 2025 report features 29 African country reports authored by African digital rights researchers. Paradigm Initiative appreciates their contributions aimed at positive and lasting change. We are truly grateful for the support of the editorial team, which invested time and knowledge to ensure key aspects of this publication are covered. We celebrate the ability to provide a tool of engagement that diverse stakeholders can leverage to engage duty-bearers and understand the digital rights ecosystem in Africa.

CONTRIBUTORS

Angola - Anonymous

Benin - Dr. Qemal Affagnon

Botswana - Oarabile Mudongo

Cameroon - Rigobert Kenmogne

Central African Republic - Arsène Tungali

Cote d'Ivoire - Steven Akomain

Democratic Republic of Congo: Noel Kabeya

Egypt - Mohamed Farahat

Ethiopia: Anonymous

Gambia: Muhammed B. Sowe

Ghana: Selassie Tay

Kenya - Miriam Beatrice Wanjiru

Lesotho - Sibongile Mokapane

Malawi - Charles Kajoloweka

Mozambique - Dércio Tsandzana

Namibia - Emsie Erastus

Nigeria - Khadijah El-Usman and Muhammed Bello Buhari

Rwanda - Louis Gitinywa

Sierra Leone - Jonette-Ann Greene

Senegal - Moussa Waly Sene

Somalia - Ayaan Khalif and Abdifatah Ali

South Africa - Claire Dehosse, Phenyo Sekati and Sophie Smit

Sudan - Anonymous

Tanzania - Anonymous

Togo - Emmanuel Elolo Agbenonwossi

Tunisia - Anonymous

Uganda - Sandra Aceng

Zambia - Chiti Mbizule Mutati

Zimbabwe - Bridgette Ndlovu

EDITORIAL TEAM

Chief Editor:
'Gbenga Sesan

Editors:
Thobekile Matimbe
Nnenna Paul-Ugochukwu
Judith Ogutu
Bridgette Ndlovu
Sani Suleiman
Giyo Ndzi
Moussa Waly Sene

Translators:
Gilmore Qhawe Khumalo (English/ French Translation)

Copy Editors:
French Copy Editor - Mouhamed Diop
English Copy Editor - Sabine Matsheka

Designer:
David Chima

A Paradigm Initiative Publication

The African Digital Rights Landscape 2025

By Thobekile Matimbe



Introduction

This consolidated edition of the Londa Report captures the state of digital rights and digital inclusion across 29 countries in Central, East, North, Southern and West Africa. The significance of this annual report lies in its succinct presentation of the gaps and developments in the reported countries and in guiding reformative actions by stakeholders, led by duty bearers comprising African States and the private sector. The consolidated report is the joint effort of PIN's editorial team, as well as in-house and external researchers who dedicate time to monitoring, documenting, and reporting occurrences that maintain, raise or lower countries' profiles regarding their digital rights and inclusion records. The Londa report calls for a multi-stakeholder approach to promoting and defending digital rights.

Country reports are drafted by digital rights researchers whose approaches are multi-faceted, combining empirical and desk research methods to assess both quantitative and qualitative aspects of digital rights and inclusion in specific countries. The assessment of state performance is benchmarked against human rights standards. The Londa Report addresses digital rights and digital inclusion, assessing them through 12 key indicators through The Score Index, developed by Paradigm Initiative as a tool for evaluating country compliance with regard to key human rights elements and is inspired by the African Commission on Human and Peoples' Rights' Declaration of Principles on Freedom of Expression and Access to Information in Africa (the Declaration)[1]. Any reference to The Score Index should reference the tool as a Paradigm Initiative Index.

1. ACHPR Declaration https://achpr.au.int/en/node/902#:~:text=The%20Declaration%20establishes%20or%20affirms,to%20express%20and%20disseminate%20information. (accessed on 5 February 2025)

Key Indicators for Assessing State Performance

1. Internet shutdowns



2. Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet
3. False News Criminalisation
4. Sedition Legislation
5. Arbitrary Arrests and Harassments of the Media, Human Rights Defenders (HRDs) and Citizens



6. Data Protection Legislation
7. States shall not require the removal of online content by internet intermediaries without due process
8. Invasion of Privacy of Communications



9. Failure by the government to proactively disclose and disseminate information on digital technologies
10. AI and Emerging Technologies National Strategies



12. Digital Inclusion
11. Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online

Table 1: The Score Index Key Indicators

An Overview of 2025

2025 was a year marked by key developments in specific countries towards a better digital rights ecosystem, while challenges affecting several thematic areas were observed. Amidst the ailing and prospering areas, at the regional level, key actions were taken to strengthen digital rights and digital inclusion. Key actions by Paradigm Initiative, such as hosting the Digital Rights and Inclusion Forum (DRIF) and presenting the reporting platform Ripoti, enabled ecosystem actors to launch regional consultations and challenge digital rights violations. PIN remained committed to monitoring the state of digital rights and inclusion in Africa[2].

Regional Developments

What is notable at the continental level to inform advocacy strides?

"The African Commission on Human and Peoples' Rights took progressive strides to guide both the private sector and governments on compliance with international human rights standards. With compliance happening, there will be a notable shift towards the realisation of freedom of expression and privacy rights in Africa." - Paradigm Initiative

2. https://ripoti.africa/

In March 2025, the African Commission on Human and Peoples' Rights (ACHPR) passed Resolution 630 on developing Guidelines to assist States monitor technology companies in respect of their duty to maintain information integrity through independent fact checking[3], calling on digital companies that provide services in Africa to adopt transparent human rights impact assessments as part of due diligence for any changes being contemplated, or for any upcoming risk situations in line with the UN Guiding Principles on Business and Human Rights, applying these assessments especially in cases of elections, health crises and the possibility of violent conflict.

The Resolution also called on the Special Rapporteur on Freedom of Expression and Access to Information in Africa (the Special Rapporteur) to develop Guidelines with all interested parties, such as civil society, regulatory bodies and technology companies, to enable States Parties to effectively monitor the platforms' performance in order to inform of the efforts to advance information integrity online, including the role of independent fact-checking in the African context. Media Monitoring Africa and UNESCO launched consultations in compliance with Resolution 630, at the Digital Rights and Inclusion Forum held in Lusaka, Zambia, from April 29 to May 1 2025.

The ACHPR also passed Resolution 631 on working towards the assessment of public interest content in this digital era and developing guidelines to ensure a public interest element for all platforms operating in Africa[4]. The Resolution called on the Special Rapporteur to consult with African role players with an interest in broadcasting, freedom of expression, media freedom, digital rights, access to information policy and lawmaking to assess their concept of public service content in current times. It also mandated the Special Rapporteur to develop Guidelines for Member States that can assist them in developing a future-focused policy framework for universal access to public service content in Africa.

The ACHPR decided to conduct a one-year continental study on developments in the areas of freedom of expression and

3. https://achpr.au.int/en/adopted-resolutions/achprres630-lxxxii-2025
4. https://achpr.au.int/en/adopted-resolutions/631-achprres631a-lxxxii-2025

access to information in the digital era, with a view to reviewing and updating the Model Law on Access to Information for Africa[5]. This was adopted in August 2025 in Resolution 639 on the need to undertake a study on the review of the Model law on Access to Information for Africa. This is an advocacy inroad, calling on diverse stakeholders to cooperate with the Special Rapporteur to support this study.

Concerned by continental trends on decreased voter turnout during general elections, shrinking civic space during electoral campaign periods and the violation of various human and peoples' rights prior to, during and in the aftermath of elections, the ACHPR adopted Resolution 648 on strengthening electoral integrity in Africa[6] in October 2025 which calls on African States to embrace and legislate for a more open civic space including in the digital sphere and expunge restrictive laws that hinder freedom of assembly, association, and expression, which are critical to robust political participation.

Appreciating the regional strides in the year towards an enabling digital rights environment, the reflections by the ACHPR Special Rapporteur on Freedom of Expression and Access to Information complement the strides documented in this report on the state of digital rights in Africa in 2025.



5. https://achpr.au.int/en/adopted-resolutions/639-achprres639-lxxxiv-2025
6. https://achpr.au.int/en/adopted-resolutions/648-achprres648-lxxxv-2025

Reflections from the ACHPR Special Rapporteur on Freedom of Expression and Access to Information

The digital age has ushered in a completely new critical environment where technology has made access to information so much easier and information can reach a wider audience. However, it has also highlighted inherent risks associated with the digital sphere, namely the risks of surveillance, data misuse, and algorithmic discrimination, to name a few. Human rights, as enshrined in the African Charter on Human and Peoples' Rights (the African Charter), must apply online as they do offline. My mandate as Special Rapporteur for Freedom of Expression and Access to Information with the African Commission on Human and Peoples' Rights (the Commission) is to ensure that freedom of expression and access to information in terms of Article 9 of the African Charter thrive in both spaces. My mandate also calls upon me as Special Rapporteur to remind States to refrain from stifling these rights. I observed in 2025 that many times the tenets of basic human rights, as embodied in the African Charter, soft law instruments such as the Declaration of Principles on Freedom of Expression and Access to Information in Africa and the Commission Resolutions, were not adhered to. Many African countries shut down the Internet at critical times when the free flow of information was vital, such as before, during and after elections. Journalists, the media and human rights defenders were also threatened, harassed, arbitrarily arrested and sometimes killed whilst performing their work. The Commission addressed such concerns through letters of urgent appeal and press statements reminding Member States of the

rights to freedom of expression and access to information. Any internet shutdown or throttling of internet services impeaches these important human rights, as per the principles enunciated in Resolution 580 on Internet Shutdowns and Elections in Africa.

It is worth highlighting that the digital environment also resulted in online harms where misinformation and disinformation harm the integrity of the information ecosystem. Measures to promote a thriving information ecosystem should safeguard human rights and build the capacity of online users to use the internet responsibly. In the Commission's Resolution 573 on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa the Commission calls on member states to align surveillance practices with human rights laws, protect privacy and personal data and implement stricter regulations on digital surveillance technologies.

In 2024, the Commission adopted Resolution 620 on promoting and Harnessing Data Access as a tool for advancing human rights and sustainable development in the digital age, which frames data access as an extension of the right to information and urges member States to create transparent policies for data held by public institutions and private companies. The draft guidelines have just been presented to the Commission at the last 86th session of the Commission and can be accessed on the website of the Commission for a 3-month period for further consultations. In 2025 the Commission passed Resolution 630 on developing Guidelines to assist States monitor technology companies in respect of their duty to maintain information integrity through independent fact checking sending a clear message for the protection of rights online through independent fact checking. The Commission at the same time also adopted Resolution 631 on working towards the assessment of public interest content in this digital

era and developing guidelines to ensure a public interest element for all platforms operating in Africa mandating me to consult with African role players with an interest in digital rights, media freedom and access to information policy and lawmaking to assess their concept of public service content and to develop Guidelines for governments in Africa that can assist them in developing a future-focused policy framework for universal access to public service content in Africa. To this end, I urge all State parties as well as CSOs and platforms to engage meaningfully with the Commission in relation to these resolutions by making submissions in relation to all these resolutions. These three resolutions will be used to update the model law on Access to Information to cater for the digital era.

The digital era is characterised by information technology, computers, the internet, A1 and it is transforming the information landscape. The potential for information access is enormous, provided these tools are used responsibly and the human rights components are in-built.

Hon Geereesha Topsy-Sonoo

Special Rapporteur on Freedom of Expression and Access to Information in Africa, African Commission on Human and Peoples' Rights

Countries Cautioned on Digital Rights by the ACHPR

Country	ACHPR Resolutions/Press Releases	Key Calls on the Country
Tanzania	Resolution 640 Resolution on the Human Rights Situation in the United Republic of Tanzania[7]	Ensure freedom of expression and access to information, during the electoral period, including providing unrestricted and uninterrupted access to the internet.
Tanzania	Press release on the Nationwide Internet Outage on Election Day in the United Republic of Tanzania	Refrain from ordering the interruption of telecommunications services, shutting down the internet, and/or disrupting access to any other digital communication platforms before, during or after the elections.
Cameroon	Press release on the human rights situation in the Republic of Cameroon	To guarantee freedom of expression, noting internet shutdowns of concern. Exercise its duty of protecting human rights in the country, by ensuring that the citizens' right to freedom of expression and access to information are respected and protected.

Table 2: Countries cautioned by ACHPR

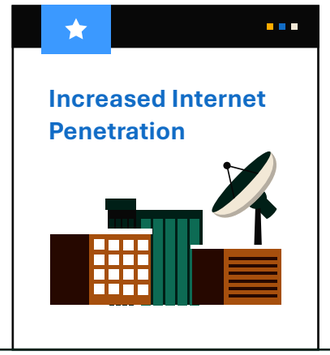
In June 2025, the African Union (AU) adopted the AU Continental Education Strategy for Africa 2026-2035, with Strategic Area 1 on Resources and Enabling Environment, citing Objective 2, which focuses on upgrading curricula to reflect current and emerging challenges. Under this objective, countries are urged to promote digital literacy in education curricula, integrating Artificial Intelligence (AI). The strategy also notes the digital inclusion challenge in Africa, affecting the right to education, citing that many schools lack access to ICT equipment, the internet, and electricity. Digital inclusion is referenced as problematic in country reports in this Londa edition. This strategy reinforces the need to prioritise internet access and digital literacy in underserved communities.

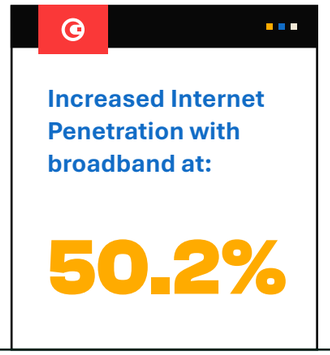
7. https://achpr.au.int/en/adopted-resolutions/640-achprres640in -lxxxiv-2025

Unpacking Londa Highlights

Internet Access

Internet access in Africa remained a key gap, a carryover from Londa 2024, that also had 8 reported countries that shut down the internet. Some countries, like Somalia, increased their internet penetration in the phase of implementation of a new Digital Transformation Strategy (2025–2030)[8]. Tunisia also showed a stable increase in internet penetration with broadband internet at 50.2% while mobile data at 89.3%[9]. Apart from the internet shutdowns recorded below in 2025, a concerning development in Mozambique was the enactment of Decree No. 48/2025, which legalises internet shutdowns in times of risks to public security and can be subject to abuse, violating necessity and proportionality tests of limiting rights as prescribed in international human rights law[10].







Reported Countries Recording Internet Shutdowns

Country	Type of Disruption	Period	Context
Angola[11]	Filtering	July 19, 2025	Protests
Cameroon[12]	Filtering	October 23, 2025	Political tensions & demonstrations.
DRC[13]	Filtering	February 25, 2025	Security & conflict
Kenya[14] Kenya[15]	Filtering	May 2025 June 25, 2025	Protests
Sudan[16]	Filtering	July 7-10, 2025	Examinations
Tanzania	Total blackout	October 29, 2025	Elections
Togo[17]	Filtering	From June 26, 2025 and ongoing	Political unrest

8. Digital Inclusion Policy: https://moct.gov.so/en/wp-content/uploads/2025/08/Somalia-Digital-Inclusion-Policy_High-Level-Policy-document.pdf (Accessed 20 February 2026)
9. INTT, "Tableau de bord trimestriel TR2- 2025", https://www.intt.tn/upload/files/TB-Trimestriel-TR2-2025.pdf (Accessed on 15 November 2025)
10. Club of Mozambique, Mozambique introduces new regulation to tighten telecom traffic control and security https://clubofmozambique.com/news/mozambique-introduces-new-regulation-to-tighten-telecom-traffic-control-and-security/, accessed on 4 January 2026. See also Principle 9 of ACHPR Declaration of Principles on Freedom of Expression and Acces to Infomation in Africa https://achpr.au.int/en/node/902
11. Cloudfare. Online Outages Q32025. https://blog.cloudflare.com/q3-2025-internet-disruption-summary/
12. https://x.com/netblocks/status/1981323147333833165 (Accessed 15 February 2026)
13. Paradigm Initiative. Press release-Net Rights Coialition condemns internet shutdown in Goma. https://paradigmhq.org/press-release-net-rights-coalition-condemns-internet-shutdown-in-goma-drc/ (Accessed February 15 2026)
14. IFreedoms. Telegram down in Kenya despite court orders to bar blockage. https://ifreedoms.co.ke/2025/06/telegram-down-in-kenya-despite-court-orders-to-bar-blockage/ (Accessed February 17 2026)
15. Netlocks https://x.com/netblocks/status/1937850265597534670 (Accessed 19 February 2026)
16. Cloudfare. Q3 2025 Internet disruption summary) https://blog.cloudflare.com/q3-2025-internet-disruption-summary/#sudan (Accessed 19 February 2026)
17. Pulse. Internet Society. Blocking of Internet services in Togo. https://pulse.internetsociety.org/en/shutdowns/blocking-of-services-in-togo/ (Accessed 18 February 2026)

Country	Type of Disruption	Period	Context
Nigeria	Filtering	From August to October 2025 in Zamfara North[18] and in Birnin Gwari since 2021[19]	Organised crime and infrastructure failures
Uganda[z]	Filtering	Ongoing since 2021	Elections

Table 3: This table lists the countries and contexts during which internet shutdowns are deployed.

Freedom of Expression

To promote and protect human rights, national human rights institutions play a critical role. In 2025, Paradigm Initiative engaged with the NHRIs in Ghana, Nigeria and Uganda as part of raising awareness and increasing accountability for digital rights. Somalia had not had a national human rights institution, and one notable win for human rights protections in the country was the signing into law of

18. Access Now . Press release- Keepiton-Authorities in Nigeria must reconnect people in Zamfara North. https://www.accessnow.org/press-release/keepiton-authorities-in-nigeria-must-reconnect-people-in-zamfara-north-now/ (Accessed March 3 2026)
19. Humanglemedia. Birnin-Gwari is still offline three years after nigerias telecom shutdown. https://humanglemedia.com/birnin-gwari-is-still-offline-three-years-after-nigerias-telecom-shutdown/ (Accessed March 9 2026)
20. https://allafrica.com/stories/202405270409

To promote and protect human rights, national human rights institutions play a critical role

the establishment of the Independent National Human Rights Commission on 10 December 2025[21]. It is hoped that this NHRI will, from the onset, take oversight over digital rights protections in the country, including addressing freedom of expression, access to information and privacy rights.

The state of free expression was marred by the criminalisation of news, with countries like Kenya still using Section 23 of the Computer Misuse and Cybercrimes Act No. 5 of 2018 to arrest people for false news. However, some judiciaries applied a human rights lens in adjudication, promoting freedom of expression. July 6 2025 saw Malawi's impanelled Constitutional Court declare section 200 of the Malawi Penal Code, which criminalised defamation, unconstitutional[22]. Media freedom continued to suffer attacks with countries like Malawi, Somalia, Ghana and Tunisia recording a series of arbitrary arrests of journalists, political actors and human rights defenders at the hands of penal codes, digital codes addressing electronic communications or cyber crimes.



21. Signing the law of the Independent National Human Rights Commission: https://www.hiiraan.com/news4/2025/Dec/203885/somali_president_signs_law_establishing_independent_national_human_rights_commission.aspx (Accessed February 26, 2026)
22. Nation Publications Limited 'Court outlaws criminal defamation provision', 16 July 2025 https://mwnation.com/court-outlaws-criminal-defamation-provision/ (Accessed November 30 2025)

Gendered Threats

The online space was marked by misinformation and disinformation as areas that require multistakeholder approaches to address challenges. Technology-facilitated gender-based violence (TFGBV) was noted in countries like Tanzania and Uganda, with the main cyber threats including online threats and hate campaigns targeting women. TFGBV incidents were also heightened in political seasons, as highlighted in the Togo country report. The incidence of TFGBV in Africa remained a key concern across Africa, raising concerns as to approaches being deployed to curb this gendered pandemic[23]. In Ethiopia, TFGBV was also highlighted as challenging with the use of deepfakes a major concern, especially for women.



23. Paradigm Initiative. Clicks that hirt an exploratory TFGBV Study of survivor narratives https://paradigmhq.org/report/clicks-that-hurt-an-exploratory-tfgbv-study-of-survivor-narratives/ (Accessed March 3 2026)

Privacy and Surveillance

Privacy concerns were noted in country reports covering public space surveillance and communications surveillance. Malawi raised concerns[24] in January 2025, after MACRA reportedly procured a tool to monitor online misinformation and disinformation, following new reports that authorities had acquired a surveillance system. In South Africa, the problematic Privately-Owned Closed-Circuit Television Surveillance Camera By-law, adopted by the City of Johannesburg seeking to regulate installation and operation of private CCTV cameras, was repealed after its enactment in 2025, following privacy outcries by civil society actors demonstrating the power of advocacy.

The Gambia was the only reported country that adopted a data protection law in 2025, from the 29 reported countries, with adoption taking place on 29 September 2025. In 2025, data breaches and cyber threats occurred across the continent, with breaches in Kenya attributed to telecommunications companies' failure to safeguard personal data. The DRC violated communications, ordering several takedowns of content and blocking specific websites. In Nigeria, Google's transparency data showed 6 content takedown requests via court orders, two requests from government officials, and one from the police, with compliance ranging from 50% to 100%.

Concerning data breaches and cyber crimes that happened in countries like Somalia, where there was a security breach of their e-visa platform, exposing the personal data of visa applicants was noted[25]. This necessitates governments rolling out e-platforms and e-services and being more vigilant, with strengthened capacities to secure their platforms and guard against cyber attacks. Paradigm

24. Paradigm Initiative. Press release- Civil society groups call for digital rights protection in Malawi's upcoming general election. https://paradigmhq.org/press-release-civil-society-groups-call-for-digital-rights-protection-in-malawis-upcoming-general-election/ (Accessed March 4 2026)
25. The 2025 E-Visa breach: https://www.aljazeera.com/news/2025/12/18/new-somalia-evisa-security-puts-passport-details-of-thousands-at-risk (Accessed 30 November 2025)

Initiative recorded a litigation win where, in 2025, the Federal High Court in Abuja, Nigeria, set a precedent judgment against the Domino's Pizza company for using a customer's data for direct marketing purposes. The court ruled that the restaurant's use of the applicant, Chukwunweike Araka Akosa's, data for direct marketing was unlawful and violated Section 37 of the Constitution of Nigeria and Sections 25 and 26 of the Nigeria Data Protection Act, 2023[26].



Access to information

Countries like the DRC remained without an access to information law, showing no commitment to proactively provide information to citizens. In Nigeria, the media reported challenges with access to information, while proactive disclosures were not forthcoming across the continent. In Mozambique, there are numerous concerns about information requests not being responded to, and proactive disclosures are not practised. This is a challenge also noted in the Togo, Zimbabwe and Sierra Leone country reports. The need for proactive disclosures

26. Paradigm Initiative. Press Release- Paradigm Initiative applauds countries with data protection laws. https://paradigmhq.org/press-release-paradigm-initiative-applauds-countries-with-data-protection-laws/ (Accessed 17 February 2026)

is key to managing the information ecosystem, ensuring information integrity, especially during elections. This is an area that governments need to address, in compliance with country constitutions that acknowledge and entrench access to information as a fundamental right in the reported countries.

Digital Inclusion

Bridging digital divides and enhancing connectivity remains a pressing need in Africa. To this end, implementation and utilisation of the Universal Service Funds (USF) is a critical tool to better address digital gaps in Africa's underserved communities. The Botswana Communications Regulatory Authority (BOCRA) accounted for its Universal Access and Service Fund (UASF), a fund amounting to approximately P44.6 million (approximately US$3.39 million) supporting connectivity initiatives[27]. Malawi is reported to have embarked on 2025 with a USF budget of about US$7.5 million (MK13.1 billion), with implemented projects estimated at US$6.8 million[28]. A drive towards improved connectivity is required for Africa's digital development to be a reality in achieving the Sustainable Development Goals. This Londa report still emphasised the need for bridging digital divides for women and persons with disabilities (PWDs), increasing access to assistive technologies for PWDs. In March 2025, Namibia officially launched the Universal Service Fund (USF) with a series of initiatives in the year towards advancing connectivity[29]. Countries like Somalia have no USF in place, restricting the potential to scale connectivity initiatives.

27. Ibid
28. USF Key Informant Interview
29. https://economist.com.na/96240/technology/communications-regulator-launches-universal-service-fund-to-boost-ict-access/

Child Online Safety

Most African countries still lag behind in addressing safety in the digital age. With the Children's Acts not yet amended to include digital safety, there remains a need to adopt laws that address online child safety. Countries like Benin, Sierra Leone, the Democratic Republic of Congo (DRC), and Ethiopia lacked such laws or policies. Nevertheless, in 2025 a few countries adopted child online safety policies. Kenya issued the child online protection and safety industry guidelines, also promoting digital literacy for children[30]. Lesotho launched its Child Online Guidelines, developed in 2024[31] and Tunisia adopted the National Charter for the Protection of Children Online in November 2025[32].

> **With the Children's Acts not yet amended to include digital safety, there remains a need to adopt laws that address online child safety.**

30. Communications Authority of Kenya 'Industry Guidelines For Child Online Protection and Safety In Kenya April 2025' https://www.ca.go.ke/sites/default/files/2025-04/%20Industry%20Guidelines%20for%20Child%20Online%20Protection%20%28COP%29%20and%20Safety%20in%20Kenya_Apr2025.pdf (accessed on 19 February 2026).
31. https://lca.org.ls/wp-content/uploads/filr/3941/CHILD-ONLINE-PROTECTION-GUIDELINES_FINAL-2.pdf
32. "Un pacte national pour protéger les enfants dans l'espace numérique" [A National Pact to Protect Children in the Digital Space], Mosaique FM, November 2025, https://www.mosaiquefm.net/fr/national-tunisie/1481005/un-pacte-national-pour-proteger-les-enfants-dans-l-espace-numerique (accessed on 29 January 2026)

AI and emerging technologies

According to the Global Table of National AI Strategies[33], 17 African countries have national AI strategies, showing a slow but improving AI governance landscape compared to 2024. Countries like Kenya[34], Zimbabwe[35] and Zambia[36] developed their National AI strategies in 2025, amid concerns about inadequate engagement with key stakeholders. Egypt[37] launched a second edition of their national AI strategy for 2025-2030, the first launched in 2021, highlighting AI's obligation to respect human rights, safeguard privacy, and promote social justice. The first edition launched in 2021 was development-based, while the second edition leans on human rights, guidance prescribed by the AU Continental AI Strategy[38] that embeds human rights as key in AI governance.

Reported Countries new with Data Protection Laws

The Gambia

Date of Enactment:
November 7, 2025

33. https://worldprivacyforum.org/posts/ai-strategies/
34. ICT. Kenya's AI Startegy 2025-2030. https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf (Accessed January 22 2026)
35. Veritas. Zimbabwe National AI Strategy. https://veritaszim.net/sites/veritas_d/files/Zimbabwe%20National%20Artificial%20Intelligence%20Strategy.pdf (Accessed February 28 2026)
36. Ministry of Technology and Science. Zambia AI Strategy. https://www.mots.gov.zm/wp-content/uploads/2025/02/Zambia-Ai-Strategy-Book-option-2.pdf (Accessed November 12 2025)
37. AI.GOV. AI Strategy. https://ai.gov.eg/SynchedFiles/en/Resources/AIstrategy%20English%2016-1-2025-1.pdf (Accessed November 7 2025)
38. African Union. Continental AI Stategy. https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf (Accessed November 2 2025)

Universal Service Funds

Country	Existing USF as per law.	USF Being Implemented	Accessible USF information on websites
Uganda	Yes	Yes	Yes
Namibia	Yes	Yes	Partially
Nigeria	Yes	Yes	Yes
Mozambique	Yes	Yes	No
Sudan	Yes	Yes	No
Tanzania	Yes	Yes	No
Tunisia	Yes	Partially	No
Zambia	Yes	Yes	No
Benin	Yes	Yes	No
Central African Republic	Yes	Partially	Partially
Democratic Republic of Congo	Yes	No	No
Senegal	Yes	Yes	No
Togo	Yes	Yes	No
Egypt	Yes	Yes	No
Ethiopia	Yes	Yes	No
Ghana	Yes	Yes	No
Rwanda	Yes	Yes	Partially
South Africa	Yes	Yes	Partially
Kenya	Yes	Yes	No
The Gambia	No (existing law, USF not yet established)	No	No
Lesotho	Yes	Yes	No
Angola	Yes	Yes	No
Zimbabwe	Yes	Yes	No
Botswana	Yes	Yes	No

Country	Existing USF as per law.	USF Being Implemented	Accessible USF information on websites
Malawi	Yes	Yes	Partially
Cote d'Ivoire	Yes	Yes	No
Sierra Leone	Yes	Yes	No
Cameroon	Yes	Yes	No
Somalia	No	No	No

2025 Findings from Ripoti[39]

Ripot is PIN's continental-wide reporting platform, implemented with the support of Ripoti partners[40] who monitor digital rights in Africa. Ripoti's collective mission is to safeguard the digital space, ensuring that everyone enjoys their fundamental rights in the digital age. It serves as a central platform for documenting, responding to, and addressing incidents of digital rights violations. In 2025, the reporting platofrm recorded 111 digital rights violations reported through the platform from 13 African countries (Kenya, Nigeria, Uganda, Senegal, Cameroon, Ghana, Namibia, DRC, Tanzania, Zimbabwe, South Sudan, Malawi and Togo), of which 97 were verified with most of the reported incidents concerning Illegal access and misuse of personal data, internet access restrictions and technology facilitated gender based violence. There is a need for digital rights actors to continue using the platform effectively to report cases and contribute to a continental documentation that informs various efforts, including litigation, digital security, and advocacy.

39. Ripoti. https://ripoti.africa/ (Accessed 30 November 2025)
40. Ripoti. About us https://ripoti.africa/about-us (Accessed 30 November 2025)

Conclusion

The Londa 2025 Report presents the level of compliance by African countries with human rights obligations, demonstrating that some countries, such as the DRC, have regressed in their compliance with digital rights, while others, such as Ghana and Botswana, have slightly improved. Concerns about freedom of expression, access to information and privacy persisted in the year. However, at the regional level, key accountability calls were made on some governments to secure digital rights and address violations. The role of stakeholders, such as the media, remained critical to addressing the information ecosystem, while civil society actors, such as Paradim Initiative (PIN), monitored it and engaged governments, private-sector actors, and regional accountability mechanisms to seek redress for concerns in the space. The country reports make critical recommendations for reformation to be implemented by diverse stakeholders. Regional accountability agencies such as the African Union and the African Commission on Human and Peoples' Rights are urged to make clear calls to governments to comply with international human rights standards, among others, to keep the internet open and increase digital access. The private sector is urged to fulfil its human rights responsibilities to foster a thriving digital and online environment.

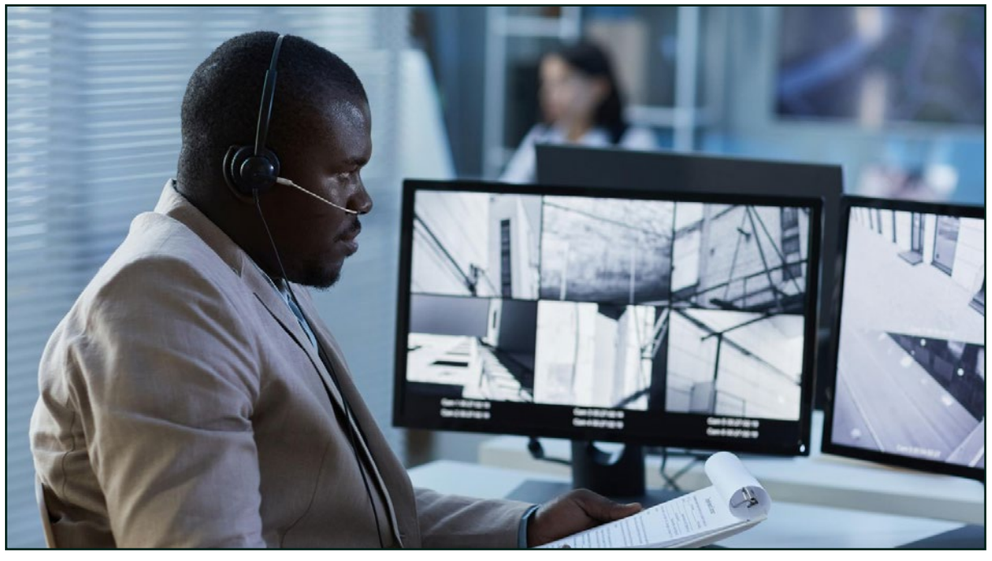
Angola

Anonymous

Executive Summary

Angola's digital landscape in 2025 shows significant progress but also faces growing human rights risks. The expansion of digital infrastructure, including the establishment of the first virtual hearing room, the ongoing development of the National Data Centre, and connectivity improvements, demonstrates a commitment to digital transformation. However, these advances are weakened by restrictive laws, suspected shutdowns such as the July 2025 disruption during nationwide protests, increased surveillance, harassment of online users, and rising online gender-based violence that is not reflected in national statistics. Despite the draft revision of the Data Protection Law, enforcement remains weak, cyberattacks are rapidly increasing, and transparency around content governance and public information remains limited. Rural and marginalised communities continue to face substantial barriers to digital literacy and access, while major national strategies near completion show no clear outcomes.

To protect civic space and promote inclusive digital transformation, this report recommends that the Government should lower connectivity costs, ban shutdowns, reform laws that criminalise online expression, enhance data protection systems, and increase transparency in platform governance and management of the Universal Service Fund. Additional priorities include developing a rights-based AI framework, regulating biometric surveillance, and investing in community-led digital literacy. Civil society is encouraged to monitor violations, support survivors of tech-facilitated violence, strengthen youth- and community-led advocacy, track public investments in connectivity, and bolster regional solidarity on digital rights. Collectively, these measures aim to ensure Angola's digital transition upholds justice, accountability, and equitable participation. The private sector should lower connectivity costs, expand rural access, and invest in inclusive digital literacy to reduce structural inequalities. At the same time, companies must strengthen transparency, resist unlawful shutdowns, safeguard data and AI systems, and address online gender-based violence to ensure Angola's digital transformation is rights-respecting and equitable.





Angola is advancing its digital transformation by expanding infrastructure, including its first virtual hearing room, the National Data Centre, and improved connectivity.

Angola's progress is undermined by restrictive laws, suspected internet shutdowns (notably during the July 2025 protests), increased surveillance, and rising online gender-based violence.

Weak enforcement of data protection laws, surging cyberattacks, and limited transparency in content governance and public information further strain the system.

Rural and marginalized communities lack digital literacy and access, while major national strategies nearing completion show few clear results.

Introduction

Digital transformation in Angola is reshaping governance, public services, and civic participation, driven by increased investment in broadband expansion, e-government tools, and emerging technologies[1]. Yet this progress occurs within a constrained digital rights environment characterised by restrictive legal reforms, rising cybersecurity threats, and ongoing gaps in privacy protections. While efforts to modernise the data protection framework suggest heightened attention to rights risks, implementation capacity and transparency remain limited. Parallel concerns, such as the expansion of surveillance technologies, opaque interactions with global platforms, and widespread online gender-based violence, emphasise the need for stronger safeguards. As digitalisation advances, rural and marginalised communities continue to face barriers related to affordability, infrastructure, and digital literacy. This report examines these dynamics across seven thematic areas to provide a comprehensive overview of Angola's digital rights landscape in 2025.

Internet Access

Angola has made progress, albeit unevenly, in expanding connectivity. The country recorded 17.2 million internet users at the start of 2025, representing 44.8% of the total population, an increase of approximately 3.1% in user numbers since January 2024[2]. There has been no change in the overall penetration rate. This can be attributed to population growth outpacing digital inclusion. Mobile networks remain the dominant access mode, with most

1. Transformative Legal Experts, White Paper on Information and Communication Technologies 2023-2027: Strategic Vision for ICTs in Angola, Available at https://www.plmj.com/xms/files/07_Guias_e_Manuais/2025/Colab_-_Livro_branco_-_TIC_EN.pdf#:~:text=In%20order%20for%20the%20digital%20transformation%20in%20Angola%20to%20enable%20the&text=on%20improving%20public%20services%20and%20promoting%20digital%20interaction%20between%20citizens%20and%20the. accessed November 18, 2025
2. Kemp, S (2025), Digital 2025: Angola, Available at Digital 2025: Angola — DataReportal – Global Digital Insights accessed November 18, 2025

users connecting via smartphones and mobile broadband.

High prices remain a significant access barrier. The 2024 Londa report highlighted that mobile data consumption accounted for up to 9.5% of average income amongst multidimensionally poor individuals[3]. The percentage was far above the UN Broadband Commission for Sustainable Development's broadband advocacy target of 2%[4]. Although the nominal cost of mobile data in Angola appears relatively low in 2025 at approximately US$1.01 per 1GB[5],affordability cannot be assessed solely by price but rather relative to purchasing power. In the country, widespread economic vulnerability significantly constrains effective access. With approximately 42.5% of the population living below US$3 per day[6], a substantial share of households face severe income constraints. Consequently, while headline data prices may appear affordable relative to national averages, they remain inaccessible to a large proportion of the population due to persistent poverty and income inequality.

Thus, the issue in Angola is not solely the nominal price of mobile data, but rather the structural economic precarity that reduces real affordability. The continued high percentage of people living below the poverty line underscores the gap between theoretical affordability benchmarks and lived economic realities.

Geographical inequalities continue. Urban centres like Luanda, Benguela, and Huíla benefit from stronger cellular networks and public Wi-Fi initiatives supported by the Universal Service Fund (FADCOM). Meanwhile, remote provinces still experience weak signals, limited tower coverage, and frequent power outages. The National Broadband Plan (2016–2025) and the Digital Transformation Strategy (2020–2025) have not yet been fully implemented, and there is limited public information on progress, budgets, or rural deployment. Nevertheless, the government indicated in 2025 its aim to reach network coverage targets of 93% (3G), 32% (4G), and 21% (5G) by 2027 through projects such as Connecta Angola, Angola Online, and Ngola Digital[7].

While satellite initiatives such as Angosat-2 have been presented as tools to enhance national coverage and e-government services, they have not yet translated into affordable, reliable broadband for most marginalised communities. For women, young people, people with disabilities and rural communities, connectivity is still mediated by shared devices, cyber-cafés or public wi-fi spots, often with limited privacy and safety.

Freedom of Expression

The environment for freedom of expression, particularly online, remains fragile and contradictory. In January 2025, the release of social media influencer Neth Nahara and four other government critics, all imprisoned for peaceful expression and protest, represents a significant victory for human rights defenders and digital rights campaigners[8]. Nehara was arrested in 2023 for 'outrage against the state, its symbols, and bodies' after posting a TikTok video criticising President João Lourenço.

Despite this positive development, the National Security Law and Anti-Vandalism Law, both enacted in 2024, provide authorities with broad discretion to interfere with media and telecommunications, restrict content, and criminalise protest activity that disrupts public services, including digital services. Article 36 of the National Security Law authorises the government to prohibit broadcasts and "disrupt telecommunications services" in vaguely defined exceptional circumstances, enabling

3. Paradigm Initiative (2024), Digital Rights and Inclusion in Africa Report, Available at https://paradigmhq.org/wp-content/uploads/2025/04/Londa-2024-2.pdf accessed November 18, 2025
4. For more information on the broadband advocacy target, see https://www.broadbandcommission.org/advocacy-targets/2-affordability/
5. Bestbroadbanddeals (2025), The cost of 1GB of mobile data in 237 countries, Available at https://bestbroadbanddeals.co.uk/mobiles/worldwide-data-pricing/ accessed November 18, 2025.
6. World Bank (2025), Macro Poverty Outlook: Angola, Available at https://thedocs.worldbank.org/en/doc/bae48ff2fefc5a869546775b3f010735-0500062021/related/mpo-ago.pdf accessed 15 November 2025.
7. GlobalValidity (2025), Angola: National Strategy Expands Internet Access and Digital Inclusion, Available at https://globalvalidity.com/angola-national-strategy-expands-internet-access-and-digital-inclusion/ accessed November 18, 2025
8. Amnesty International (2025), Angola: Five government critics released after more than a year of arbitrary imprisonment, Available at https://www.amnesty.org/en/latest/news/2025/01/angola-five-government-critics-released-after-more-than-a-year-of-arbitrary-imprisonment/, accessed November 18, 2025

disproportionate restrictions on online expression and information flows[9].

On July 19 2025, between 12:45 and 15:45 UTC, Angola experienced an internet disruption with the largest mobile network provider, UNITEL, recording a 95% drop in traffic[10]. While UNITEL attributed the outage to public road works,civil society organisations argued that the government directed the shutdowns due to nationwide protests over rising fuel prices and school fees, which were met with heavy police repression[12].

> **It is no coincidence that the internet shut down on the day of the protests. The government obviously shut it down yet feigned ignorance.**
>
> Key Informant A

This episode confirms long-standing fears that the government would use 2024 laws to justify shutdowns and deepen digital repression. In response, civil society organisations, including OMUNGA, Friends of Angola, Upange, FORDU and ALDA, condemned the shutdown and called on the Attorney General's Office to investigate it[13]. However, the Attorney General's Office has not investigated the shutdown.

Beyond formal laws, self-censorship persists. Journalists, bloggers, and social media users report being monitored by

9. Freedom House (2025), Freedom on the Net 2025: Angola, Available at Angola: Freedom on the Net 2025 Country Report | Freedom House, accessed November 18, 2025
10. Belson, D (2025), Online Outages: Q3 2025 Internet Disruption Summary, Available at https://blog.cloudflare.com/q3-2025-internet-disruption-summary/, accessed November 18, 2025
11. Unitel Angola (2025), Available at https://x.com/unitelao/status/1946644209370358120 accessed November 18, 2025
12. Lusa (2025), Angola: Internet Cut for Saturday Protests, anti-democratic, dictatorial- NGOs, Available at https://www.aman-alliance.org/Home/ContentDetail/92713, accessed November 18, 2025
13. As above.

the National Information Services Agency (SINS) and facing harassment and threats for critical content[14].

> **Neth Nahara's case is an example of why we self-censor. What you say online has grave implications for your physical safety.**
>
> Key Informant A

Online gender-based violence (OGBV) remains a critical and insufficiently addressed issue in Angola. The 2024 Londa report indicated that nearly 60% of women politicians have experienced various forms of online harassment, highlighting how digital spaces are increasingly becoming extensions of offline patriarchal violence. However, national policies and data systems have not kept up with this growing threat. The country's 2024 Multi-Indicator Health Survey (released in 2025) included statistics on physical, sexual, and emotional violence but completely omitted OGBV, reflecting a persistent gap in national acknowledgement and measurement. This lack of official statistics reflects a broader policy oversight that leaves survivors without protection, redress, or visibility, thereby reinforcing digital impunity and undermining national response mechanisms.

International indexes also reflect constraints related to freedom of expression. Freedom House's 'Freedom on the Net' 2025 report describes Angola's internet as "Partly Free", noting increased legal restrictions, surveillance, and intimidation[15]. Projections based on Reporters Without Borders (RSF) data place Angola at 100th out of 180 countries in the 2025 World Press Freedom Index- slightly better than 2024 (104th), but still indicative of structural constraints on independent media[16].

14. Key Informant interview with a member of civil society on the 14th of November 2025
15. Freedom House (2025), Freedom on the Net 2025: Angola, Available at Angola: Freedom on the Net 2025 Country Report | Freedom House, accessed November 18, 2025
16. ESCWA (2025), ISPAR Index Simulator for Policymakers: Angola, Available at ISPAR | Simulator accessed November 18, 2025

Data Protection and Privacy

The Protection of Personal Data Law (Law 22/21) remains the backbone of the country's data protection framework. However, the law is still in the early stages of implementation. The data protection authority's capacity, resourcing, and visibility remain limited, and there is little public information on enforcement actions, sanctions, or guidance issued to state agencies and private companies. On March 17 2025, the Government of Angola released a draft revision of the Personal Data Protection Law for public consultation, signalling its intention to modernise the legal framework in line with rapid digitalisation and the need to balance innovation, security, and citizens' rights[17]. The proposal introduces more precise definitions for key concepts, including pseudonymisation, anonymisation, genetic data, and biometric data. It designates "special data" to include sensitive information related to belief systems, organisational membership, private life, origin, health, sexual life, sexual orientation, and biometric and genetic identifiers[18].

Angola remains among the countries most affected by cyberattacks[19]. Organisations experienced an average of 3,648 attempted breaches per week in 2025[20]. Despite the existence of the National Cybersecurity Strategy (2021–2030) and the Cybercrime Law, the speed and complexity of cyber threats continue to surpass institutional preparedness. Gaps in enforcement, limited technical capacity, and weak cross-sector coordination mean the country's cybersecurity infrastructure continues to struggle to provide sufficient protection for citizens, public institutions, and essential services.

17. 360 Mozambique (2025), Angola launches Public Consultation on fake news and Cybersecurity Laws, Available at https://360mozambique.com/world/angola/angola-launches-public-consultation-on-fake-news-and-cybersecurity-laws/ accessed November 18, 2025
18. 360 Mozambique (2025), Angola launches Public Consultation on fake news and Cybersecurity Laws, Available at https://360mozambique.com/world/angola/angola-launches-public-consultation-on-fake-news-and-cybersecurity-laws/ accessed November 18, 2025
19. Interpol (2025), Interpol Africa Cyberthreat Assessment Report 2025 4th Edition
20. Tredger (2025), Cyber Attackers zero in on Africa's Education Sector, Available at https://allafrica.com/stories/202510010028.html, accessed November 18, 2025

The deployment of smart city technologies and facial recognition cameras in Luanda continues to raise serious concerns about mass surveillance without clear safeguards. Civil society organisations warn that the government could use these tools to monitor protesters, human rights defenders, and political opponents if not subject to robust, transparent oversight mechanisms that adhere to human rights standards.

Censorship and Content Moderation

Angola's interactions with global platforms such as Meta (Facebook, Instagram), Google (YouTube), and TikTok continue to shape the digital information ecosystem. Previous transparency reports showed Angolan authorities requesting the removal or geo-blocking of content, often for alleged defamation, incitement, or "false news", with a significant share linked to political speech. The 2024 Londa Report reported 12 takedown requests from the Angolan government to Meta, 25 to TikTok, and 15 to YouTube[21]. 2025 saw a reduction in the number of cases, according to available data. Meta reported 19 total takedown requests[22], Google reported one[23] while Wikimedia and TikTok reported none. At the national level, the National Communications Institute (INACOM) does not publish regular statistics on content takedown requests, site-blocking orders, or other forms of state-mandated moderation, which weakens transparency and accountability.

In practice, the opacity from INACOM means Angolans have limited visibility into when and why content is removed, or accounts are restricted, and whether

21. Paradigm Initiative (2024), Digital Rights and Inclusion in Africa Report, Available at https://paradigmhq.org/wp-content/uploads/2025/04/Londa-2024-2.pdf accessed November 18, 2025.
22. Meta (2025), Angola Country Report, Available at https://transparency.meta.com/reports/government-data-requests/country/AO/ accessed 20 January 2026
23. Google (2025), Transparency Report: Google removal requests by the numbers: Angola, Available at https://transparencyreport.google.com/government-removals/government-requests/AO?hl=en&lu=country_request_amount&country_request_amount=period:2025H1 accessed 20 January 2026

such actions adhere to international human rights standards on necessity and proportionality.

Access to Information

The Angolan Constitution recognises the right to access information, but the legal framework remains fragmented and poorly enforced. The main instruments are the Data Protection Law (Law 22/11 – an older framework still referenced in some practices) and the Law on Access to Administrative Documents (Law 11/02), which allows citizens to request information from public authorities. Both instruments offer limited sanctions for non-compliance.

In practice, bureaucratic hurdles, broad exceptions, and a culture of secrecy limit meaningful access to state-held information, especially regarding public spending, security, telecoms regulation, and the Universal Service Fund.

As highlighted in the Londa 2024 report, digital literacy gaps intersect with these legal barriers. UNESCO estimates that more than a quarter of the population remains digitally illiterate, with rural communities, older people, women, and people with disabilities disproportionately excluded. This makes it harder for communities to navigate online portals, e-government platforms, or data dashboards, even when information is nominally available.

> **The Universal Service Fund is treated as a 'private matter'. Information is not published on how much there is and what the resources are used for. It is only mentioned sometimes in newspaper articles as contributing to increased internet access**
>
> Key Informant A

AI and Emerging Technologies

Artificial intelligence and emerging digital technologies are consistently transforming Angola's financial sector, telecommunications landscape, and public administration. A major milestone in 2025 was the launch of the Ombudsperson's Office's first virtual hearing room in Talatona, Luanda, developed in collaboration with UNDP[24]. This innovation enables citizens to lodge and track complaints more effectively, enhances the protection of their rights, and expands access to justice through digital channels. As of 2025, the initiative was in the early stages of a nationwide rollout, with 24 municipalities across 12 provinces poised to benefit[25]. This marks a significant step toward a more responsive and technology-driven public service system.

Further progress has been made on the ongoing construction of the National Data Centre, which is designed to integrate and streamline all public services. By the end of 2025, the facility had reached 75% completion, marking a significant step toward a centralised digital infrastructure for the country[26]. Once operational, the centre is expected to significantly enhance the efficiency, interoperability, and reliability of public service delivery, reducing bureaucratic delays and improving citizens' access to essential services.

Digital Inclusion

Digital inclusion remains a key challenge. Fundo de Apoio ao Desenvolvimento das Comunicações (FADCOM), the Angolan Universal Service Fund, aims to support connectivity projects in underserved areas and free public Wi-Fi initiatives. While officials report using it to build

24. Carreira, I. (2025). Digital Justice as a Foundation for Inclusive Development, Available at https://www.undp.org/angola/blog/digital-justice-foundation-inclusive-development accessed November 18, 2025
25. Carreira, I. (2025). Digital Justice as a Foundation for Inclusive Development, Available at https://www.undp.org/angola/blog/digital-justice-foundation-inclusive-development accessed November 18, 2025
26. Kassouwi, I.K (2025), Angola nears completion of National Data Centre, set for 2026 Launch, Available at https://www.ecofinagency.com/news-digital/1411-50505-angola-nears-completion-of-national-data-center-set-for-2026-launch accessed November 18, 2025

towers and expand coverage, financial allocations, project selection criteria, and impact evaluations are not proactively disclosed, which limits public oversight and transparency.

Between 2022 and 2025, the government recorded more than seven million instances of free internet access[27]. In addition, as part of its digital expansion agenda, the government had established 260 free public internet access points and 174 digital classrooms nationwide by 2025, aiming to widen connectivity and strengthen digital learning opportunities[28]. One of the beneficiary institutions, Escola de Deficientes Visuais do Golf 1 in Luanda, supports students with visual disabilities, underscoring a strong commitment to inclusive education[29]. While these investments represent meaningful progress, their concentration in urban centres risks reinforcing existing geographic and social inequalities. Young people with disabilities living in rural and peri-urban areas, particularly those from low-income households, remain disproportionately excluded from digital infrastructure, assistive technologies, and accessible learning environments. As a result, digital inclusion efforts, though promising, may unintentionally deepen marginalisation for young people experiencing intersecting forms of discrimination linked to disability, poverty, and rural residence.

The National Broadband Plan (2016–2025) and the Digital Transformation Strategy (2020–2025) set ambitious targets for fibre expansion, mobile coverage, and digital literacy. With both frameworks nearing their final year, implementation gaps remain especially pronounced in rural communities, peri-urban informal settlements, and areas affected by conflict or economic marginalisation. Mobile and broadband coverage are exceptionally high in Luanda, yet rural communities in provinces such as Bie, Moxico, and Cuando Cubango face inconsistent connectivity.

27. Figuereido, K. (2025).Angola regista mais de sete milhoes de acessos a internet gratuita nos ultimos tres anos, Available at https://www.menosfios.com/angola-regista-mais-de-sete-milhoes-de-acessos-a-internet-gratuita-nos-ultimos-tres-anos/, accessed November 23, 2025
28. Adelino, S. (2025). Governo fala em inclusao digital apos lancamento de 260 pontos de internt gratis e 174 salas digitais pelo pais, Available at https://angorussia.com/tech/governo-fala-em-inclusao-digital-apos-lancamento-de-260-pontos-de-internet-gratis-e-174-salas-digitais-pelo-pais/ accessed 18 November 2025
29. As above.

Although Angola has expanded digital infrastructure and connectivity in recent years, progress in access has not been matched by a comprehensive framework to safeguard children in online spaces. Existing legislation offers only partial protection. Lei 25/12 (Law on the Protection and Integral Development of Children) mandates that families, schools, communities, and the State prioritise the best interests of the child. The Código Penal de Angola criminalises online harassment, exploitation, and the dissemination of harmful content, while Lei 22/11 regulates the processing of personal data. However, these laws were not specifically designed to address the growing risks children face in digital environments, such as cyberbullying, online grooming, technology-facilitated sexual exploitation, data profiling, and exposure to harmful content. The lack of dedicated child online protection legislation, clear enforcement mechanisms, and child-centred digital literacy programmes creates substantial gaps between legal protections and the real experiences of children navigating increasingly digital spaces.

Conclusion

Angola's digital transformation is experiencing a moment of both possibility and risk. The country is investing in modern infrastructure, new justice mechanisms, and updated legal frameworks, signalling a commitment to harnessing technology for governance and development. The launch of virtual hearing rooms, progress on the National Data Centre, and expansion of connectivity initiatives demonstrate the potential for digital tools to expand access to services, strengthen accountability, and improve public administration.

However, this progress is counterbalanced by restrictive laws, opaque regulatory practices, systemic surveillance risks, and persistent patterns of repression. The events of July 2025, the increasing use of broad security legislation, and rising online gender-based violence highlight the

ongoing fragility of freedom of expression and digital safety. Implementing the new data-protection reforms, building cybersecurity capacity, and ensuring transparent, rights-based oversight over emerging technologies will be essential to prevent the digital ecosystem from becoming a site of exclusion and control. For Angola's digital transition to be inclusive and rights-affirming, stronger safeguards, public transparency, and meaningful community participation are required. This includes protecting civic space online, addressing gendered and intersectional harms, ensuring accountability for shutdowns and content restrictions, reforming access-to-information systems, and bridging the digital divide affecting rural and marginalised groups.

Angola stands at a crossroads. With deliberate, human-centred governance and strengthened institutional accountability, digital transformation can advance equity, dignity, and participation. Without such measures, it risks deepening inequalities and entrenching new forms of digital repression. The task ahead is to ensure that digitalisation becomes a tool for justice and liberation—not surveillance and silencing.

Recommendations

The Government should:

1. Reduce the cost of connectivity
- Implement tax relief or targeted subsidies for low-income users and community networks.
- Review spectrum and licensing policies to encourage competition and lower consumer prices.
2. Prohibit internet shutdowns and disproportionate disruptions
- Publicly commit to upholding Principle 38 of the ACHPR Declaration (no shutdowns), and amend the National Security and Anti-Vandalism Laws to remove provisions that allow broad telecoms disruption in "exceptional circumstances".
3. Reform laws that criminalise online expression
- Repeal or significantly amend Penal Code provisions on "false news", "outrage against state institutions" and related offences to prevent their misuse against journalists, activists, and content creators.
4. Strengthen data protection and privacy
- Fully operationalise the data protection authority with adequate budget, independence and enforcement powers.
- Adopt clear rules on the use of CCTV, facial recognition and other biometric systems, ensuring strict necessity, proportionality and independent oversight.
5. Increase transparency in content governance
- Mandate INACOM to publish periodic reports on site blocking, content takedown orders, and collaboration with platforms, disaggregated by legal basis and topic.
6. Open up the Universal Service Fund and digital strategies
- Publish annual FADCOM (USF) reports (revenues, allocations, project locations, implementers, and impact).
- Issue a public review of the National Broadband Plan and Digital Transformation Strategy as they end in 2025, co-creating the next strategy with communities, youth groups, women's rights organisations and people with disabilities.
7. Regulate AI and emerging technologies in line with human rights
- Develop and adopt a national AI framework aligned with regional standards to address discrimination, transparency, accountability, and redress.
- Prohibit AI applications that pose unacceptable risks, such as real-time biometric tracking of protesters.
8. Invest in inclusive digital literacy
- Integrate digital literacy, including online safety, gender-based violence prevention, and critical information skills, into primary and secondary curricula and non-formal youth programmes.
- Fund community-led digital literacy in rural areas, led by youth, women's and disability organisations.

Civil Society Organisations should:

1. Monitor and document digital rights violations
- Continue to document shutdowns, blocking, arrests, online violence, and data breaches, feeding evidence into regional mechanisms (ACHPR, UPR, UN Special Procedures) and initiatives like Londa.
2. Strengthen community-led and youth-led advocacy
- Support youth collectives, feminist groups and disability organisations to engage regulators, parliament and regional bodies on digital policy, shutdowns, AI regulation and data protection.
3. Track the Universal Service Fund and public investments
- Collaborate with budget-tracking and transparency organisations to monitor USF revenues and expenditures, and advocate for participatory governance of connectivity projects.
4. Support survivors of online and tech-facilitated violence
- Provide legal, psychosocial and digital security support to women, LGBTQI+ communities, human rights defenders, journalists and youth facing online harassment and surveillance.
5. Build cross-border solidarity
- Engage with regional coalitions to situate Angola's experience within broader continental struggles against shutdowns, censorship and surveillance.

Private Sector should:

1. Lower connectivity costs and reduce exclusion
- Adopt affordable pricing models for low-income users, including education-focused bundles.
- Expand rural infrastructure beyond commercially profitable areas through transparent public-private partnerships, and prioritise underserved provinces in tower deployment, broadband expansion, and service reliability.
- Ensure that digital inclusion efforts explicitly reach women, young people, persons with disabilities, and rural communities who remain structurally excluded.
2. Commit to non-participation in internet shutdowns and unlawful restrictions
- Publicly commit to respecting freedom of expression and resisting disproportionate government directives to disrupt services.
- Increase transparency by publishing information on government requests to restrict content or access, and ensure that any compliance is guided by the principles of legality, necessity, and proportionality under international human rights standards.
3. Strengthen data protection and cybersecurity practice
- Implement privacy-by-design standards across digital products and services, conduct human rights impact assessments for high-risk technologies, and ensure timely disclosure of data breaches.
- Invest in robust cybersecurity systems and cross-sector coordination to address the growing volume of cyberattacks affecting public and private institutions.
4. Improve transparency in content moderation and platform governance
- Publish accessible information on content takedown requests, account restrictions, and appeal mechanisms affecting users in Angola.
- Ensure moderation systems are culturally and linguistically responsive, and protect political speech, civic activism, and journalistic expression from disproportionate removal.
5. Address online gender-based violence and digital harms
- Develop responsive reporting and redress systems for survivors of online harassment, non-consensual image sharing, doxxing, and hate speech.
6. Increase transparency in public-private partnerships and connectivity funds
- Disclose information on contracts, funding allocations, and infrastructure projects supported through public mechanisms, such as the FADCOM (Universal Service Fund).
- Engage communities in participatory consultation processes to ensure connectivity investments respond to local needs and reduce geographic inequalities.

The Score Index

Angola, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	4	2	Although there were no confirmed shutdowns in 2024, in July 2025, reports from civil society and network measurement organisations documented a nationwide internet blackout during protests over fuel prices, marking a serious regression and demonstrating that shutdowns are now part of the state's response toolkit. Civil society organisations raised concerns, calling on the Attorney General's office to investigate, but there was no judicial pronouncement.
2. Laws and measures for universal, equitable, affordable and meaningful access	P37	3	3	Laws and strategies (National Broadband Plan, Digital Transformation Strategy, FADCOM (USF) framework) exist, but implementation, transparency, and affordability remain limited. Rural communities, women, youth and PWDs remain significantly underserved
3. False News Criminalisation	P22(2)	2	2	Penal Code provisions on "fake news" and related offences remain overly broad and open to misuse against media and activists, despite limited evidence of reform in 2024–2025.
4. Sedition Legislation	P22(2)	2	2	Offences such as "outrage against the state, its symbols and bodies" continue to exist and were used to prosecute Neth Nahara and others. While those individuals were pardoned and released, the underlying provisions remain in force.
5. Arbitrary Arrests and Harassment of Media, HRDs and Citizens	P20(1) & (2)	2	2	The release of Neth Nahara and four activists in January 2025 is a positive step, but arrests, intimidation, and violent dispersal of protests, particularly in July 2025, indicate ongoing risks for those exercising digital and offline expression.
6. Data Protection Legislation	P42	4	4	Angola has a modern data protection law, but enforcement, institutional capacity and oversight of surveillance technologies remain weak. No significant legislative backsliding occurred in 2024–2025, but implementation gaps persist
7. State interference and content removal via intermediaries	P38 & P39(4)	2	2	The state continues to request the removal or restriction of political content from platforms; lack of transparency from INACOM and limited public data from platforms hamper oversight.
8. Invasion of Privacy of Communications	P41	3	3	Legal data-protection safeguards exist, but the expansion of security powers, facial recognition and smart-city surveillance without strong oversight raises significant risks of unlawful intrusion.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
9. Failure to proactively disclose information on digital technologies	P29(3)	3	3	Some sectoral information is available, but there is no systematic disclosure of USF spending, shutdown decisions, or surveillance/AI deployments.
10. AI and Emerging Technologies National Strategies	P39(6)	2	2	Discussions on AI ethics are underway, but no dedicated AI law or strategy exists; regulations have not kept pace with the deployment of AI in finance, surveillance, and public services.
11. Children's Digital Safety and Privacy Online	P37(5)	2	2	Children's rights are protected through general child protection laws, but there is no specific framework on children's digital safety, online privacy, or platform accountability.
12. Digital Inclusion	P37(3)	2	2	Free Wi-Fi initiatives in parts of Luanda and USF-supported projects offer partial inclusion, but high costs, rural exclusion and limited accessibility for PWDs remain significant barriers.
Total (out of 60):			29	

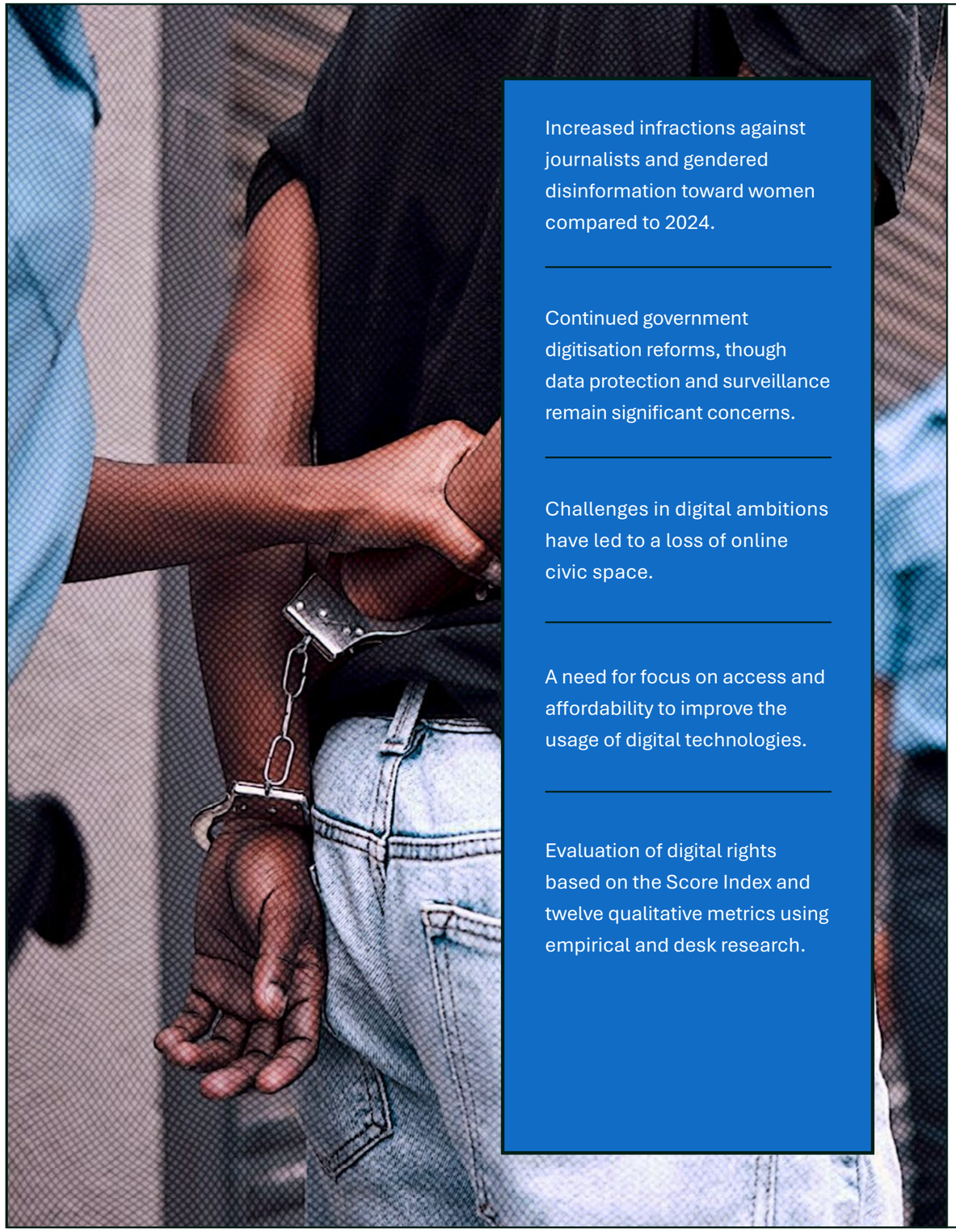


Benin

By Dr. Qemal Affagnon

Executive Summary

In comparison to the 2024 Londa report, more concerning infractions against journalists were found, and women are subjected to gendered disinformation. The government continued its strategic reforms focusing on digitisation but serious concerns remained about data protection, privacy and surveillance. If the updated national Artificial Intelligence strategy represents a cornerstone of Benin's digital ambitions, the country has faced challenges that have resulted in a loss of online civic space. Access and affordability should be given special consideration in policy decisions and the frameworks that support them in order to improve the use of digital technologies. Alongside the Score Index by Paradigm Initiative that evaluates the nation's performance on key human rights issues, the report's methodology is based on a comprehensive approach, integrating empirical and desk-research techniques to analyse the digital landscape .Using twelve qualitative metrics, this study evaluates the factors influencing digital rights and inclusion in Benin.



Increased infractions against journalists and gendered disinformation toward women compared to 2024.

Continued government digitisation reforms, though data protection and surveillance remain significant concerns.

Challenges in digital ambitions have led to a loss of online civic space.

A need for focus on access and affordability to improve the usage of digital technologies.

Evaluation of digital rights based on the Score Index and twelve qualitative metrics using empirical and desk research.

Introduction

Since 2016, Benin has made significant strides toward digitalisation in an effort to become a hub for digital services in West Africa. With the enhancement of the digital infrastructure, various reforms were implemented, including the establishment of specialised institutions. The establishment of the Ministry of Digital economy and communications in 2016 highlights the government's dedication to the digital agenda[1]. Similarly, the launch in 2020 of an extensive national public services portal is another important accomplishment[2]. From business registration to passport issuance, this site offers residents the possibility to obtain information on over 560 governmental services. The portal was created with the intention of facilitating citizens' access to public services and improving the quality of governance. Nowadays, the portal also allows its users to make and manage requests for 132 online services[3]. Despite advancements in digitalisation, the country continues to encounter major challenges like a digital divide within its population. On another level, the Internet has accelerated the rate at which misinformation has been spread in recent years, reaching more people as a result. Cybercrime is another significant concern, driven by increasing digitalisation, with a focus on cyber-enabled financial crimes like romance scams and sextortion. Also, online freedoms are being compromised by government legislation. Hate speech and malicious use of artificial intelligence continue to affect digital spaces in addition to the failure of major tech companies to prioritise rights and freedoms.

1. See Ministère de la communication : Rafiatou Monrou s'installe ! https://mamabenin.com/2016/04/07/ministere-de-la-communication-rafiatou-monrou-sinstalle/ (accessed on 04 November 2025).
2. See Lancement du Portail national des services publics: Le gouvernement rend accessible l'administration en ligne https://lanationbenin.bj/actualites/lancement-du-portail-national-des-services-publics-le-gouvernement-rend-accessible-ladministration-en-ligne (accessed on 03 November 2025).
3. See Trois nouveaux e-services disponibles en ligne https://andf.bj/liste-des-3-nouveaux-e-services-disponibles/ (accessed on 01 November 2025).

Online Freedom of Expression and Access to Information

The Constitution of Benin, 1990, as amended by Law no. 2019-40 of 7 November 2019, ensures that everyone has the fundamental right to obtain information[4]. In Article 8, the Constitution declares that the State guarantees to its citizens equal opportunities in health, education, culture, information, vocational training, and employment. The Constitution of Benin does not explicitly mention the acknowledgement of the right to access administrative information. However it refers to information in general, particularly information that the State must share with its citizens[5].

After the adoption of the Constitution, the Benin administration has been quite unclear regarding public access to information. Later, the first move towards increased transparency was made in 1996 by the Council of Ministers[6]. This initiative underlined the importance of developing user guides and procedural manuals to enhance citizens' comprehension of their right to access administrative information, and was validated by a decree in 2000.[7] Thanks to significant pressure from civil society groups, a law related to access to information was passed in 2015.[8]

However, the establishment of rules and procedures via laws on information access does not always ensure their consistent application. In recent years, alongside the issue of accessing information, journalists have begun encountering additional challenges in managing public information. Under Patrick Talon's regime, arrests and judicial harassment of journalists or digital activists have increased such that this move tends to develop as a normal behaviour. Several online media suffered cyberattacks that defaced their website pages during the reported period[9].

During the period between 2024 and 2025, Benin grappled with a surge in infringements on freedom of expression in an evolving landscape of online threats towards several journalists. An example is that of Cosme Hounsa, editor of the newspaper La Boussole[10]. The journalist was arrested by agents of the National Centre for Digital Investigations (CNIN) on charges of harassment by electronic means under the Digital Code. The incident followed a complaint filed by Minister Counsellor Rachidi Gbadamassi[11]. Even though Hounsa is free for now, he is still facing legal proceedings and may be summoned at any time as part of the judicial process. Under the Digital Code, anyone who initiates coercive, intimidating, harassing or emotionally distressing electronic communication can be charged. The same applies to anyone who initiates or relays false information against others through social networks.

Recently, the Digital Code was also applied to Olivier Allocheme, editor of the daily newspaper L'Evenement Précis. The arrest of Allocheme comes amid heightened tensions between independent media outlets and Benin authorities[12]. Physical attacks against journalists and harassment in reprisal for journalists' work are on the rise. Known for his criticism of President Patrice Talon, Hugues Comlan Sossoukpè, was first arrested in Ivory Coast and later, extradited to Benin. His case is pending a judicial investigation on charges of inciting rebellion, inciting hatred and violence, but also for harassing through electronic communication. Since 2019,

4. See Trois nouveaux e-services disponibles en ligne https://andf.bj/liste-des-3-nouveaux-e-services-disponibles/ (accessed on 01 November 2025)
5. See Problématique de l'accès de l'information administrative au Bénin https://www.memoireonline.com/12/07/739/m_problematique-acces-information-administrative-benin9.html (accessed on 09 November 2025).
6. idem
7. idem
8. See Loi N' 2015-07 DU 20 MARS 2015 portant code de l'information et Communication du Bénin https://sgg.gouv.bj/doc/loi-2015-07/ (accessed on 07 November 2025)
9. See des médias en ligne victimes de perturbations numériques https://shorturl.at/8ts7f (accessed on 05 November 2025)
10. See Benin: Newspaper editor arrested after Minister's online harassment complaint https://mfwa.org/country-highlights/benin-newspaper-editor-arrested-after-ministers-complaint-of-online-harrassment/ (accessed on 07 October 2025).
11. See Beninese journalist jailed over critical reporting (accessed on 04 November 2025). https://ifex.org/beninese-journalist-jailed-over-critical-reporting/ (accessed on 03 November 2025).
12. See Bénin : Le dossier du journaliste Olivier Allochémé reporté au 15 janvier devant la Criet https://lanouvelletribune.info/2025/10/benin-le-dossier-du-journaliste-olivier-allocheme-reporte-au-15-janvier-devant-la-criet/ (accessed on 02 November 2025)

Sossoukpè has been living in exile in Togo, under refugee status. On July 14 2025, the Court for the Repression of Economic Offences and Terrorism upheld his detention, like Steve Amoussou, a digital activist, convicted on charges of politically motivated insult and spreading false information[13].

Taking into account the cases referenced above, in addition to the extensive list of journalists who face prosecution or imprisonment, there is fear of the government continuing on this path. So far, the introduction of the Digital Code in Benin presents new obstacles to freedom of expression, limiting certain opposition media and encouraging the detention or imprisonment of journalists.

Internet Access and Disruptions

According to the latest update from the Electronic Communications and Postal Regulatory Authority (ARCEP Benin), the Beninese internet market continues to expand. Among the 14 operators who are competing, Société Béninoise d'Infrastructures Numériques (SBIN SA) and Isocel SA, maintain their dominant positions with national coverage, while intermediate players such as FirstNet SA, SUD Telecom Solutions SA, Euphorbia SARL and GVA Bénin continue to operate in major urban areas. The dominance of SBIN SA and ISOCEL SA can mainly be attributed to their ability to offer Fibre to Home solutions, a technology that offers stability and speed to customers.

Nevertheless, despite the existence of all these services, Benin still experienced significant internet service outages last year. A number of underwater telecommunications cables, including two that connect the West African country, sustained damage, which resulted in connection failure[14]. With the exception of Moov Africa and Starlink, all the telecom giants operating in Benin were affected by the outage that impacted their installations[15].

Starlink was able to avoid the outage because it uses low-Earth orbit satellites to provide internet access. It is important to note that the majority of Beninese consumers mostly rely on systems connected by physical cables. With the low-Earth orbit satellites, Starlink is attempting to bolster its presence in Benin, particularly by offering connectivity for more efficient border surveillance[16]. If it is true that digital infrastructure could enable a more effective management of areas facing terrorism in Benin, Starlink's potential can also be harmful[17]. For example, this potential brings up issues with privacy, corporate control over space infrastructure, environmental effects like space debris, and criminal organisations using it[18]. Nevertheless, a large portion of internet service is currently provided via mobile operators in Benin. Given that the nation is still developing its digital infrastructure, mobile operators are often the primary gateway to connect people, especially in areas lacking an infrastructure of fixed lines. Between 2024 and 2025, an increase in active mobile subscriptions was noted throughout the country. With almost nine million customers and a roughly 50% market share, MTN leads the Benin mobile phone industry[19].

13. See Benin: Digital activist sentenced to two years imprisonment https://mfwa.org/country-highlights/benin-activist-steve-amoussou-sentenced-fined/ (accessed on 27 October 2025).
14. See Perturbation de réseau depuis le 14 mars : Celtiis assure la continuité du service internet https://matinlibre.com/2024/03/20/perturbation-de-reseau-depuis-le-14-mars-celtiis-assure-la-continuite-du-service-internet/ (accessed on 09 November 2025).
15. See Pourquoi Maroc Telecom a échappé à la coupure internet en Afrique https://www.jeuneafrique.com/1550309/economie-entreprises/pourquoi-maroc-telecom-a-echappe-a-la-coupure-internet-en-afrique/ (accessed on 12 November 2025)
16. See Des cadres de Starlink en mission au Bénin https://www.afrique-sur7.fr/starlink-des-emissaires-delon-musk-en-mission-au-benin (accessed on 15 November 2025)
17. See Elon Musk offensif au Bénin https://mondafrique.com/decryptage/elon-musk-a-la-tete-de-starlink-mise-sur-lafrique/ (accessed on 11 November 2025).
18. See Le groupe « Starlink » d'Elon Musk, un outil de pouvoir au coeur du Sahel https://mondafrique.com/decryptage/le-groupe-starlink-delon-musk-un-outil-de-pouvoir-au-sahel/ (accessed on 13 November 2025).
19. See Inclusion financière : MTN Bénin veut accélérer sur la Fintech https://www.agenceecofin.com/actualites-numerique/1401-124902-inclusion-financiere-mtn-benin-veut-accelerer-sur-la-fintech (accessed on 10 November 2025).

Table 1: Mobile subscriptions - Change in active mobile subscriptions

Designations	T2_2024	T3_2024	T4_2024	T1_2025	T2_2025
SPACETEL BENIN	8 467 023	8 951 193	8 860 782	8587 373	8 467 024
MOOV AFRICA BENIN	6 46 9731	6 103 953	5705 177	5 938 114	5 520 384
CELTIIS	2 867 222	3 191 516	3 648 522	4 178 572	4 649 114
Total Abonnements mobiles	**17 803 976**	**18 246 662**	**18 214 481**	**18 704 059**	**18 636 522**

Source : Electronic Communications and Postal Regulatory Authority (ARCEP Benin)

In the mobile internet market, which comprises around 64.25% of Benin's Internet customers, MTN Benin and Moov Benin benefited greatly from the transition to mobile data services[20]. According to GSMA, around 3.8 million people, which corresponds to 28% of the population (48% of adults), routinely used their phones to access the Internet[21].

Table 1: Mobile subscriptions - Change in active mobile subscriptions

Designations	T2_2024	T3_2024	T4_2024	T1_2025	T2_2025
SPACETEL BENIN	6 101 371	6 265 262	6 852 058	5 283 369	4 616 644
MOOV AFRICA BENIN	3 303 734	3 169 805	2 923 627	2931 394	2 639 727
CELTIIS	1 661 841	2 289 253	2 585 697	2931 753	3317 431
Total Abonnement Internet mobile actif	**11 066 946**	**11 724 320**	**12 361 382**	**11 146 516**	**10 573 802**
Dont FEMMES	**27%**	**28%**	**26%**	**22%**	**22%**

Source : Electronic Communications and Postal Regulatory Authority (ARCEP Benin)

Canal box (GVA Bénin) is also trying to attract new clients in this competitive environment. In this regard, Canal Box (GVA Bénin) started to offer two unlimited monthly plans, including 50 Megabits per second (Mbps) for CFA15,000, approximately US$27,and 200 Mbps for CFA30,000, approximately US$53[22]. During the period covered by the report, high-speed mobile internet (3G and 4G) expanded to nearly 90% of the country[23]. Despite an increase in the number of internet subscribers between 2024 and 2025, GSMA points out that there is an increasing discrepancy between the number of individuals who have access to high-speed networks and those who actively use them[24]. Known as the usage gap, this phenomena refers to the percentage of Benin's population which is offline even though they reside close to high-speed mobile networks. According to GSMA, between 39% and 66% of Benin's population were offline despite the fact, they live near a high-speed mobile network[25].

Gendered disinformation

In Benin, a country where leadership is considered to be patriarchal, significant progress has been achieved politically in terms of gender inclusiveness in recent years. Nevertheless, tradition still retains an important influence despite evolving social perspectives. First, this situation acts as an obstacle for women wishing to engage in political affairs. In this context, gendered misinformation can be understood as the dissemination

20. See Benin: 94% mobile Internet coverage, but actual usage can improve (GSMA) https://extensia.tech/benin-94-mobile-internet-coverage-but-actual-usage-can-improve-gsma/ https://www.agenceecofin.com/actualites-numerique/1401-124902-inclusion-financiere-mtn-benin-veut-accelerer-sur-la-fintech (accessed on 05 November 2025).
21. See Benin Expands Mobile Internet, but Many Still Lack Access https://www.ecofinagency.com/telecom/1702-46429-benin-expands-mobile-internet-but-many-still-lack-access (accessed on 06 November 2025).
22. See Fiber optic internet in Benin: Canal Box triggers a price war https://extensia.tech/fiber-optic-internet-in-benin-canal-box-triggers-a-price-war/ (accessed on 08 November 2025).
23. See Benin Expands Mobile Internet, but Many Still Lack Access https://www.ecofinagency.com/telecom/1702-46429-benin-expands-mobile-internet-but-many-still-lack-access (accessed on 08 November 2025).
24. Idem
25. See New insights on mobile internet connectivity in Sub-Saharan Africa https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/new-insights-on-mobile-internet-connectivity-in-sub-saharan-africa/ (accessed on 09 November 2025).

of false or misleading information that relies on misogyny or stereotypes related to gender. For instance, Marie-Elise Gbèdo, has admitted facing challenges in navigating her aspirations in a country dominated by male politicians[26]. Marie Elise Gbèdo, the 63-year-old attorney who attempted to persuade voters to back her political campaign, lamented that, due to her gender, no one took into account her skills or accomplishments[27]. This type of disinformation generally depicts women as deceitful, lacking intelligence, or incites rivalries among women. Among those impacted by gendered misinformation in Benin are women activists, government officials, political leaders, and those in public roles. Mariam Chabi Talata, the first woman Vice President of Benin and one of the few women to hold higher positions, is among those who encounter false information based on misogyny[28].

The election in which President Patrice Talon secured a second term was fueled by gender disinformation, particularly due to the widespread availability of the Internet and smartphones[29]. During this election, Reckya Madougou, another woman in politics, has endured sexist, discriminatory, and degrading comments from multiple individuals, including those in office[30].

In addition to being detrimental, gendered misinformation can put women who are engaged in politics and governance at risk of danger. This is the case of Marie-Elise Gbèdo, a four-time presidential candidate who narrowly escaped assassination in 1998. This year, Gbèdo was attacked in front of her home by six armed men. She narrowly survived five severe shots with one hitting her chest[31]. Following the general elections on January 8 2023, the Ninth Benin Parliament (2023-2026) has 28 women Parliamentarians among 109 members[32]. This accounts for 25.69% of the overall total, compared to 7.23% of women elected in the Eighth legislature (2019-2023). The advancements noted in 2023 during the legislative elections can be linked to the reform started in 2019, via the amendment of Article 26 of the Constitution,1990 and Article 144 of the Electoral Code[33]. Despite improvements in the representation of women in decision-making bodies, gendered disinformation aimed at keeping women out of politics persists.

26. See Benin Election: Female candidate makes fourth attempt at presidency https://www.africanews.com/2016/03/04/benin-election-female-candidate-makes-fourth-attempt-at-presidency// (accessed on 18 November 2025).
27. idem
28. See Benin's first female vice-president on women's bodies, Amazon warriors and being called a feminist https://www.theguardian.com/global-development/2022/mar/15/mariam-chabi-talata-benin-first-female-vice-president-on-abortion-rights (accessed on 12 November 2025).
29. See Enlightened West African dictatorship challenged by state capture ? Insights from Benin, Togo and Senegal https://www.researchgate.net/publication/362832783_'Enlightened'_West_African_dictatorship_challenged_by_state_capture_Insights_from_Benin_Togo_and_Senegal (accessed on 08 November 2025).
30. See des doutes face aux accusations contre Reckyath Madougou https://www.dw.com/fr/des-doutes-face-aux-accusations-contre-reckyath-madougou/a-56789203 (accessed on 09 November 2025).

Data Protection and Cybersecurity

In an increasingly digitalised environment, personal data of online users can be sold for advertising, leveraged by companies to enhance productivity, or employed by governments to forecast voter turnout[34]. For example, in order to provide highly targeted advertisements, Meta's business strategy relies on collecting copious amounts of personal data[35]. However, such use and exploitation of data helped to undermine privacy, whereas the security of personal data should be considered fundamental. In Benin, the Constitution assures various fundamental rights, including the right to privacy[36]. However in reality, many Beninese users are still

31. See Présidentielle au Benin : Marie-Elise Gbèdo, une femme dans la mêlée https://www.jeuneafrique.com/296397/politique/presidentielle-benin-marie-elise-gbedo-femme-melee/ (accessed on 01 November 2025).
32. See Une amélioration de la représentativité des femmes à la 9ème législature de l'Assemblée nationale du Bénin https://www.undp.org/fr/benin/actualites/une-amelioration-de-la-representativite-des-femmes-la-9eme-legislature-de-lassemblee-nationale-du-benin (accessed on 02 November 2025).
33. See Benin republic adopts new electoral Code https://www.africanews.com/2018/09/05/benin-republic-adopts-new-electoral-code-the-morning-call// (accessed on 03 November 2025).
34. See A closer look at modern digital political advertising https://illumin.com/insights/blog/modern-digital-political-advertising/ (accessed on 04 November 2025).
35. See Mad at Meta? Don't Let Them Collect and Monetize Your Personal Data https://www.eff.org/deeplinks/2025/01/mad-meta-dont-let-them-collect-and-monetize-your-personal-data (accessed on 05 November 2025).
36. See Privacy Law at Benin https://lawgratis.com/blog-detail/privacy-law-at-benin (accessed on 06 November 2025).

unaware or do not understand their data rights, and for those, the true power of everything from geolocation data to health data is still not starkly apparent. Furthermore, many people in Benin do not understand the ways in which their data is used or the laws surrounding such. This situation raises serious human rights concerns. This is the reason why the Personal Data Protection Authority of Benin (APDP) opted to raise awareness among people in different regions of the country, regarding the importance of protecting their personal data[37]. APDP also periodically organises open days to engage with the general public. In recent months, the Personal Data Protection Authority has held these events outside Cotonou, the country's economic capital[38].

APDP is able to impose financial sanctions on data controllers who do not comply with Law No. 2017-20 of the Digital Code. The body also verifies public files and checks whether file managers comply with Law No. 2017-20 of the Digital Code. APDP also receives and investigates complaints in accordance with its mission and the law. Because APDP is expected to operate as an autonomous organisation, it must assess if the government's ongoing utilisation of personal data adheres to legal standards. Specifically, APDP is charged with the responsibility of making sure that Benin's digitisation of public services doesn't lead to or exacerbate existing data protection rules and regulations[39]. With over 560 services already offered, the digitisation of public services is advancing, but data protection and cybersecurity should not be overlooked[40].

37. See Protection des données : l'APDP quitte Cotonou pour sensibiliser tout le Bénin https://afriqueitnews.com/tech-media/protection-donnees-apdp-quitte-cotonou-sensibiliser-benin/ (accessed on 07 November 2025).
38. See Protection des données personnelles: L'APDP en campagne de sensibilisation à Parakou https://matinlibre.com/2025/06/11/protection-des-donnees-personnelles-lapdp-en-campagne-de-sensibilisation-a-parakou/ (accessed on 03 November 2025).
39. See Digitalisation des services publics : un pilier important pour le développement https://lematinal.bj/digitalisation-des-services-publics-un-pilier-important-pour-le-developpement/ (accessed on 13 November 2025).
40. See Bénin : une stratégie numérique intégrée et ambitieuse https://www.teamfrance-export.fr/infos-sectorielles/37110/37110-benin-une-strategie-numerique-integree-et-ambitieuse (accessed on 14 November 2025).

Privacy and Surveillance

In Benin, digital technologies continue to transform how citizens are able to obtain information, communicate and interact with the environment surrounding them. Yet, this progress in technology has also brought about new challenges and risks to essential human rights, such as surveillance. According to the surveillance legislation in Benin, surveillance measures apply to anyone whom there are legitimate reasons to gather information for intelligence purposes, with the exception of members of Parliament, judges, public prosecutors, and barristers during their mandate or professional activity, as well as individuals who are likely to be aware of the indictment of the President of the Republic and government members due to their statute[41].In general, this surveillance involves methods, technology, or frameworks that make control possible by identifying, tracking, monitoring, or analysing personal data. There are two forms of digital surveillance: targeted surveillance and passive surveillance. Targeted surveillance concentrates on particular people, usually by using spyware. Passive surveillance, entails wide population monitoring, such as internet monitoring, mobile phone tapping, SIM card registration, location tracking, deep packet inspection, network interception, cable tapping, and telecom surveillance.

Both types of surveillance pose significant threats to human rights and civic freedoms. For example, the right to privacy can be compromised, as constant surveillance weakens individuals' capacity to communicate, associate, or organise freely without worrying about being observed. This can also result in a significant chilling effect on the freedom to express oneself. Yet, the Constitution of Benin contains several provisions promoting freedom of expression and information. Article 23 states that everyone has the right to freedom of expression and opinion while respecting public order as stipulated in laws and regulations.

Article 24 specifically recognises and protects freedom of the press and

41. See Loi n° 2017-44 portant recueil du renseignement en République du Bénin https://lanouvelletribune.info/wp-content/uploads/2018/02/DSL-LOI-N%C2%B0-2017-44-PORTANT-RECUEIL-DU-RENSEIGNEMENT.pdf (accessed on 12 November 2025).

gives this responsibility to the Higher Authority for Audio-Visual Media and Communication. Thus, it is clear that surveillance activities constitute a violation of the Benin Constitution. In the same vein, significant privacy concerns arise from the fact that both passive and targeted monitoring frequently include the collection of personal data without consent. In such a context, these actions can violate the right to privacy, which is guaranteed under Article 8 of the Benin Constitution. At the beginning of 2025, reports of the government's interest in invasive surveillance surfaced again[42]. In previous years, these actions were conducted with Pegasus spyware[43].

Digital Inclusion of Persons with Disabilities

Article 26 of the Constitution of Benin, 1990, asserts that the State shall guarantee equal treatment under the law for everyone, regardless of origin, race, gender, religion, political views, or social status. However, one reality persists, as marginalised groups such as persons with disabilities continue to encounter exclusion and marginalisation in various social processes. In Benin, the promotion and protection of the Rights of Persons with Disabilities Act encompasses a variety of social benefits for individuals with disabilities, such as enhanced access to healthcare, education, job training, transportation, and recreational activities[44]. This act includes rules pertaining to the construction or alteration of buildings to make them accessible to persons with disabilities. Also, this Act states that schools are required to admit children with disabilities.

Additionally, the Act emphasises that the State is obligated to guarantee the right to education, instruction, and training for persons with disabilities. In the Act, kids and teens with disabilities have the right to access free and inclusive education in regular public schools. The protection of children in the digital space, including children and teenagers with disabilities in Benin, is mainly governed by Law No. 2017-20 of April 20, 2018, on the Digital Code, amended in 2020, which punishes cybercrime and child pornography and guarantees the protection of personal data[45]. Despite all these provisions, one truth remains as the exclusion of persons with disabilities is still an issue in Beninese society, even in the digital sphere.

To address this problem, the government has established internet community centres, with three specifically dedicated to people with disabilities[46]. In Benin, the community digital centres, are government-led initiatives to provide public access to computers and internet, support public service applications, and promote digital literacy[47]. In addition to the community digital centers, Benin authorities have launched a project called les cases numériques. The project is a satellite-connected version of the community digital centers in areas of the country where the internet fiber is not yet available[48].

Although these initiatives for individuals with disabilities seem encouraging, additional efforts are necessary. Benin officials should implement measures that consider the ICT requirements of individuals with disabilities and the interrelation of the inequalities they face. In general, these inequalities result in fewer opportunities compared to individuals without disabilities. Moreover, the digital divide remains a significant problem, particularly for persons with disabilities, whose ability to access digital opportunities and resources continues to be limited by insufficient digital skills.

42. See Veterans of Israeli spyware firm NSO bounce back in Africa https://www.africaintelligence.com/west-africa/2025/01/10/veterans-of-israeli-spyware-firm-nso-bounce-back-in-africa,110359430-art (accessed on 11 November 2025)
43. See Londa 2023 Digital Rights and Inclusion Reports https://paradigmhq.org/wp-content/uploads/2024/06/Benin-Londa-Report.pdf (accessed on 04 November 2025).
44. See Les avancées en matière de protection des personnes handicapées au Bénin https://journals.openedition.org/rdctss/6591 (accessed on 01 November 2025).
45. See A study on children's right to privacy in the digital sphere in the African region https://www.chr.up.ac.za/images/researchunits/cru/files/publications/Childrens_rights_reports_2022_for_web.pdf (accessed on 06 November 2025).
46. See Pourquoi l'avenir numérique du Bénin repose sur la patience, les partenariats et le peuple https://techcabal.com/fr/2025/07/04/benin-digital-future/ (accessed on 08 November 2025)
47. See Bénin /Point numérique communautaire : un pilier de la connectivité locale à Ouidah https://lechasseurin-fos.bj/benin-point-numerique-communautaire-un-pilier-de-la-connectivite-locale-a-ouidah/ (accessed on 03 November 2025).
48. See Bénin numérique : « C'est ce qu'ont fait les Coréens, les Chinois, les Japonais… » (Marc-André Loko, DG ASIN) https://www.agenceecofin.com/actualites/0304-127222-benin-numerique-c-est-ce-qu-ont-fait-les-coreens-les-chinois-les-japonais-marc-andre-loko-dg-asin (accessed on 08 November 2025)

Universal Service Funds

In Benin, the government has established the Universal Service Fund (USF) to financially support the development of telecommunication services, including internet access and mobile networks, in isolated and underserved areas. The USF is established by Benin law, but it encounters irregular reporting regarding fee collection. This scenario complicates the assessment of funds available[49]. In Benin, the main aim of the Universal Service Funds is to expand network infrastructure to isolated areas that are not profitable for service providers. In this regard, the government of Benin intends to link more municipalities to fiber-optic networks, as part of its larger objective to increase high-speed internet access to all 77 municipalities across the country.[50] This project is expected to cost CFA207 billion (approximately US$375000000) and represents a key component of the government's 2021–2026 Action Plan[51].

If this project has the potential to greatly improve internet access and telecommunications coverage across the country, there is a lack of financial integrity and public transparency regarding the accounting of funds received and distributed within the Universal Service Funds. This situation makes it challenging to ascertain whether the payments are truly towards supporting USF[52].

Given the extensive utilisation of telecommunications by the public in Benin, the challenge arises that politicians may use USF and potentially create regulations that deviate from their intended objectives. Another point to note is that Benin's communications sector continues to encounter multiple challenges.

49. See Loi n° 2014-14 relative aux communications électroniques et à la poste en République du Bénin https://admin.theiguides.org/Media/Documents/DSL-LOI%20N%C2%B0%202014-14%20RELATIVE%20AUX%20COMMUNIC.pdf (accessed on 07 November 2025).
50. See Digitalisation dans les collectivités territoriales: Le projet e-Commune lancé https://lanation.bj/actualites/digitalisation-dans-les-collectivites-territoriales-le-projet-e-commune-lance (accessed on 10 November 2025)
51. See Benin to Connect All Municipalities to High-Speed Internet by 2025 https://www.wearetech.africa/en/fils-uk/news/public-management/benin-to-connect-all-municipalities-to-high-speed-internet-by-2025 (accessed on 11 November 2025)
52. See Trois ans après la réforme, la mise sous contrôle des mairies est un échec https://www.africaintelligence.fr/afrique-ouest/2025/01/17/trois-ans-apres-la-reforme-la-mise-sous-controle-des-mairies-est-un-echec,110362211-art (accessed on 12 November 2025)

Digital adoption is hampered by obstacles such as exorbitant sector-specific taxation. For example, the Benin government levies a variety of industry-specific fees on mobile service providers. However, excessive taxes may deter investment in network infrastructure and mobile telecom services.

Telecoms Sector Specific Taxes in Benin

Tax	Application	Base	Current Value
Numbering fee	Specific	One-off connection charge	XOF 100
Import Duty on handsets	Ad valorem	Import value of goods	10%
Universal Service Fund	Ad valorem	Revenue	2.0%
Annual licence fee	Ad valorem	Revenue	13%
Annual spectrum fees	Various	% of revenues	7%
Import duties on equipment	Ad valorem	Import value of goods	10%

Source GSMA report : Driving digital transformation of the economy in Benin .

Developments in ICT and Emerging Technologies

Through several initiatives, Benin is currently trying to seize the opportunity to turn artificial intelligence (AI) into a vital tool for growth. For instance, President Talon's administration has established a national policy for big data and artificial intelligence, valid from 2023 until 2027[53]. The activities related to AI are being shaped by initiatives around start-ups, academic institutions, training organisations, and the private sector. Consequently, several training centres in this area have been established and are thriving, particularly

the Institute for Training and Research in Computer Science and the Institute of Mathematics and Physical Sciences. On one hand, the Institute of Mathematics and Physical Sciences is equipped with a supercomputer that offers substantial computing capabilities to aid in the advancement of AI in Benin[54]. On the other hand, Benin is also investigating new ways to connect culture and technology as part of its commitment to put its artificial intelligence policy into practice. For instance, the government of Benin has officially launched a project called JaimeMaLangue[55]. This initiative is led by the Information Systems and Digital Agency (ASIN). For three years, ASIN has absorbed the Agency for Universal Electronic Communications and Postal Services, previously responsible for the Universal Service Fund in Benin[56]. Inaugurated with the theme "Benin speaks to the future," citizens are encouraged to join through the jaimemalangue.bj platform, where they can record sentences in their mother tongue.

The recorded data will then form a national training base for AI models capable of understanding and reproducing local languages. The pilot phase is starting with Fongbe, the largest indigenous language in Benin, before being extended to other languages such as Yoruba and Baatonu[57]. However, such projects are not without risks. As Benin is preparing to hold three elections in 2026, several threats should be taken into account[58]. This includes, for example, speech synthesis, which is the artificial generation of speech. In addition to more realistic-sounding artificial voices, speech synthesis can also include voice cloning, which artificially reproduces the characteristics of an individual's voice, known as audio deepfakes. In such conditions, manipulated audio could blur reality and erode trust of the public in available information during the upcoming elections.

53. See National AI and Big Data Strategy (Stratégie Nationale d'Intelligence Artificielle et des Mégadonnées 2023-2027) https://www.aipolicy.africa/national-strategies/0e574345-6d15-4eb3-b6b2-b2f039b2db48 (accessed on 15 November 2025)
54. See L'intelligence artificielle au Bénin et les révolutions pour le développement https://hal.science/hal-04527846/document (accessed on 16 November 2025)
55. See Bénin : lancement du projet « JaimeMaLangue » https://www.africatopsuccess.com/benin-lancement-du-projet-jaimemalangue/ (accessed on 18 November 2025)
56. See Bénin : l'ASIN conclu trois accords clés pour accélérer la transformation numérique https://www.wearetech.africa/fr/fils/actualites/tech/benin-l-asin-conclut-trois-accords-cles-pour-accelerer-la-transformation-numerique (accessed on 19 November 2025)
57. See Bénin : comment contribuer au projet d'IA en langues locales «JaimeMaLangue» https://lanouvelletribune.info/2025/11/benin-comment-contribuer-au-projet-dia-en-langues-locales-jaimemalangue/ (accessed on 11 November 2025)
58. See Benin MPs Vote to Extend Presidential Terms Ahead of 2026 vote https://www.bloomberg.com/news/articles/2025-11-15/benin-mps-vote-to-extend-presidential-terms-ahead-of-2026-vote (accessed on 15 November 2025)

Conclusion

During the reporting period under observation, numerous violations of digital rights have been identified. This led to situations where issues with freedom of speech, discriminatory rhetoric, lack of transparency, and possible AI manipulations emerged. Legislation to counter such digital rights violations remains weak, as Benin has yet to revise the Digital Code. As discussed in Londa Report 2024, Benin received recommendations relating to freedom of expression, and the need to ensure that its national legislation complies with international standards. If no measures are implemented, this is probably going to foster greater infringement of digital rights, ahead of the upcoming elections. On the basis of all the above, Benin barely met the minimal requirements set by TheScore Index, despite the government's continuous efforts in the digital realm during the reporting period.

Recommendations

Government should:

- Adapt constitutional norms to the digital context.
- Create flexible constitutional frameworks for technological change in the digital age.
- Adopt a balanced approach to safeguarding rights and addressing inequalities caused by digital technologies.
- Harness digitalisation to enhance democratic processes.

Civil Society Organisations should:

- Combat rights violations and inequalities caused by digital technologies.
- Provide more opportunities to refine and clarify the language of digital rights with citizens enabling them to better protect themselves online.
- Continue to build tools that advance rights, provide essential analysis, and conduct critical advocacy.

Private sector should:

- Respect the rights of individuals who use their platforms, and address any negative
- Effects that their products may impose on human rights.
- Oppose governmental directives to restrict internet access or digital services.
- Minimise the collection of personal information, such as health, biometric, and
- Location data, and limit how third parties can access and use it.

Media should:

- Report on human rights concerns with a strong and professional commitment.
- Take measures to promote digital literacy as well as critical thinking, by covering these topics and by engaging with civil society organisations and other stakeholders to raise awareness about these issues.

The Score Index

Benin, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
1. Internet Shutdowns	P38(2)	4	4	As a result of civil society pressure, Benin chose not to disconnect the Internet following the shutdown in 2019. Nonetheless, the country will hold its presidential elections in 2026. During election season, the possibility of shutdowns might be present.
2. Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internetv	P37	3	3	Previous calls to bring its domestic law into compliance with international human rights standards persists. Benin is yet to reform the Digital code and Benin Electoral Code. (even though articles 131, 174, 179, 180) of the Electoral code allows state organs to collect personal and biometric data for voters' registration. Data collected includes pictures and fingerprints for both hands
3. False News Criminalisation	P22(2)	1	1	Many journalists, bloggers, and political adversaries of President Patrice Talon's administration have faced prosecution due to the Digital Code. Per the Article 550-paragraph 3 of this law, individuals who create or spread false information regarding another person on social media or via any electronic means risk imprisonment for one to six months, a fine ranging from CFA500,000 (US$1803) to CFA1,000,000 (US$1606), or both penalties.
4. Sedition Legislation	P22(2)	1	1	Article 553 of the Digital Code and Articles 454, 455, and 456 of the Penal Code have a stifling effect on civil society and the media. Through an ambiguous formulation, the provisions address provocation and sedition offenses related to media and audiovisual communications, imposing penalties of CFA200,000 (US$360) or six months in prison up to CFA10,000,000 (US$18000) or five years in prison.
5. Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	3	3	While the Digital Code may benefit Benin, it has resulted in numerous arbitrary arrests and harassment of citizens, human rights defenders and journalists
6. Data Protection Legislation.	P42	4	4	By using a national interoperability platform, the Council of Ministers can allow the transfer of personal data to a third country or international entity lacking adequate protection, potentially threatening Benin's digital rights and the aims of the Digital Code. This exception is set by the provisions of the Digital Code regarding data protection and privacy.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
7. States interfere and require the removal of online content by internet intermediaries	P38 and P39 (4)	3	3	Benin has contacted Facebook's parent company, Meta[59] as it did last year, requesting information on user accounts for emergency or legal purposes. There is a sense of regulatory uncertainty because the Presidency and the National Center for Digital Investigation (CNIN) have considerable power over the unilateral removal of internet information by intermediaries.
8. Invasion of Privacy of Communications	P41	3	3	Paid operatives are used to run covert dirty tricks in the fragile democratic systems of Benin
9. Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	3	3	Key implementation issues that public administration still faces include poorly trained staff, lack of resources and the community's access to and understanding of information.
10. AI and Emerging Technologies national strategies	P39 (6)	3	3	Benin has formally embraced a National Strategy pertaining to Megadata and artificial intelligence. Nevertheless, the nation has postponed the consideration of any international human rights standards.
11. Adoption of specific	P37(5)	3	3	Benin has established a digital infrastructure for the management of childcare and
child laws, policies and measures promoting children's digital safety and privacy online				protection facilities. Nevertheless, it is imperative that the nation implements a regulatory framework that governs the utilisation of minors' data on this platform, while also considering the advancements in the realm of human rights
12. Digital Inclusion	P37(3)	3	3	The installation of optic fiber connections has been one of the major initiatives and investments made to expand the country's internet coverage. However,the digital divide is still quite noticeable in both urban and rural areas.Large swathes of Benin remain dark at night, which serves as a sobering reminder of the nation's unreliable access to energy.
Total (out of 60):				33

Botswana

By Oarabile Mudongo

Executive Summary

The 2025 Londa Digital Rights and Inclusion report for Botswana provides a comprehensive assessment of the country's digital landscape, drawing on an extensive review of legislation, policies, platform transparency data, and over 40 authoritative sources across twelve core thematic areas. Through the Londa Score Index, Botswana has achieved a historic leap from mild-to-moderate compliance (28 points) in the 2024 assessment to a considerably compliant status with a total of 35 points out of 60. This reflects substantial legal advancements, most notably the Data Protection Act of 2024 (effective 14 January 2025), the Access to Information Act of 2024 (effective January 2025), and the Persons with Disability Act of 2024 (operational from December 2025) coupled with near-universal 4G coverage (~98%) and a consistent record of zero internet shutdowns. Yet these gains are tempered by persistent implementation gaps, including a stark urban-rural digital divide (household internet access at 79.2% urban versus ~20.8% rural), affordability barriers, underfunded inclusion efforts for persons with disabilities, weak surveillance oversight, and emerging risks from technology-facilitated gender-based violence and unregulated smart city traffic surveillance technology deployments.

Introduction

Since 2016, Botswana has evolved from a landscape marked by legislative silence, lacking dedicated data protection, freedom of information, or robust digital rights safeguards, into one of Southern Africa's quieter success stories. Early assessments highlighted self-censorship under vague laws, rising online harassment of women in public life, and limited household connectivity that marginalised rural communities and persons with disabilities. However, the period from 2020 to 2025 of the LONDA report series delivered a cascade of crucial reforms, including the landmark Access to Information Act of 2024 (effective January 2025) and the progressive Persons with Disability Act of 2024 (operational from December 2025). These legislative milestones, supported by an active Information and Data Protection Commission and expanded public participation in tech policy, have yielded tangible progress: minimal government content-takedown requests, strengthened privacy safeguards, and near-universal 4G population coverage (~98–99%).

Despite these gains, a persistent gap remains between legal progress and everyday digital access. Rural household internet access stands at roughly 20.8%, far below urban levels, and affordability challenges continue to limit meaningful connectivity for low-income households. Emerging risks, such as the deployment of unregulated smart city traffic surveillance technology without comprehensive oversight, and the absence of dedicated child online safety and AI governance laws, underscore the need to consolidate recent legislative momentum with stronger implementation. Botswana's current phase is therefore defined not by the absence of reform, but by the need to translate rapid legislative progress into equitable outcomes for all citizens.

Internet Access

Despite steady strides in national network coverage, Botswana contends with a persistent and stark urban-rural digital divide. This is quantified by Statistics Botswana's 2025 Household Access and Individual Use of ICTs Survey, which reveals a national household

internet access rate of 68.9%, buoyed by urban access at 79.2% but dragged down by significantly lower rates in rural households (around 20.8%).[1] In response, a concerted government initiative led by the Universal Access and Service Fund (UASF) under the Botswana Communications Regulatory Authority (BOCRA) has driven progress through broadband expansion and last-mile projects. These efforts are substantiated by major financial commitment, including the BWP1.2 billion (approximately US$91.15 million) allocated in the 2024/25 national budget for ICT infrastructure. Consequently, near-universal 4G population coverage (~98–99%) has been achieved, though a core challenge remains: rural areas (25.8–26.2% of the population) still lack fixed-line options. The ongoing intent to narrow the gap is clear, however, from UASF initiatives targeting hundreds of additional rural schools for connectivity in 2025.[2]

Affordability and Quality

Beyond coverage, meaningful access is challenged by affordability and quality. As evidence of the affordability challenge, GSMA's State of Mobile Internet Connectivity 2025 report notes that 1GB of mobile data across Sub-Saharan Africa (including Botswana) averaged ~5.7% of monthly income in 2024–2025, with entry-level smartphones costing roughly 30% of income, modest gains that still exclude many low-income households.[3] Nevertheless, Botswana is showing measured progress toward improved data affordability. According to BOCRA's May 2025 Pricing and Costing study, mobile operators have introduced lower-priced, higher-volume bundles, with 1GB-equivalent data now retailing at approximately BWP 49–69 (approximately US$3.72 – $US5.24) for 30 days following the approved tariff reductions.[4] This shift is driven by a September 2025 BOCRA directive that saw operators like Orange Botswana effectively slash data prices by 60%.[5] While these price adjustments represent a downward shift, the cost of 1GB still translates to roughly 4–5% of GNI per capita in 2025, indicating that mobile data remains above the 2% affordability target despite recent regulatory interventions.

On the quality front, improvements have also been marked. For instance, Ookla Speedtest Global Index data for 2025 show Botswana maintaining strong mobile download speeds (often second in Africa regionally), with fixed broadband median speeds rising sharply (e.g., +25–45% year-on-year in recent periods) thanks to 4G/5G expansion and fibre investments.[6] Rural connections, however, continue to suffer instability from frequent power outages, a persistent issue that underscores that reliable electricity remains as essential as network infrastructure.

1. Statistics Botswana (2025) https://www.statsbots.org.bw/sites/default/files/press-releases/Press%20Release-Statistics%20Botswana%202024%20ICT%20Household%20Survey%20Results.pdf (accessed on 10 January 2026)
2. BOCRA (2025) https://www.bocra.org.bw/sites/default/files/sites/default/files/documents/BOCRA2025_ANNUAL_REPORT_(WEB)_compressed.pdf (accessed on 10 January 2026)
3. K Bahia "The State of Mobile Internet Connectivity 2025: Understanding Mobile Internet Use in Low- and Middle-Income Countries" (2025) https://www.gsmaintelligence.com/research/the-state-of-mobile-internet-connectivity-2025-understanding-mobile-internet-use-in-low-and-middle-income-countries (accessed on 09 January 2026)
4. BOCRA "Press Release - Bocra Approves Reduced Data Prices For Orange Botswana" (2025) https://www.bocra.org.bw/sites/default/files/Press_Release_-_Reduction_in_Data_Charges_for_Orange.pdf (accessed on 10 December 2025)
5. L Timothy "BOCRA approves Orange data price cuts" (2025) https://www.mmegi.bw/business/bocra-approves-orange-data-price-cuts/news (accessed on 05 January 2026)
6. Speedtest "Ookla Speedtest Global Index – Botswana 2025 data" (2025) https://www.speedtest.net/global-index/botswana (accessed 05 December 2025)

Disruptions and the lingering Digital Divide

Deliberate internet shutdowns, one of the gravest threats to digital rights, remain absent in Botswana. However, non-governmental connectivity interruptions, primarily caused by rural power failures, remain a significant challenge, as noted in BOCRA's 2025 annual report.[7] This infrastructural fragility compounds the structural inequalities of the digital divide. Key data exposes the gap: urban household internet access (79.2%) vastly outpaces rural access (20.8%), and usage among the wealthiest (85%) is nearly double that of the poorest (45%).[8] An estimated 18.6% of the population remained offline in early 2025, a stagnation highlighting the need for more effective, targeted policy measures to translate national progress into equitable access.[9]

Online Freedom of Expression and Access to Information

Botswana's legal landscape for online expression starts strong with constitutional protections, but is quickly undercut by outdated, restrictive laws. Specifically, Article 12 of the Constitution of Botswana guarantees freedom of expression, which extends to digital spaces. However, this broad guarantee clashes with the Sedition Provisions (Sections 50-56) of the Penal Code and the broadly defined offences in the Cybercrime and Computer Related Crimes Act of 2018.[10] Consequently, these laws create a chilling effect, as they are susceptible to being used to criminalise criticism of public officials. This framework therefore falls short of full compliance with the principles of the African Charter on Human and Peoples' Rights (Article 9),[11] as the threat of prosecution stifles open dialogue. On a more positive note, the Data Protection Act of 2024 strengthens privacy safeguards,[12] offering a better-aligned counterbalance to surveillance risks.

Freedom House's Freedom in the World 2025 report maintains Botswana's score at 3/4 for freedom of expression, noting reduced political pressure after the 2024 elections but repeating its call for repeal of sedition provisions.[13] Botswana's Access to Information Act No. 16 of 2024 (effective November 2024) finally gives citizens a statutory right to public records without having to justify their request (Section 6), with presumptive disclosure and narrow exemptions (Section 17).[14] To operationalise this right, public bodies are required to appoint information officers and submit compliance plans (Section 47). While the Act was passed, it lacked a formal commencement date in late 2025, meaning it had not yet come into use.

Botswana holds no record of direct request for content removal or request for user data. For instance, Meta's Transparency Report (January–June 2025) shows two government requests (both emergency disclosures, none via legal process), affecting eight users/accounts, with 0% compliance (no data produced).[15] Similarly, Google received no user-data request in H1 2025 (and no content removal requests),[16] while TikTok reported zero removal requests in its 2025 enforcement reports.[17] No public information is available on any direct government requests made

7. ibid
8. Statistics Botswana "Statistics Botswana Releases 2025 ICT Household Survey Results" (2025) https://www.statsbots.org.bw/sites/default/files/press-releases/Press%20Release-Statistics%20Botswana%202024%20ICT%20Household%20Survey%20Results.pdf (accessed on 03 December 2025)
9. Data Reportal "Internet use in Botswana in 2025" (2025) https://datareportal.com/reports/digital-2025-botswana (accessed on 12 January 2026)
10. Cybercrime and Computer Related Crimes Act, 2018 (Act No. 18 of 2018): https://www.bocra.org.bw/sites/default/files/documents/18%20Act%2029-06-2018%20Cybercrime%20and%20Computer%20Related%20Crimes.pdf
11. African Commission on Human and People's Rights (ACHPR) Declaration on Freedom of Expression and Access to Information (the Declaration) https://achpr.au.int/en/node/902 (accessed on 11 January 2026)
12. Data Protection Act, 2024 (Act No. 18 of 2024): https://www.studocu.com/row/document/botho-university/corporate-governance/botswana-data-protection-act-2024-government-gazette-extraordinary/127442966
13. Freedom House 'Freedom in the World 2025: Botswana' (2025) https://freedomhouse.org/country/botswana/freedom-world/2025 (accessed on 11 December 2025)
14. Access to Information Act, 2024 (Act No.16 2024): https://botswanalaws.com/consolidated-statutes/acts-on-notice/2024/access-to-information-act
15. Meta "Integrity Reports, Third Quarter 2025" (2025) https://transparency.meta.com/reports/government-data-requests/country/BW/ (accessed 26 December 2025)
16. Google "Transparency Report on Government Request to Remove Content Section for Botswana" (2025) https://transparencyreport.google.com/government-removals/government-requests/BW?hl=en (accessed 11 December 2025)

to telecommunications operators (e.g., Orange, Mascom) for content restriction or user data during the year. The draft Digital Services Bill (still under consultation in late 2025) proposes clearer, more transparent takedown procedures with stronger appeal mechanisms.[18]

Despite this minimal direct censorship, fear of prosecution under sedition and defamation laws continues to drive significant self-censorship. This environment is reflected in the 2025 World Press Freedom Index by Reporters Sans Frontières, where Botswana's ranking dropped to 81out of 180 countries (down from 79 in 2024).[19] The report attributes this decline to a surge in intimidation and doxxing incidents targeting journalists throughout 2024 and 2025. This intimidation has tangible effects, as the Media Institute of Southern Africa (MISA) Botswana condemns "emerging threats to media freedom" and harassment of journalists.[20] Regarding the most severe consequences, arbitrary arrests for online speech remained rare in 2025. This overall picture represents a continued low incidence of prosecution in the country for this period.

Gendered Disinformation

Gendered disinformation has rapidly become one of the biggest barriers keeping women and girls out of the digital space. The severe pattern of similar issues documented during the 2024 election cycle persisted into 2025, transitioning from acute electioneering to a chronic feature of the online environment. While no major new large-scale study quantified a further electoral drop in engagement, the UN Women's November 2025 report on digital violence in East and Southern Africa confirmed that women leaders, journalists, and human-rights defenders across these regions, notably in Botswana, continued to face coordinated online threats.[21] This demonstrates a lack of enforcement of existing cybercrime-related legislation, most of which does not recognise the gender dimensions of digital abuse.

Currently, the Cyber Crime and Computer Related Crimes Act of 2018 criminalises harassment, stalking, and revenge pornography, while the Data Protection Act of 2024 strengthens privacy safeguards. However, no amendments specifically targeting deepfakes were passed in 2025, though discussions in the Ministry of Youth and Gender Affairs' 2025 '16 Days of Activism' campaign statements signal intent to strengthen penalties and draft a Gender-Based Violence Bill as part of broader regional harmonisation, called for by UN Women.[22]

Concerning platform governance, Meta and Google reported zero gender-specific removal requests from Botswana authorities in 2025. However, neither provides localised moderation guidelines tailored to Botswana's context, meaning reports of gendered abuse often rely on global policies that do not fully account for local cultural or political dynamics. By contrast, broader policy efforts are more promising: the National ICT Policy and SmartBots 4IR Strategy now embed gender targets for digital literacy.[23]

The most significant development is the ongoing work on dedicated Gender-Based Violence legislation. The Ministry of Youth and Gender Affairs confirmed in December 2025 that drafting instructions for a comprehensive GBV

17. Tiktok "Government Removal Requests Report" (2025) https://www.tiktok.com/transparency/en/government-removal-request-2025-1 (accessed 15 December 2025)
18. Digital Services Bill, 2025 (Published On ,2025): https://www.gov.bw/sites/default/files/2025-06/Digital%20Services%20Bill%20%28revised%20draft%29June2025.pdf
19. Reporters Without Borders (2025) https://rsf.org/en/rsf-world-press-freedom-index-2025-economic-fragility-leading-threat-press-freedom?data_type=general&year=2025 (accessed 20 January 2026)
20. MISA "MISA Botswana Condemns Emerging Threats to Media Freedom" (2026) https://misa.org/blog/misa-botswana-condemns-emerging-threats-to-media-freedom/ (accessed 29 January 2026)
21. UN Women "Digital violence in East and Southern Africa: Urgent action needed to protect women and girls online" (2025) https://africa.unwomen.org/en/stories/press-release/2025/11/digital-violence-in-east-and-southern-africa-urgent-action-needed-to-protect-women-and-girls-online (accessed on 21 November 2025)
22. See Minister's Facebook Post: https://www.facebook.com/100042906802765/posts/botswanas-first-gender-based-violence-bill-the-ministry-of-youth-and-gender-affa/1713059906800886/ (accessed on 04 January 2026)
23. Daily News "Strategy addresses gender inequality" (2025) https://dailynews.gov.bw/news-detail/86439 (accessed on 05 January 2026)

Bill have been finalised and submitted to the Attorney General's Chambers,[24] with a target presentation to Parliament set for July 2026. The Minister recognises that technology-facilitated gender-based violence (TFGBV) silences women and girls, necessitating that the new legal frameworks move beyond solely addressing physical violence, representing a major leap from 2024's fragmented approach. Crucially, its success depends first on passage into law (not yet achieved in 2025), and then on effective police enforcement and adequate resourcing. While the Ministry has not yet published a specific 2025 enforcement budget figure, the overall GBV response is tied to national planning. Ultimately, without sustained political will and funding, even strong legislation risks remaining on paper

Data Protection and Cybersecurity

Botswana established a comprehensive data protection regime with the Data Protection Act No. 18 of 2024, effective 14 January 2025.[25] The Act consolidates earlier fragmented laws by recognising individual rights to access, rectifying, and erasing personal data, while imposing GDPR-aligned principles like data minimisation and accountability on controllers.[26] Furthermore, it applies extraterritorially, includes safeguards for cross-border transfers, and sets significant penalties of up to BWP50 million (approximately US$3.80 million). While the law aligns well with the African Union Convention on Cyber-security and Personal Data Protection,[27] it lacks explicit protections for children's data and automated decision-making gaps that 2025 amendment proposals aim to address.

The Information and Data Protection Commission (IDPC) of Botswana, established under the 2024 Act, now holds powers to investigate, audit, and impose these fines. Operationalising these powers, regulations require 72-hour breach notifications. While this research does not detail the specific mechanics of the breach reporting portal, the regulatory environment is now fully operational. Data regarding the number of complaints received or resolved by the IDPC in 2025 remains unavailable. Although enforcement efforts are underway, controller compliance is inconsistent; resource constraints continue to hinder the transition toward comprehensive oversight. To date, there have been no confirmed major data breaches or instances of data misuse. This could suggest that IDPC has focused on proactive compliance rather than reactive penalties.

The Cybersecurity Bill (No.24 of 2025),[28] gazetted on August 8, 2025, strengthens national security by regulating critical infrastructure and establishing a Cybersecurity Commission and a 24/7 Cyber Security Incident Response Team (CSIRT). Operationally, a 2025 Cyble-BOCRA MoU will improve threat intelligence sharing.[29] However, a significant concern remains: Section 12 of the Bill grants broad interception powers without mandatory judicial oversight, and vague "national security" definitions risk abuse. Consequently, while awareness campaigns can reduce incidents, proportional safeguards and whistleblower protections are still absent.

The Omang biometric ID system, which captures fingerprints and facial images, had achieved 86.7% coverage among individuals aged 15 and over, according to the 2022 Population and Housing Census.[30] As a result, it has expanded access to essential services including voting, banking, health care, social assistance, land-title registration,

24. Mmegi "Chombo announces GBV Bill drafting" (2025) https://www.mmegi.bw/news/chombo-announces-gbv-bill-drafting/news (accessed on 06 January 2026)
25. Data Protection Act, 2024 (Act No. 18 of 2024): https://www.studocu.com/row/document/botho-university/corporate-governance/botswana-data-protection-act-2024-government-gazette-extraordinary/127442966
26. General Data Protection Regulation (GDPR), Art. 5 GDPR Principles relating to processing of personal data: https://gdpr-info.eu/art-5-gdpr/ (accessed on 27 January 2026)
27. AUC 'African Union Convention on Cyber Security and Personal Data Protection' https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed on 08 January 2026)
28. Cybersecurity Bill (No.24 of 2025): https://www.bocra.org.bw/sites/default/files/sites/default/files/documents/Draft_Cybersecurity_Bill_2025_AG_Comments.pdf (accessed 05 December 2025)
29. Cyble Inc "Cyble and Botswana Communications Regulatory Authority (BOCRA) Sign MoU to Advance National Cybersecurity in Botswana" (2025) https://cyble.com/press/cyble-bocra-mou-botswana-cybersecurity/ (accessed 06 January 2026)
30. Statistics Botswana "Population and Housing Census 2022: Key Demographic and Socio-Economic Indicators" (2023) https://www.statsbots.org.bw/sites/default/files/Population%20%20Housing%20Census%202022-%20Key%20Demographic%20and%20Socio-Economic%20Indicators.pdf (accessed 18 December 2025)

and SIM-card registration. However, this widespread adoption creates a significant trade-off, as the centralised repository of sensitive biometric data poses major privacy and security risks, including potential identity theft and state surveillance if breached.

Notably, approximately 13.3% of the eligible population (~200,000 people) remain unregistered. This gap disproportionately affects Basarwa (San) communities, rural populations in remote western districts, persons with disabilities, economically disadvantaged groups, and youth who have just reached registration age.[31] Consequently, without an Omang card, these individuals are excluded from exercising fundamental rights and accessing public services, thereby perpetuating cycles of marginalisation.

In terms of legal governance, the system is now subject to the Data Protection Act 2024 (effective January 2025), which establishes IDPC as the supervisory authority and introduces modern principles for lawful data processing. Nevertheless, a critical challenge persists: the National Registration Act of 1986 (amended 1993),[32] the primary legal foundation, predates modern digital-ID technologies and does not adequately address contemporary privacy and inclusion risks.

Privacy and Surveillance

Botswana's primary law authorising surveillance is the Criminal Procedure and Evidence (Controlled Investigations) Act 2022.[33] This permits interception with a judicial warrant, but defines its scope by a broad and undefined term:

31. Institute of development Studies "Biometric Digital-ID in Africa: Progress and Challenges to Date – Ten Country Case Studies Botswana Country Report" (2025) https://opendocs.ids.ac.uk/articles/book/Biometric_Digital-ID_in_Africa_Progress_and_Challenges_to_Date_Ten_Country_Case_Studies/30773789?file=60062471 (accessed on 28 December 2025)
32. National Registration Act, 1986 (amended 1993): https://botswanalaws.com/StatutesActpdf/1993Actpdf/NATIONAL%20REGISTRATION%20%28AMENDMENT%29%20ACT%2C%2017%20OF%201993.pdf (accessed on 20 January 2026)
33. Criminal Procedure and Evidence (Controlled Investigations) Act 2022: https://natlex.ilo.org/dyn/natlex2/natlex2/files/download/113962/BTW113962.pdf (accessed 14 January 2025)

"serious offences." Consequently, this vagueness allows orders without clear necessity or proportionality, meaning the framework only partially meets the African Commission on Human and Peoples' Rights (ACH PR) Article 9[34] and International Covenant on Civil and Political Rights (ICCPR) Article 17 standards.[35]

Subsequent legislation has added safeguards. The Data Protection Act of 2024 now requires impact assessments and a lawful basis for surveillance-related data processing, addressing earlier gaps. Similarly, the Act requires that any systematic monitoring or high-risk data processing be both necessary and proportionate to its purpose. Specific legislation dedicated to online harms is not included in the current legal framework. Importantly, no amendments addressed automated surveillance in 2025, leaving a regulatory gap.

The launch of Botswana's Greater Gaborone Centralised Traffic Control Centre introduces advanced smart city surveillance capabilities, utilising real-time camera networks and predictive data analytics for traffic management and infrastructure planning.[36] While enhancing urban efficiency, this integrated system is an evolution of the 2020 Safe City surveillance project. Currently, no specific legal framework publicly governs the operation, data retention, or oversight of this predictive system, highlighting a pressing regulatory gap as Botswana's smart city infrastructure expands.

Oversight of surveillance remains limited. On one hand, the Data Protection Act empowers the IDPC to audit data processing and report to Parliament, and it resolved 30 surveillance-related complaints in early 2025. Also, the Criminal Procedure and Evidence (Controlled Investigations) Act of 2022 (CPE Act) requires the issuance of judicial warrants. However, a significant accountability gap exists,

34. African Commission on Human and People's Rights (ACHPR): https://achpr.au.int/en/node/902 (accessed on 11 January 2026)
35. International Covenant on Civil and Political Rights (ICCPR) Article 17: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed on 11 January 2026).
36. Daily News "High-Tech Traffic Control Centre To Tackle Road Safety" (2025) https://dailynews.gov.bw/news-detail/89428 (accessed on 18 December 2025)

as the Directorate of Intelligence and Security Services (DISS) is not subject to the same warrant or reporting requirements. In Botswana, primary legislative oversight of surveillance is conducted by the Intelligence and Security Parliamentary Committee and the Public Accounts Committee (PAC); however, there remains a critical gap as no independent body currently possesses investigative authority over intelligence surveillance activities.

Developments in ICT and Emerging Technologies

Botswana has not yet enacted a standalone AI law or formal national strategy, resulting in an indirect and foundational approach to AI governance. While policies like the Maitlamo ICT Policy and the SmartBots strategy promote digital innovation, UNESCO's 2025 AI Readiness Assessment notes that AI-specific regulation, risk-assessment, and oversight structures remain overshadowed by broader digital initiatives.[37] Plans to partner with European institutions, including Estonia and other donors, on a national AI strategy were initiated in 2024 and have since advanced from foundational discussions to high-level strategic engagement.[38] However, no confirmed progress has been made following these developments since the change in government, leaving Botswana's AI framework in 2025 as policy-driven and preparatory rather than legally binding.

Botswana's institutional readiness for AI remains mixed. According to the Oxford Insights Government AI Readiness Index 2025, Botswana scored 37.10 overall, ranking 109th globally and 9th in Sub-Saharan Africa, above the regional average score of 29.12. The country performs comparatively well in regulatory compliance (60.0) and e-government delivery (68.21).[39] While the data shows emerging strengths in AI sector maturity and technology diffusion relative to regional averages, this underscores that the country's AI ecosystem in 2025 remains foundational, with stronger infrastructure and governance readiness than strategic policy direction or skills development.

Alongside policy discussions, several 2025 developments signal Botswana's growing investment in AI-enabling infrastructure and capacity. The launch of BOTSAT-1, the country's first satellite, marks a significant step toward strengthening national digital infrastructure and expanding connectivity needed to support data centres, cloud services, and AI-driven industries.[40] At the institutional level, the Botswana Unified Revenue Service (BURS) began exploring frameworks to integrate AI into tax administration, including proposals to use automated systems to improve audit efficiency, digital tax services, and voluntary compliance. Skills development is also receiving increased attention.[41] Under Vision 2036 and through partnerships with UNESCO and other international actors, government and education stakeholders continued initiatives to expand STEM and digital-skills training, including school-level programmes such as BRAST aimed at preparing learners for participation in an AI-driven economy.[42] Meanwhile, Botswana's broader digital ecosystem is expanding: the Internet of Things (IoT) market is projected to reach approximately US$135.9 million by 2025 (Statista),[43] reflecting rising connectivity, mobile adoption, and digital-transformation investments.

37. UNESCO "Botswana Artificial Intelligence Readiness Assessment Report" (2025) https://unesdoc.unesco.org/ark:/48223/pf0000396211/PDF/396211eng.pdf.multi (access on 04 January 2026)
38. Daily News "Artificial Intelligence Policy in Final Stage" (2025) https://dailynews.gov.bw/news-detail/88106 (accessed on 28 January 2026)
39. Oxford Insights "Government AI Readiness Index" (2025) https://oxfordinsights.com/wp-content/uploads/2026/01/2025-Government-AI-Readiness-Index-Report_01_26.pdf (accessed 15 December 2026)
40. Africa Defence forum "Botswana's First Satellite Launch a Model for African Countries" (2025) https://adf-magazine.com/2025/08/botswanas-first-satellite-launch-a-model-for-african-countries/ (accessed on 19 January 2026)
41. E Munjeyi and D Schutte "Development of an artificial intelligence framework to combat tax noncompliance in Botswana" (2025) https://adf-magazine.com/2025/08/botswanas-first-satellite-launch-a-model-for-african-countries/ (accessed on 20 December 2025)
42. Human Resource Development Center "Introducing The Botswana Robotics & Automation Skills Transfer (Brast) Project" (2025) https://www.hrdc.org.bw/case/introducing-botswana-robotics-automation-skills-transfer-brast-project (accessed on 15 December 2025)
43. Statista "Internet of Things - Botswana" (2025) https://www.statista.com/outlook/tmo/internet-of-things/botswana?srsltid=AfmBOooaJZOAqPWX4yCdFP9U1WCtvrdbGSPNWW74mnQzTCG63x2S9_72#revenue (accessed 05 January 2026)

Taken together, these developments indicate growing technological ambition; however, without parallel progress on dedicated AI governance and oversight, infrastructure and skills expansion continue to outpace the establishment of clear regulatory safeguards.

Digital Inclusion

The landmark Persons with Disability Act of 2024 officially came into force on December 4, 2025,[44] marking a significant legal milestone for digital and broader inclusion in Botswana. It established a National Disability Council to coordinate implementation, which became operational in 2025. Progress in the year focused on turning this framework into action; with UN agency support, initiatives advanced digital inclusion and inclusive education.[45] For instance, UNICEF supported the finalisation of a National Functional Curriculum for learners with severe disabilities, aligning with SDG 4 goals.[46]

However, implementation challenges persist, particularly a pronounced rural-urban divide in digital accessibility and resource gaps. Public engagement during International Day of Persons with Disabilities (IDPD) 2025 events highlighted these ongoing disparities, calling for sustained efforts to ensure the Act promises to translate into equal access.[47]

In parallel, child online safety efforts advanced in 2025 through strengthened legal safeguards and operational programs. Botswana continued to align with the African Union's Child Online Safety Policy,[48] while the Data Protection Act 2024 (effective January 2025) introduced critical protections for children's data, requiring verifiable parental consent (Section 29). Operationally, UNICEF partnerships helped scale digital protection, including safer reporting tools and expanded child-friendly services.

Nevertheless, structural gaps remain. The country still lacks a standalone child online protection law, and critical issues like rural coverage and platform age verification are limited. Overall, 2025 was defined by foundational progress, from enacting key legislation to launching supportive programs, honouring commitments under the ACHPR and Convention on the Rights of Persons with Disabilities (CRPD). Yet, uneven access persists underscoring that full digital inclusion requires accelerated scaling of resources and targeted rural interventions

Universal Service Fund (USF)

The Universal Access and Service Fund (UASF), administered by the Botswana Communications Regulatory Authority (BOCRA), remained a central policy instrument for advancing equitable connectivity during the reporting period. Designed to subsidise infrastructure in commercially unviable areas, the Fund continued to support national broadband and universal access objectives by extending services to underserved communities and public institutions.[49]

From a financial standpoint, the Fund maintained a stable revenue base derived from sector levies on telecommunications, broadcasting, and postal operators. Total collections for the year amounted to approximately

44. Persons with Disability Act, 2024 (No.6 of 2024): https://covid19portal.gov.bw/sites/default/files/2025-03/Act%20No%206%20of%202024%20PERSONS%20WITH%20DISABILITY%20(1).pdf (accessed on 03 December 2025)
45. UNICEF Botswana "Giga and the Learning Passport are advancing Digital Learning in Botswana" (2025) https://www.unicef.org/botswana/media/1161/file/Case%20Study%20Giga%20%20Learning%20Passport%20%20Botswana.pdf (accessed on 15 January 2026)
46. UNICEF Botswana "Botswana has validated a national Functional Curriculum for learners with Severe to Profound Intellectual and Multiple Disabilities (SPIMD) - a major step toward" (2025) https://www.facebook.com/100064662072875/videos/botswana-has-validated-a-national-functional-curriculum-for-learners-with-severe/785437827894220/ (accessed on 20 January 2026)
47. Facebook Post: Botswana Society for the Deaf (2025) Botswana Society for the Deaf (BSD) proudly joined the nation in Jwaneng yesterday for the commemoration of the International Day of Persons with Disabilities (IDPD). Retrieved from https://www.facebook.com/100069342544215/posts/on-thursday-december-4th-2025-jwaneng-town-will-host-the-un-international-day-fo/1161225459532195/
48. The African Union: Child Online Safety and Empowerment Policy (2024): https://au.int/sites/default/files/documents/43798-doc-African_Union_Child_Online_Safety_and_Empowerment_Policy_Feb_2024.pdf (accessed on 10 January 2026)
49. BOCRA "BOCRA Advancing Communications Regulation For An AI World Annual Report 2025" (2025) https://www.bocra.org.bw/sites/default/files/sites/default/files/documents/BOCRA2025_ANNUAL_REPORT_%28WEB%29_compressed.pdf (accessed on 12 January 2026)

BWP44.6 million (approximately US$3.39 million), with a surplus of around BWP37.6 million (approximately US$2.86 million) transferred into the UASF trust to support ongoing and future projects.[50] Fuelled by these collections, the Fund retained reserves to finance targeted infrastructure expansion, although the scale of available resources remains modest relative to long-term universal access ambitions.[3]

To translate these funds into tangible outcomes, the reporting period saw continued expansion of connectivity and broadcasting infrastructure in underserved regions. LTE and mobile network deployments in remote villages contributed to maintaining national 4G population coverage of approximately 98%, significantly improving access to voice and data services in previously unserved areas.[51] In parallel, new FM transmission sites expanded commercial radio coverage to 34 rural communities, increasing national reach to about 80% and improving access to information and public-interest broadcasting.[5] These infrastructure investments supported connectivity for more than 50,000 residents, including students, educators, and local service institutions.

Building on this momentum, the Fund also prioritised connectivity within educational institutions as a mechanism for strengthening long-term digital inclusion. Prefabricated computer laboratories and broadband connections were delivered to rural schools, enabling access to digital learning platforms and public e-services. Early usage indicators suggest that these interventions contributed to a measurable rise in rural internet adoption during the reporting period.[52]

Despite these advancements, disparities persist between urban and rural connectivity levels and across income groups. Infrastructure expansion has not yet fully addressed affordability constraints or accessibility gaps for persons with disabilities. To address remaining connectivity deficits, the Fund is expected to prioritise further rural broadband rollout, expanded institutional connectivity, and strengthened monitoring of project outcomes in the coming year.

50. Ibid
51. Ibid
52. Ibid

Conclusion

Botswana in 2025 stands as a nation of quiet, consistent progress, rarely repressive, steadily advancing toward global standards, and ahead of many regional peers in freedom of expression, privacy restraint, and participatory policy-making on emerging technologies. This upward trajectory is evident in the dramatic year-on-year improvement on the LONDA index, yet the path to true leadership remains defined by the need to close the gap between ambitious legislation and lived realities for all citizens. Future success hinges on decisive action to reach higher ratings in coming years: enacting dedicated Child Online Protection and AI Governance laws by 2026 with mandatory human rights impact assessments; strengthening independent oversight of surveillance through judicial warrants and transparent mechanisms; and scaling Universal Access and Service Fund resources by at least 50% to prioritise rural last-mile connectivity, affordability subsidies, and assistive technologies for persons with disabilities. Sustained multi-stakeholder commitment, pairing legislative energy with bold enforcement and funding, will determine whether Botswana fully realises its potential as the continent's exemplary digital-rights success story.

Recommendations

The Government should:

- Enact a standalone Child Online Protection Act by 2027 to centralise safeguards for children's privacy and safety. The Act must mandate age-appropriate design standards, robust reporting mech

- anisms, and compulsory child-rights impact assessments for all digital service providers operating within the jurisdiction.
- Establish an AI Governance and Automated Surveillance Framework, requiring human-rights impact assessments, transparency, and independent oversight for high-risk technologies.
- Scale UASF investment and targeting, prioritising rural last-mile connectivity, affordability subsidies, and assistive technologies for persons with disabilities. Public reporting on fund allocation and impact should be strengthened.
- Strengthen independent surveillance oversight by requiring judicial authorisation for all interception activities. Establishing an independent review mechanism for intelligence surveillance and clarifying national-security exemptions in data-protection laws.
- Operationalise the Access to Information Act fully through implementation guidelines, trained information officers, and proactive disclosure obligations.

The Media should:

- Build and sustain dedicated fact-checking and digital-literacy desks to raise awareness of Technology-Facilitated Gender-Based Violence (TFGBV), providing a critical defence against the gendered disinformation that routinely targets women in public life.
- Protect their own personnel, news organisations must adopt and enforce gender-sensitive newsroom policies. These should include rapid-response protocols for online harassment, backed by legal-support funds and strong partnerships with the Statutory Press Council.
- Proactively partner with regulators like BOCRA and the Information Commission. By training reporters on using the Access to Information Act proactively to strengthen investigative reporting on digital governance and public-interest technology.

Civil Society Organisations should:

- Amplify their voice, organisations should form a permanent Digital Rights Coalition to transition from passive observation to strategic advocacy. This coalition should prioritise strategic litigation to challenge unconstitutional practices, specifically aiming to close “national security” loopholes in the Data Protection Act and demanding a public registry of automated surveillance tools used by law enforcement to ensure transparency and accountability.
- This coalition should then systematically use the new Access to Information Act as a strategic tool, requesting and publishing detailed data on UASF spending.
- On the ground, CSOs must scale up community-based digital literacy programmes in rural and marginalised communities. Simultaneously, they should continue to push for mandatory representation of these communities in all future tech policy consultations, ensuring that the digital future is shaped by everyone it will affect.

Private Sector should:

- Before rolling out new technologies, companies should conduct and publish independent human rights impact assessments, especially for biometric systems like facial recognition. This builds public trust and mitigates potential harm.
- To directly tackle the affordability barrier, the private sector should actively contribute to the Universal Access Service Funds. Together, they can create subsidised bundles that include affordable assistive devices and adaptive software alongside standard data packages.
- Finally, platforms must take a stronger stand against online abuse by strengthening localised content-moderation teams and adopting clear, transparent guidelines on gender-based violence. Establishing direct, prioritised reporting channels for women in public life facing coordinated attacks is a critical step in making the digital space safer for all.

The Score Index

Botswana, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	5	5	Botswana maintained a perfect record of zero internet shutdowns in 2025, continuing its long-standing practice of non-interference with network access. No deliberate disruptions were recorded by regulators or platforms.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	3	4	National 4G population coverage reached ~98–99% and UASF projects expanded rural connectivity and school access. However, rural household internet access remains ~20.8% and data affordability still exceeds the global 2% income benchmark despite 2025 tariff reductions.
False News Criminalisation	P22(2)	1	2	False-news and cybercrime provisions remain in law and can be used to restrict expression. Although no prosecutions were recorded in 2025, the existence of these provisions continues to produce a chilling effect.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Sedition Legislation	P22(2)	1	1	Sedition provisions under the Penal Code remain in force. While few or no prosecutions occurred in 2025, their continued presence creates legal uncertainty and risk for journalists and activists.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	2	3	Arrests for online speech remain rare. The report notes limited incidents of harassment and intimidation, including doxxing threats against journalists, but no widespread arrests or enforced disappearances.
Data Protection Legislation.	P42	3	4	The Data Protection Act No.18 of 2024 (effective January 2025) established a comprehensive regime and created the Information and Data Protection Commission (IDPC) with enforcement powers, breach-notification rules, and penalties up to P50 million (~USD 370,000). Implementation capacity gaps remain.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	2	2	Platform transparency reports from Meta for 2025 shows a total of two government requests for content removal in Botswana. Meta received 2 emergency disclosure requests (no legal-process requests), affecting 8 users/accounts, but produced 0% data (no compliance). Google and TikTok reported no removal requests at all.
Invasion of Privacy of Communications	P41	2	2	Surveillance laws require warrants under the Controlled Investigations Act (2022), but broad “national security” provisions and limited independent oversight of intelligence agencies remain. Smart-city surveillance expansion lacks a dedicated regulatory framework.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	3	4	The Access to Information Act No.16 of 2024 provides a statutory right to information and requires public bodies to appoint information officers. Implementation has begun but full operationalisation and reporting remain ongoing.
AI and Emerging Technologies national strategies	P39(6)	2	2	Botswana completed a UNESCO AI Readiness Assessment (2025) and is developing a national AI strategy. Infrastructure investments (e.g., BOTSAT-1 satellite) and policy consultations are underway, but no binding AI law exists yet.
Adoption of specific child laws, policies and measures promoting children’s digital safety and privacy online	P39(6)	2	2	Child protections exist through the Data Protection Act (2024) and AU policy alignment, but Botswana still lacks a standalone Child Online Protection law and enforcement structures remain fragmented.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Digital Inclusion	P37(3)	3	4	The Persons with Disability Act (2024) and UASF programmes support inclusion and school connectivity. However, implementation gaps persist, particularly for rural communities and persons with disabilities, and affordability barriers remain.
Total (out of 60):	2024: **28**		**2025 35**	

Botswana records a solid improvement in the LONDA Score Index for 2025, rising from 28/60 in 2024 to 35/60. This 7-point increase reflects meaningful progress in several areas, particularly the entry into force of key legislation (Data Protection Act, Access to Information Act, Persons with Disability Act), strong connectivity expansion, and a stable environment free from shutdowns. Remaining gaps relate to rural access, affordability, surveillance oversight, and the absence of dedicated AI and child online safety laws. The trajectory is positive, but sustained implementation and funding are needed to close the remaining gaps and move toward the high 40s or above.



Cameroon

By Rigobert Kenmogne

Executive Summary

In 2025, several internet outages and disruptions[1], network technical problems, monitoring and surveillance of personal data, and intimidation of journalists for expressing their opinions all contributed to violations of digital rights in Cameroon. This study aims to demonstrate how these violations impact respect for the rule of law and the development of democracy, in addition to highlighting efforts implemented to promote digital inclusion and mitigate these defects. Based on various Cameroonian practices and laws, we focus on identifying the mechanisms of online violations of digital rights and freedoms, assessing the shortcomings of the current legal framework, and finally evaluating progress, particularly new laws that support respect for digital rights and digital inclusion.

Our research methodology employs a mixed-methods approach, combining semi-structured interviews and

testimonies with users and stakeholders in the internet ecosystem, along with a quantitative analysis of data on violations and progress recorded in telecommunications systems, platforms, and internet users for the period up to 2025. The overall methodology utilises the Paradigm Initiative's Score Index[2]. The data in this report are collected through a review of legislation, government policy documents, press articles, and public statements; a comparative analysis of regional and international human rights instruments; and an analysis of progress in digital policies.

Cases of digital rights violations in Cameroon in 2025 are a central concern, given the socio-political context. Recorded violations include internet shutdowns, arrests of journalists and activists, website censorship, website blocking, social media blocking, internet network disruptions, communications monitoring or mass surveillance systems, and theft of personal data. The 2025 report analyses the legal framework governing Cameroon's digital landscape through the following laws: the 2024 law on the protection of personal data, the 2023 law on the protection of children online[3], the 2010 law on cybersecurity and cybercrime, the 2010 law on electronic communications[4], the 2011 framework law on consumer protection[5], and the 2012 decree establishing the procedures for managing the Special Telecommunications Fund[6]. Due to the socio-political context, particularly the presidential election of October 12, 2025[7], Cameroon experienced major internet outages between October 23 and November 7, 2025, according to a report by OONI[8]. All electronic communication systems were severely disrupted both before and after the announcement of the presidential election results.



1. Reuters ''Cameroon's Internet access disrupted as election protests continue'' https://www.reuters.com/world/africa/internet-connectivity-cameroon-is-significantly-disrupted-netblocks-says-2025-10-23/ (Accessed on December 20, 2025).
2. Paradigm Initiative '' The Score (TS) Index '' https://paradigmhq.org/londa-score-index/#:~:text=Where%20there%20is%20a%20bill,publishes%20reports%20of%20actions%20taken.&text=When%20countries%20,,issue%20content%20removal,allows%20a%20right%20of%20appeal. (Accessed on November 24, 2025).
3. Presidency of the Republic of Cameroon. "Law No. 2023/009 of July 25, 2023, establishing a charter for the protection of children online in Cameroon" https://www.prc.cm/fr/multimedia/documents/9701-loi-n-2023-009-du-25-07-2023 (Accessed on November 24, 2025).
4. Telecommunications Regulatory Agency. "Law No. 2010/021 of December 21, 2010 governing electronic commerce in Cameroon" https://www.art.cm/sites/default/files/documents/Loi_2010-013_communications_electroniques.pdf (Accessed on November 24, 2025).
5. Ministry of Commerce. "Framework Law No. 2011/012 of May 6, 2011 on consumer protection in Cameroon"https://www.mincommerce.gov.cm/sites/default/files/documents/loi-cadre-n-2011-012-du-06-mai-2011-portant-protection-du-consommateur-au-cameroun.pdf (Accessed on November 24, 2025).
6. National Agency for Information and Communication Technologies. "Decree No. 2012/308 of June 26, 2012, establishing the procedures for managing the Special Telecommunications Fund" https://www.antic.cm/images/stories/data/IMG/pdf/decrets/Modalites_de%20gestion_FST-26-06-2012.pdf. (Accessed on November 24, 2025).
7. Business Human Rights: "Cameroon: Internet access disruptions as the country awaits presidential election results" https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/cameroun-perturbations-de-lacc%C3%A8s-%C3%A0-internet-alors-que-le-pays-attend-les-r%C3%A9sultats-de-l%C3%A9lection-pr%C3%A9sidentielle/ (Accessed on November 24, 2025).
8.

Introduction

Cameroon's real GDP grew by 3.5% between 2024 and 2025, compared to 3.2% in 2023[9]. Cameroon is a lower-middle-income country with a population of 28.37 million in 2023. [10]By 2025, mobile phone penetration had reached 87%, while internet penetration was 41.9%, representing a year-on-year increase of 2.6%[11]. 4G/5G coverage reached 64.72% of the country. Cameroon has over 25 million connected devices and 12.87 million internet users[12]. According to a report entitled "State of Digital Development and Trends in Africa: Challenges and Opportunities", published in April 2025 by the International Telecommunication Union (ITU), more than 40% of Cameroonians used the Internet individually in 2023[13]. In the context of the evolution of ICT in Africa for 2025, Cameroon ranks 30th out of 42 countries with 46.3 points, indicating progress in the ICT sector.

In 2025, Cameroon made slight progress in its strategy for developing its internet ecosystem. The National Development Strategy 2020-2030 (SND30), [14]which outlines the main areas for infrastructure development and technological growth, recorded progress in 2025, according to a report[15] from the steering committee. However, the reform of laws on information and communication technologies (ICTs), which had been initiated, made little progress in 2025, despite the Ministry of Posts and Telecommunications (MINPOSTEL) announcing an urgent review of several laws.

Internet Access and Network Disruptions

Cameroon experienced several internet and telecommunications network disruptions in October and November 2025[16]. Amid the post-election crisis, internet networks were completely shut down for several hours on the morning of October 23, 2025, the date initially scheduled for the Constitutional Council of Cameroon to announce the presidential election results. According to a report published by OONI[17], partial internet disruptions were severe between November 1 and 7, 2025, affecting major platforms including TikTok, Facebook, Instagram, and Telegram. During the same period, communications and messaging services were disrupted across the country[18].

Cameroon is one of the countries in sub-Saharan Africa where broadband internet prices remain high[19]. Despite the high costs, the quality of internet

9. https://www.banquemondiale.org/fr/news/press-release/2025/07/15/cameroon-economic-update-harnessing-forests-and-natural-wealth-for-sustainable-growth
10. World Bank "Cameroon" https://www.banquemondiale.org/ext/fr/country/cameroon (Accessed on November 24, 2025).
11. Kamer Android. "Internet and social networks in Cameroon: key figures for 2025" https://kamer-android.com/2025/02/26/internet-et-reseaux-sociaux-au-cameroun-les-chiffres-cles-de-2025/?srsltid=AfmBOoqjkOt-0mpuDJhU4Uj3LSP0YUCDtYoMKz4bB_9hm569qg5SPkVw1 (Accessed on November 24, 2025).
12. Kamer Android. "Internet and social networks in Cameroon: key figures for 2025" https://www.teamfrance-export.fr/fiche-marche/tech/telecom-internet-et-broadcast/CM (Accessed on November 24, 2025).
13. Investing in Cameroon. "Internet: With over 40% of individuals active, Cameroon surpasses the African average despite lagging behind in broadband access." https://www.investiraucameroun.com/telecom/1606-22118-internet-avec-plus-de-40-d-individus-actifs-le-cameroun-depasse-la-moyenne-en-afrique-malgre-le-retard-sur-le-haut-debit (Accessed on November 24, 2025)
14. Ministry of Economy, Planning and Regional Development 'SND30' https://minepat.gov.cm/fr/snd30/
15. Minepat. "Implementation of the SND30" https://minepat.gov.cm/2025/12/16/mise-en-oeuvre-de-la-snd30-des-progres-significatifs-enregistres/#:~:text=La%20session%20de%202025%20du,ajuster%20la%20trajectoire%202025%2D2030. (Accessed on December 20, 2025).
16. Investing in Cameroon: 'Internet disrupted in Cameroon due to a failure on submarine cables' https://www.investiraucameroun.com/telecom/1503-20447-internet-perturbe-au-cameroun-a-cause-d-une-panne-sur-des-cables-sous-marins (Accessed on November 24, 2025).
17. ONNI. ''Cameroon blocked social media amid post-election protests'' https://explorer.ooni.org/findings/393608039300 (Accessed on November 24, 2025).
18. Investing in Cameroon: "Poor network quality: Camtel and Orange Cameroon pass the buck amid widespread discontent" https://www.investiraucameroun.com/gestion-publique/1802-21669-mauvaise-qualite-du-reseau-camtel-et-orange-cameroun-se-renvoient-la-responsabilite-dans-un-climat-de-mecontentement (Accessed on December 20, 2025).
19. Ecofin Agency. "In sub-Saharan Africa, the price of broadband remains the most expensive" https://www.agenceecofin.com/actualites/2104-127727-en-afrique-subsaharienne-le-prix-du-haut-debit-reste-le-plus-cher-du-monde-uit (Accessed December 20, 2025).

services is frequently poor[20]. Despite the high costs, the quality of internet services is frequently poor. At Orange Cameroon and MTN, 2 gigabytes cost 1,000 FCFA (US$1.80) for 24 hours. At Camtel, 1 gigabyte costs 500 FCFA (US$0.90). Settings facilitating connections without internet credit for MTN and Orange operators were deactivated for users during October and November 2025.

Disruptions to internet networks, whether intentional or unintentional, constitute a violation of Principle 38(2) of the Declaration of Principles of the African Court on Human and Peoples' Rights (ACHPR), which states that "States shall not tolerate or be involved in the interruption of access to the internet and other digital technologies targeting segments of the population or the entire population."

Freedom of Expression and Access to Information

In 2025, freedom of expression in Cameroon was severely threatened due to the presidential election. Journalists, activists, and bloggers were intimidated, directly or indirectly, for their online opinions or political choices. A month before the presidential election, a letter from the president of the National Communication Council (CNC) called for the suspension, effective September 27, 2025, of political debate programmes on several private media outlets, including Radio Télévision Siantou and Equinoxe TV. [21]

The post-election[22] crisis that shook the entire country, compounded by the political crises in the two Anglophone

20. Invest in Cameroon. "Poor network quality: Camtel and Orange Cameroon pass the buck in a climate of discontent" https://www.investiraucameroun.com/gestion-publique/1802-21669-mauvaise-qualite-du-reseau-camtel-et-orange-cameroun-se-renvoient-la-responsabilite-dans-un-climat-de-mecontentement (accessed November 24, 2025).
21. DW "Presidential election in Cameroon: the media as spectators" https://www.dw.com/fr/cameroun-medias-debats-politiques/a-73981995 (accessed on December 20, 2025).
22. Amnesty International 'Cameroon rampant atrocities amid anglophone regions must be stopped' https://www.amnesty.org/fr/latest/news/2023/07/cameroon-rampant-atrocities-amid-anglophone-regions-must-be-stopped/ (accessed November 24, 2025).

regions, continues to negatively impact social life and freedom of expression in Cameroon. Within this context of crisis, political disinformation is on the rise, with consequences for young women and girls involved in politics.[23]

For nearly 10 years, hate speech has generally pitted supporters of the ruling Cameroon People's Democratic Movement (CPDM) against supporters of opposition parties, notably the Movement for the Renaissance of Cameroon (MRC) and the Cameroon Party for National Reconciliation (PCRN).[24] [25] In Cameroon, Law No. 2019/020 criminalises hate speech. In Cameroon, Law No. 2019/020 criminalises hate speech.[26] As of 2025, no explicit convictions for hate speech had been handed down in Cameroon.

Since the election of October 12, 2025, demands for LGBTQ+ rights have been increasingly voiced. This demand for respect for LGBTQ+ rights is championed by Alice Nkom,[27] a lawyer and human rights advocate. Certain provisions of the law of December 12, 2010, relating to cybersecurity and cybercrime stifle freedom of expression, in particular Article 78,[28] which punishes "anyone who publishes or disseminates by means of electronic communications or an information system news without being able to provide proof of its veracity or justify that he had good reasons to believe in the truth of said news"[29], as well as communications from LGBTQ+ communities.[30]

23. WACSI "Disinformation in Cameroon: How false narratives affect the rights of girls and women" https://fr.wacsi.org/wp-content/uploads/2025/07/Issue-Paper-FR-Desinformation-au-Cameroun-comment-les-faux-recits-affectent-les-droits-des-filles-et-des-femmes-2.pdf (Accessed on December 20, 2025).
24. MRC https://mrcparty.net/
25. PCRN https://www.pcrn-france.fr/
26. Article 241(2), Law No. 2019/020 of December 24, 2019, supplementing certain provisions of Law No. 2016/007 of July 12, 2016, establishing the Penal Code
27. BBC "I will always defend homosexuals because they are thrown in prison like dogs" https://www.bbc.com/afrique/articles/c30n6j3gng8o (accessed 24 November 2025).
28. AFAD "Cameroon-Law-relative-to-cybersecurity-and-cybercrime-of-21" https://www.afapdp.org/wp-content/uploads/2018/05/Cameroun-Loi-relative-a-la-cybersecurite-et-a-la-cybercriminalite-du-21-decembre-2010.pdf (accessed December 20, 2025).
29. Article 78(1), Law No. 2010/012 of December 21, 2010 relating to cybersecurity and cybercrime in Cameroon.
30. Article 83(1), Law No. 2010/012 of December 21, 2010 relating to cybersecurity and cybercrime in Cameroon.

In 2025, Meta's transparency report indicates that the Cameroonian government made one (1) data access request for legal proceedings[31] and one (1) request for user account data. No emergency disclosure requests were made during this period.

Between 2023 and 2025, 38 global restrictions[32] requested by Meta based on community standards were applied to platform users in Cameroon.

All the requested data relates to cases of legal proceedings. Content restrictions were implemented by Meta based on Cameroonian legislation, specifically the law on cybersecurity and cybercrime, during the same period. Meta responded to the Cameroonian government's requests for data access, but the rate of compliance and due diligence was not indicated. The government did not make any requests to remove user data from the TikTok platform. In 2025, Google[33] received no requests from the government to remove content. Regarding freedom of expression, the state continues to control certain media outlets, sensitive online content, and the opinions of opposition leaders and some journalists, an attitude contrary to Principle 41[34] of the African Declaration on Human and Peoples' Rights.

Data protection, Privacy, and cybersecurity

Cameroonian cyberspace was the victim of several types of attacks in 2025,[35] including hacking of the Ascoma Cameroon (ASCOMA) website,[36] phishing attacks, identity theft, and the theft of personal data. Faced with the scale of these cyber threats, Cameroonian authorities, through the Ministry of Posts and Telecommunications (MINPOSTEL) and the National Agency for Information and Communication Technologies (ANTIC), as well as other civil society organisations, launched extensive cybersecurity awareness campaigns targeting young people in 2023

Cybersecurity and cybercrime are governed by a legal framework, specifically the 2010 law on cybersecurity and cybercrime.[37] In 2024, Law No. 2024/017 of December 23, 2024, relating to the protection of personal data was promulgated[38], but this law is not applicable in terms of sanctions due to the absence of designation of the members of the Personal Data Protection Authority as defined by Article 53.

Privacy and Monitoring

In 2025, no information was published regarding the evolution of state surveillance and the technologies deployed for this purpose. Cameroon has surveillance cameras at several intersections in major cities for security reasons, according to the police. The processing of personal data is not currently governed by the law on the protection of personal data. The 2025 elections did not benefit from this law regarding data management.

In the context of the 2025 elections, allegations were reported concerning the use of intrusive technologies by the government. These rumours mentioned software capable of tracking, grouping, tracing, and recording conversations of individuals in one or more WhatsApp groups to analyse user activity. No data was reported on technologies developing systems for monitoring disinformation.

Although the nation has several

31. Meta. ''Cameroon''. https://transparency.meta.com/reports/government-data-requests/country/CM/ (accessed November 24, 2025).
32. Meta. "Cameroon". https://transparency.meta.com/reports/content-restrictions/country/CM/ (accessed November 24, 2025)
33. Google. "Cameroon". https://transparencyreport.google.com/government-removals/government-requests/CM?hl=en (accessed November 24, 2025).
34. ACHPR. Principle 41, Declaration of Principles on Freedom of Expression and Access to Information in Africa
35. Rhopen Labs "Cybersecurity in Cameroon in 2025: a national imperative in the face of growing threats and the crucial role of soclabs" https://rhopenlabs.africa/2025/08/29/la-cybersecurite-au-cameroun-en-2025-un-imperatif-national-face-aux-menaces-croissantes-et-le-role-crucial-de-soclabs/ (Accessed on December 20, 2025).
36. Ransomware "ASCOMA Cameroon" https://www.ransomware.live/id/QVNDT01BIENhbWVyb29uQHdvcmxkbGVha3M= (Accessed on December 20, 2025).
37. Article 74, Law No. 2010/012 of December 21, 2010 relating to cybersecurity and cybercrime in Cameroon.
38. Presidency of the Republic of Cameroon 'Law No. 2024/017 of December 23, 2024, on the protection of personal data in Cameroon' https://www.prc.cm/fr/multimedia/documents/10258-loi-n-2024-017-du-23-12-2024-web (accessed November 24, 2025).

surveillance cameras on the streets of major cities, there has been no information released in 2025 regarding biometric surveillance using facial recognition systems (FRS) and other biometric technologies for mass surveillance in public spaces and their implications for privacy, non-discrimination, and freedom of assembly.

Evolution of ICT and Emerging Technologies

Cameroon has committed to the development of artificial intelligence and technological innovation. In July 2025, institutions, through the Ministry of Posts and Telecommunications, initiated consultations aimed at developing a strategic plan for artificial intelligence.[39] However, the lack of enforcement of the law on the management of personal data hinders the regulation of emerging technologies and innovation. Nevertheless, the Declaration of Principles on Freedom of Expression and Access to Information in Africa encourages states to commit to "the development, use, and application of artificial intelligence."[40] Facial recognition technologies are not yet integrated into AI development processes in Cameroon. Furthermore, emerging technologies such as blockchain and VR/AR are not yet widely adopted. Opportunities for participation in public consultations and stakeholder consultations regarding policies related to new and emerging technologies are very limited, as most of the organisations consulted are public sector bodies.

Digital Inclusion

The Special Telecommunications Fund mandates that telecom companies donate 3% of their yearly earnings to the nation's technological infrastructure.[41] A second telecommunications financing source for the ICT sector stipulates that "Network operators and service providers are subject to an annual fee of 1.5% of their revenue excluding taxes."[42] In the same year, the Ministry of Posts and Telecommunications (MINPOSTEL)[43] with assistance from the World Bank, developed a national strategy for the development of universal digital services, which was validated by the Cameroon Digital Transformation Acceleration Project (PATNUC), allowing Cameroon to take another step toward digital inclusion.

39. Ministry of Posts and Telecommunications https://www.minpostel.gov.cm/index.php/en/actualites/485-conia (accessed November 24, 2025).
40. ACHPR. Principle 39 (6), Declaration of Principles on Freedom of Expression and Access to Information in Africa
41. Investing in Cameroon: "As part of the development of the country's technological infrastructure, the Special Telecommunications Fund stipulates that telecommunications operators contribute 3% of their annual turnover." Telecommunications: ART collects 73 billion FCFA in royalties and generates a net profit of 12 billion in 2024 - Investing in Cameroon (Accessed December 20, 2025).
42. Article 34 (3), Law No. 2010/013 of 21 December 2010 Governing Electronic Communications in Cameroon
43. PATNUC "Digital for all: Cameroon validates its national universal service strategy" https://patnuc.cm/2025/07/11/numerique-pour-tous-le-cameroun-valide-sa-strategie-nationale-de-service-universel/ (Accessed on December 20, 2025).

The Score Index

Cameroon, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet outages	P38(2)	5	1	In 2025, internet outages in Cameroon originate from telecommunications operators. Operators regularly provide only brief updates on network status regarding these incidents.[44]
Non-existent laws, policies and other measures aimed at promoting universal, equitable, affordable and meaningful access to the Internet	P37	2	2	The 2010 Cybersecurity and Cybercrime Act provides provisions for universal and equitable access to the Internet.
Criminalising fake news	P22(2)	2	3	Certain provisions of the Penal Code punish false news.[45]
Sedition legislation	P22(2)	2	3	The Penal Code punishes seditious cries or songs.[46]
Arbitrary arrests and harassment of the media, human rights defenders and citizens	P20(1) & (2)	3	1	In 2025, some media men were harassed, threatened or arrested in connection with their opinions on the presidential election.[47]
6. Data protection legislation.	P42	4	3	Cameroon has a law on the protection of personal data, specifically Law No. 2024/017 of December 23, 2024, which is only partially applicable. Businesses and stakeholders must comply by June 2026.
States intervene and demand the removal of online content by internet intermediaries.	P38 & P39(4)	3	3	By 2025, requests to remove content will be made within the framework of legal proceedings.
Breach of confidentiality of communications	P41	4	2	Invasions of privacy are occurring on a small scale.
The government's inability to proactively disclose and	P29(3)	4	2	Disclosure efforts are very limited.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
disseminate information on digital technologies.				
National strategies for AI and emerging technologies	P39(6)	4	3	An AI strategy exists for 2025. It has been updated.[48]
Adoption of laws, policies and measures specific to children that promote digital safety and children's online privacy.	P8 P40(1)	2	3	Cameroon has a law on the digital safety of children.[49]
Digital Inclusion	P37(3)	1	2	The government has established a national program on digital technologies. In 2025, this program did not submit its activity report.
Total (out of 60):	2024: **31**		**2025 27**	

1. Afriqueitnews "Internet disrupted in Cameroon: an incident on the submarine cable behind the outages" https://afriqueitnews.com/tech-media/internet-perturbe-cameroun-incident-cable-sousmarin-derriere-coupures/#:~:-text=les%20coupures%20%2D%20AITN-,Internet%20perturb%C3%A9%20au%20Cameroun%20:%20un%20incident%20sur%20le,sous%E2%80%91marin%20derri%C3%A8re%20les%20coupures&text=Depuis%20le%2023%20octobre%202025,la%20remise%20en%20service%20compl%C3%A8te. (Accessed December 20, 2025).
2. Article 113, Cameroonian Penal Code.
3. Article 235, Cameroonian Penal Code.
4. Article 113, Cameroonian Penal Code.
5. We Are Tech "Cameroon develops a national AI strategy based on seven pillars" https://www.wearetech.africa/fr/fils/actualites/tech/le-cameroun-developpe-une-strategie-nationale-de-l-ia-adossee-a-sept-piliers (Accessed November 24, 2025).
6. Presidency of the Republic of Cameroon 'Law No. 2023/009 of July 25, 2023 establishing a charter for the protection of children online in Cameroon' https://www.prc.cm/fr/multimedia/documents/9701-loi-n-2023-009-du-25-07-2023 (accessed November 24, 2025).
7. Invest in Cameroon "Quality of service: the telecoms regulator imposes fines of 2.6 billion FCFA on MTN and Orange Cameroon" https://www.investiraucameroun.com/gestion-publique/0707-22216-qualite-de-service-le-regulateur-telecoms-inflige-des-amendes-de-2-6-milliards-de-fcfa-a-mtn-et-orange-cameroun (Accessed on December 20, 2025).
8. Business Human Rights "Cameroon: Internet access disruptions as the country awaits presidential election results" https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/cameroun-perturbations-de-lacc%C3%A8s-%C3%A0-internet-alors-que-le-pays-attend-les-r%C3%A9sultats-de-l%C3%A9lection-pr%C3%A9sidentielle/ (Accessed December 20, 2025).
9. British Broadcasting Corporation (BBC) https://www.bbc.com/afrique/region-41449099 (accessed 24 November 2025).

Conclusion

Due to the electoral operations, Cameroon experienced widespread disruptions to its internet network in 2025. No immediate government sanctions were imposed on telecommunications operators for their failure to provide internet services. However, a few months before the presidential election in Cameroon, the Telecommunications Regulatory Agency (ART), the regulator of telecom services in Cameroon, levied fines totalling 2.6 billion FCFA on mobile phone operators MTN and Orange Cameroon for poor service quality.[50]

These disruptions have had

repercussions on neighbouring countries.[51] Several principles of the African Charter have been violated, including those concerning freedom of expression, access to information, and the protection of personal data. Despite these violations, the government has demonstrated a commitment to improving digital rights and inclusion through ongoing reforms that promote legal instruments related to digital rights and freedoms. Cameroon recorded more than 10 days of internet disruptions in 2025 aimed at stifling political demands and limiting hate speech, as was the case in 2017.[52]

Recommendations

To the Government

- Prepare a report on the use of personal data and emerging technologies, and the implementation of the personal data law;
- Launch broad consultations for the development of the National Artificial Intelligence Strategy;
- Conduct an independent audit and ensure transparency in technology markets.

In Parliament

- Equip the country with new, appropriate laws and regulations that take into account the evolution of ICTs;
- Strengthen regulations on hateful and dangerous online content.

To Civil Society Organizations and Individuals

- Develop advocacy efforts and increase awareness-raising activities on the use of personal data;
- Strengthen the capacity of stakeholders regarding generative AI and digital rights.

To Telecommunications Companies

- Ensure transparent communication regarding disruptions and incidents on telecommunications networks;
- Limit access to data in cases of illegal requests from government institutions.



Central African Republic

By Arsène Tungali

Executive Summary

This report assesses thematic areas including internet access and disruptions, online freedom of expression and access to information with a look at gendered disinformation, data protection and cybersecurity, privacy and surveillance, a section on developments in ICT and emerging technologies as well as one on digital inclusion that also looks at the Universal Service Fund in the Central African Republic (CAR) for the year 2025.

In addition to desk research and interviews conducted, this report assessed the country's compliance with the African Charter on Human and People's Rights Declaration of Principles on Freedom of Expression and Access to Information (the Declaration) in the covered areas, using Paradigm Initiative's TheScore Index rate of 31 out of 60 (no change in the overall score from last year, although a few changes on some areas). The report ends with a set of recommendations on ways to improve the state of digital rights and inclusion in the country, drawing on some of last year's report recommendations that are yet to be implemented.

Introduction

The Central African Republic (CAR) is a French-speaking country in the central region of Africa, with Bangui as its capital. It has a surface area of 622,980 km2 and a population estimated by the Worldometer (using UN estimates) at 5.5 million in 2025. Independent since 1960, the country is currently led by Faustin Archange Touadéra, since his first election in 2016. Citizens were called for general elections on December 28 2025 which saw the incumbent win and start his third term after the 2023 change of the Constitution that scrapped the presidential term limit.

On the legislative front, this report speaks of the laws adopted in 2024 (on privacy and on cybersecurity) that are still lagging in terms of their implementation measures. It also speaks of one contentious bill, on freedom of the press, passed by the Parliament in 2025 but is yet to be signed into law by the President. This could bring the country behind by reintroducing the penalisation of press offenses which were already depenalised, constituting a threat to the freedom of journalists to do their job. This report will also highlight some improvements such as in the active use of the optic fiber deployed in 2024 and the entry of at least one new operator in the commercialisation of this fiber capacity; efforts that join those towards the operationalisation of the Universal Service Fund whose initial steps were taken in 2025.

In terms of methodology, a multifaceted approach will be considered consisting of combining empirical and desk-research methods to assess both quantitative and qualitative aspects of digital rights and inclusion in the Central African Republic. For this report, compliance with the African Charter on Human and People's Rights' Declaration of Principles on Freedom of Expression and Access to Information[1] will be assessed for every issue discussed, using all the key indicators of Paradigm Inititative's TheScore Index[2], that determines the scope of the report.

1. The ACHPR's Declaration: https://achpr.au.int/en/node/902 (accessed on November 14, 2024)
2. TheScore Index: TheScore is a digital rights index developed by Paradigm Initiative that evaluates compliance of the country about key human rights elements and is inspired by the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information.

Internet Access and Disruptions

In terms of connectivity, Data Reportal[3] shares that there were 839,000 individuals using the internet in CAR at the start of 2025 (compared to 616,600 in 2024), when internet penetration stood at 15.5% (compared to 10.6% in 2024. A total of 2.07 million cellular mobile connections were active (compared to 1.86 million in 2024), with this figure equivalent to 38.1% of the total population (compared to 32% in 2024). Unfortunately, there is no up-to-date data from the Regulatory Agency's online platforms and thewebsite[4] remains obsolete.

The progress presented above is a positive sign that draws from 2024 that we called "the year of connectivity", in the 2024 Londa report[5] because citizens of CAR witnessed the deployment and start of the operationalisation of the 900 km optic fiber cable (part of the the Central African Backbone project), linking the country to its neighbors, the Republic of Congo and Cameroon, and to the Atlantic Ocean, providing affordable and high-speed connectivity for the region. This EUR33 million project was jointly funded by the African Development Bank and the European Union.

As of 2024, the country still has three main operators (offering both internet and voice), which are Telecel Centrafrique, Orange Centrafrique and Moov Africa Centrafrique. Like in the majority of African countries, citizens in CAR access the Internet mainly through their mobile phones. With an operator like Moov, 1000XAF (US$nearly 1.8) gives 2Gb of data with a 24h validity while, according to the World Bank, daily income in the country is extremely low. The minimum wage, set at CFA35,000 per month in 2025, equivalent to US$1.15 per day. However, a large part of the population lives below the international poverty line, often on less than US$2.15 per day. This speaks to the internet affordability in CAR.

In terms of network disruptions, there are no reports of state-imposed disruptions in the year 2025. However, like in the year before, many news outlets reported the low quality of internet connectivity or some network disruptions such as with Telecel, one of the local operators. In August 2025, students complained about how the low speed was affecting their productivity for their school related activities. Business owners who do business with foreign countries and are having issues connecting with them[6]. In October 2025, inhabitants of Maka 3, a village in the south west of Bangui were complaining about the inability to even get a telephone signal in order to interact with the rest of the country, let alone internet connectivity[7]. This situation is present in various other African villages that are less economically attractive to operators, with users having to travel miles away or to locate hills or mountains to find a signal. This calls for the State to find alternative ways, including activating initiatives such as the Universal Service Fund to serve these citizens.

With the deployment of fiber optics with funding from the African Development Bank (AfDB) and the European Union (EU), a highlight of Londa 2024 report, CAR has shown positive signs in ensuring the cable reaches the countryside. The Council of Ministers on April 17 2025, revealed an agreement with SOS Telecom for that deployment in the regions of Lobaye, Mambéré-Kadéï, Ouham-Pendé as well as on the axis Bangui-Bambari. "This project aims to improve connectivity in often isolated areas, supporting access to digital services and economic development', stated the Council of ministers after their meeting."[8] A strategic diagnosis on the digital ID ecosystem and civil state was also validated, opening the way to the modernisation of public services across the country.

In practice, when the government, through its international partners, has secured the

3. Digital 2025 : The Central African Republic: https://datareportal.com/reports/digital-2025-central-african-republic (accessed on December 4, 2025)
4. https://arcep.cf/fr/#
5. Londa 2024 Central African Republic: https://paradigmhq.org/wp-content/uploads/2025/09/Londa-24-CAR.pdf (accessed on February 5, 2026)
6. Centrafrique : Telecel confirme des perturbations sur son réseau :Ministers https://www.radiondekeluka.org/89872-centrafrique-telecel-confirme-des-perturbations-sur-son-reseau
7. Centrafrique : Maka 3 plongé dans l'isolement, faute de réseau téléphonique : https://oubanguimedias.com/2025/10/22/centrafrique-maka-3-plonge-dans-lisolement-faute-de-reseau-telephonique/ (accessed on December 4, 2025)
8. Développement numérique et infrastructures en Centrafrique : avancées et défis : https://corbeaunews-centrafrique.org/developpement-numerique-et-infrastructures-en-centrafrique-avancees-et-defis/ (accessed on December 3, 2025)

connection to an infrastructure such as optic fiber, the next step is for the private sector to enter the market, request and obtain the necessary license to deploy and commercialise the capacity provided by the optic fiber. It is in that line that the Brazilian entity SOS Telecom secured one in April 2025 to deploy and commercialize fiber in the remote regions.[9]

The Brazilian entity acquired a first of its kind license, the passive infrastructure management license with authorisation "to build and lease passive mobile radio network infrastructure—including towers, antennas, and electrical installations—and to contribute to the deployment of fiber optics." As a passive infrastructure manager, the company positions itself as a technical partner rather than a commercial rival to the three existing telecom operators. It will provide operators with key infrastructure that they can lease to deploy or expand their networks, particularly in low-profitability areas.[10]

With the 33 million in funding from the AfDB and the EU that helped deploy 900km of fiber connecting CAR to Cameroon and Congo Brazzaville in 2024, success stories have started to be shared. In this video shared on AfDB website,[11] Junior Thierry was able to create a humanoid robot he named Mama Africa and make her function using the broadband connectivity that he now has access to. Students claim to be able to easily stream videos, create and deploy mobile apps made in CAR. From the Digital Incubator built at the University of Bangui, they can learn how to deploy or repair optic fiber as well as 3D printing, etc.

Online Freedom of Expression and Access to Information

Freedom of expression is recognised

9. La Centrafrique octroie une licence d'exploitation a SOS Telecoms : https://www.agenceecofin.com/actualites-numerique/1804-127674-la-centrafrique-octroie-une-licence-d-exploitation-au-bresilien-sos-telecom (accessed on December 3, 2025)
10. Ce que change l'arrivée de SOS Télécoms sur le marché télécoms centrafricain : https://www.agenceecofin.com/actualites-numerique/2407-130361-ce-que-change-l-arrivee-de-sos-telecoms-sur-le-marche-telecoms-centrafricain (accessed on December 3, 2025)
11. Succes Story: Avec l'arrivée de la fibre optique, la Centrafrique entre de plain-pied dans l'ère numérique : https://www.afdb.org/fr/news-and-events/multimedia/video/success-story-avec-larrivee-de-la-fibre-optique-la-centrafrique-entre-de-plain-pied-dans-lere-du-numerique-82970 (accessed on December 3, 2025)

and guaranteed by the Central African Republic's Constitution, 2023[12] under Article 23[13] and access to information as well as freedom of the press are guaranteed under Article 24. However in 2025, there is a set back from what was a highlight in 2024: the fact that Law No 20-027 of December 21 2020, related to freedom of communication in Central African Republic[15], was labeled as a progressive one in the sense that it depenalises press offences, making sure journalists are technically not prosecuted for what they say while doing their job. The National Assembly adopted by acclamation, on May 26 2025 a new bill on freedom of the press and of communication, that brings the country back in terms of press offenses which will now be penalised, if the legislation is passed into a law. "This is considered as a strategy to muzzle the press... This bill gives legislators the power, in cases of press offenses, to hold responsible the journalist who committed the offense, their editor-in-chief, and even the publisher", claimed press professionals.[16] As per the law, the president had to assent to it within 15 days after it had been adopted by legislators but this was not done. This Bill has therefore not yet been passed into a law.

CAR's Freedom House's Freedom In the World 2025 report ranking hasn't changed from last year's 5/100, presenting the country as "not free" and listed among the category of "worst of the worst". The Freedom House report states that the Central African Republic "suffers from pervasive insecurity in

12. The Constitution de la 7e République (enacted on August 30, 2023) : https://mjp.univ-perp.fr/constit/cf2023.htm (accessed on November 12, 2024)
13. Article 23 of the 2023 Constitution: "Everyone has the right to freedom of expression. This right implies the freedom to express one's opinions or beliefs, in particular through speech, writing and images, subject to respect for the law, public order and morality.
14. Article 24 of the 2023 Constitution: "Everyone has the right to information. Freedom of the press, of information and of broadcasting by radio and television, the written press or any other means of communication shall be guaranteed, subject to respect for the law, public order and morality..."
15. Law on Freedom of Communication: https://drive.google.com/file/d/19UeGtAbU00TQ9UWN_rs-hsypa-6xRLzq/view (accessed on January 10, 2025)
16. Centrafrique : vives protestations contre la nouvelle loi sur la liberté de la presse : https://www.rfi.fr/fr/afrique/20250529-rca-vives-protestations-contre-la-nouvelle-loi-sur-la-libert%C3%A9-de-la-presse (accessed on december 5, 2025)

much of the country; the Government forces have disbanded most rebel groups, but militias continue to operate in the country's hinterland, particularly round mining sites".[17]

The Central African Republic ranked 72nd in Reporters Without Borders (RSF) 2025 World Press Freedom Index, moving up four places from its 2024 position (76th) and from 92nd in 2023, which is a sign of improvement on how the country is perceived globally in terms of press freedom. The report notes "This annual index evaluates nations based on their commitment to free, independent, and safe journalism. It considers several criteria: political context, legal environment, economic pressures, sociocultural influence, and the safety of journalists."[18]

2025 was a year of general elections and as such the online space has been full of campaigns and signs of disinformation practices from various political stakeholders across the country. Victims could suffer invasion of their privacy, damage to their reputation and even emotional harm. This practice has been exacerbated by social media supported by the rise of artificial intelligence tools being used, including altering the truth. Groups of fact-checkers are operating across the country to help create a safe place in the online environment with the objective of helping the general public not to fall into the trap of misinformation and hate speech. "Disinformation is a real danger because it tears apart the social tissue, can create tension within the country", stated Loic, one of the fact-checkers.[19]

As mentioned in the Londa 2024 report, nothing has changed on these fronts; the current law on freedom of communications still has provisions on "fake news", with no clear definition of what "fake" is or what type of content could be considered as disturbing public peace. Similarly, the Penal Code still has provisions on "defamation" as well as "insulting speech against a public authority" which are punishable under the law. Sedition practices (language or behavior that is intended to persuade other people to oppose their government) and their criminalisation in African contexts are linked to defamation.

17. Freedom in the World 2025 (Central African Republic): https://freedomhouse.org/country/central-african-republic/freedom-world/2025 (accessed on December 4, 2025)
18. Top African countries with the best and worst press freedom in 2025: https://africaviewfacts.com/stories/top-african-countries-with-the-best-and-worst-press-freedom-in-2025/ (accessed on December 4, 2025)
19. Zoom sur deux figures de la lutte contre les discours de haine et la désinformation en Centrafrique : https://minusca.unmissions.org/zoom-sur-deux-figures-de-la-lutte-contre-les-discours-de-haine-et-la-d%C3%A9sinformation-en-centrafrique (accessed on december 5, 2025)

Access to information

The Central African Republic has no specific law on access to information, other than the 2020 Law on Freedom of Communication, that obliges the Government to be open and transparent in its processes and to be open to journalists' requests for information. Like we mentioned in 2024, government online platforms (such as websites) are not up to date which should be used to inform the public on governmental activities and ongoing projects as well as their vision for the development of the country. Although the domain "gouv.cf" is available and websites of various government related entities such as Ministries have websites hosted under that domain, most of these read "website under construction" while others have expired domain names.

Since websites are not up to date, some entities use social media platforms such as Facebook where they publish regular updates on their activities. For example the Ministry of Communications' website has content dated as far back as 2018, however more regularly posts on its Facebook page.This is the same for the ARCEP (Regulator of Electronic Communications) making it hard to gain access to specific data and statistics on the evolution of the telecoms sector in the country. The Communication Ministry does however run weekly press briefings[20] touching on burning topics and initiatives that are in line with Principle 29 of the Declaration on Proactive disclosure, especially in Section 3.[21]

20. Ministère de la Communication et médias de la RCA : https://www.facebook.com/reel/1495740901478049 (accessed on December 5, 2025)
21. ACHPR's Declaration, P29(3): "Information required to be proactively disclosed shall be disseminated through all available mediums, including digital technologies. In particular, States shall proactively publish information in accordance with internationally accepted open data principles."

Data Protection and Cybersecurity

The Central African Republic has operating laws in this area: Law No 24-001 on the Protection of personal data that was signed into law by the President on January 25 2024[22] as well as Law No 24-002 on Cybersecurity and the fight against cybercrime that was signed into law by the President on February 21 2024[23]. With the ratification of both these pieces of legislation, the CAR joined the list of African states with similar critical instruments in place.

While the law exists, the National Agency on Cybersecurity (ANCy) is not yet operational in the country which, as per the law, has the mission of "ensuring the security of information systems, handling alerts and regulating the sector, among other things". There is however an Agency, linked to the Presidency of the Republic, called "Cellule Centrafricaine de l'Internet et de la Sécurité (CCIS) that "protects citizens against cyber threats, preserves the stability of digital infrastructure, and defends the nation's image in the face of cyber-attacks and personal data breaches."[24]

Despite the passing of the law on Cybersecurity in 2024, the CAR is still working internally at accelerating its organisational measures (including reinforcing infrastructures, developing human capital through training and capacity building), with support from regional and international institutions in order to align with the African Union's Convention on Cybersecurity and Personal Data Protection, known as the Malabo Convention, which is yet to be ratified by the country.

Despite the enactment of Law No 24-002 on Cybersecurity and the Fight Against Cybercrime in 2024, a highlight of Londa 2024 report[25], the CAR's capacity to address cyberattacks is low and the country is lagging behind on the ITU's 2024 Global Cybersecurity Index (GCI) which focuses its analysis on five criteria, namely the legal framework, technical measures, organization, capacity building, and cooperation. CAR is listed at Tier 5, the lowest level in Africa alongside countries such as Guinea Bissau and Burundi.[26]

22. Loi No 24-001 portant protection des données personnelles : https://arcep.cf/fr/images/documents/reglementation/lois/Loi_24_001_portant_protection_des_donnes_a_caractere_personnel.PDF (accessed on November 14, 2024)
23. Loi No 24-002 sur la cybersécurité et la lutte contre la cybercriminalité : https://arcep.cf/fr/images/documents/reglementation/lois/Loi_24_002_relative_a_la_cyber_securite.pdf (accessed on November 14, 2024)
24. Cellule Centrafricaine de l'Internet et de la Sécurité: https://www.ccis-rca.org/MessageDuGnral (accessed on December 8, 2025)
25. Londa 2024

Privacy and Surveillance

Privacy of communications is protected by law in the Central African Republic. However, there are no readily available reports on instances where the government was actively breaching or interfering in citizens' privacy of communications. Even during the general elections year, there were no reports of opposition leaders being subjected to surveillance, despite their pleas and declared intent to boycott the elections.

Similar to 2024, research shows government requests for content take-down sent to intermediaries did not occur. It is a good sign that the state seems to be fully compliant with this requirement of the Declaration.

Developments in ICT and Emerging Technologies

The Central African Republic has been taking advantage of its connection to optic fiber cables to take on the journey of development of its ICT sector. This is mostly evident through its citizens, including students, developers and other users of digital technologies. Best practices in the world have shown that the role of the government is to set the tone by working, among others, on the legal framework as well as ensuring the necessary investments are made in this sector allowing for users to take advantage of these to support development.

An important initiative is the World Bank support for CAR's Communication Regulator (ARCEP) to strengthen its mission to better control and regulate the electronic communications sector. The core of its mandate is to track

26. Cybersecurite en Afrique : le dernier rapport revele les défis et les progrès : https://www.adiac-congo.com/content/cybersecurite-en-afrique-le-dernier-rapport-revele-les-defis-et-les-progres-161422 (accessed on December 3, 2025)

trends over time, detect anomalies, and better understand the actual state of connectivity across the entire territory. With this support in equipment and capacity building, "the regulator now has the ability to analyse detailed data on mobile network performance in real time, without relying solely on information provided by operators."[27]

The country had no strategy for artificial intelligence (AI) by the time of writing this report. The African Union, when releasing the continental strategy on AI in 2024, set an ambitious goal of "putting AI to work for Africa's development and prosperity" underlying the fact that "AI can stimulate economic growth, create new industries, drive innovation, generate employment opportunities, develop new economic niches for women and young people, support the preservation of Africa's cultural heritage, and help solve some challenges."[28]

The CAR should use this model to align itself to the spirit of this continental framework. On August 22 2025 while CAR president was attending a summit in Japan, the Japanese Prime Minister announced[29] "the launch of a large-scale training program for more than 30,000 Central African experts in artificial intelligence". As of November 2025, citizens were still waiting to hear more on the "practicability of such a program"[30]. When the Communication Minister addressed the press, he did not provide a specific agenda for such an important program.

Another important move was the validation[31] of the National Strategy for scientific research and technology innovation (2025 – 2029) by the scientific and university community in the Central African Republic on June 29, 2025, in Bangui, the capital city. Its vision for 2033 is for Central African research to be firmly rooted in innovation, structured around consistent management, sustainable funding, and enhanced multisectoral coordination.

27. Créer un regulateur telecom moderne et performant en RCA : https://blogs.worldbank.org/fr/africacan/creer-un-regulateur-telecom-moderne-et-performant-en-republique-centrafricaine (accessed on December 3, 2025)
28. Stratégie continentale sur l'intelligence artificielle : https://au.int/sites/default/files/documents/44004-doc-FR_Strategie_Continentale_sur_lIntelligence_Artificielle_3.pdf?ref=fakt-afrique.org (accessed on December 8, 2025)
29. Centrafrique – Japon : Un partenariat stratégique pour former 30.000 experts en intelligence artificielle : https://tribuneechos.com/centrafrique-japon-un-partenariat-strategique-pour-former-30-000-experts-en-intelligence-artificielle/ (accessed on December 3, 2025)
30. Formation en intelligence artificielle au Japon : Quand Touadera vend fu nouveau reve pour son troisième mandat : https://corbeaunews-centrafrique.org/formation-en-intelligence-artificielle-au-japon-quand-touadera-vend-du-reve-pour-son-troisieme-mandat/ (accessed on December 3, 2025)
31. Stratégie nationale de recherche en RCA : vers une gouvernance scientifique rénovée au service du développement durable : https://www.lecames.org/strategie-nationale-de-recherche-en-republique-centrafricaine-2025-2029-vers-une-gouvernance-scientifique-renovee-au-service-du-developpement-durable/

Digital Inclusion

Protecting children online

In the Central African Republic, initiatives to protect children online are part of a broader child protection framework led by UN agencies (such as UNICEF and the ITU) and the government, focusing on awareness-raising, strengthening the legal framework (such as the Child Protection Code adopted in 2020), and assisting victims of violations. Although the initiatives are mainly focused on protection from armed conflicts, efforts are being made to promote digital access for young girls (such as UNFPA's training on digital technologies in October 2024[32]) and the application of ITU global guidelines (such as their Child Online Protection guidelines[33] to create a safe online environment for children).

The Universal Service Fund

The Universal Service Fund (USF) is an initiative of CAR's Electronic Communications Law of 2018, Articles 77 to 81. It is defined as "a minimum set of defined services of specified quality that is accessible to the whole population under affordable tariff conditions throughout the territory" (Article 77). It is established with contributions from each operator at a rate of "2% of the previous year's turnover of each operator" (Article 79).

The 2024 Londa Report stated that nothing was done to operationalise this fund because the Committee to oversee it, as per the 2018 law, was yet to be formed. On July 9 2025, it was reported that the Ministry of Digital Economy and Telecoms launched the activities of the Electronic Communications Development Committee (CDCE) to

32. L'UNFPA s'engage pour l'accès des jeunes filles centrafricaines au numérique : https://car.unfpa.org/fr/news/lunfpa-sengage-pour-lacc%C3%A8s-des-jeunes-filles-centrafricaines-au-num%C3%A9rique (accessed on December 8, 2025)
33. Child Online Protection Guidelines: https://www.itu-cop-guidelines.com/(accessed on December 8, 2025)

operationalise the Fund.[34] The Regulator's Facebook Page announced[35] that experts from nine Ministries were convened including from the Ministries of National Education, Finances and Budget, Plan and Cooperation, Higher Education, Small and Medium Enterprises, Administration of the Territory, Public Health, Digital Economy and Telecommunications, as well as experts from the Governor of Bas-Oubangui and Telecoms Operators.

Although not much has been seen onsite after that meeting, it is a positive move in the effective implementation of the Universal Service Fund (USF) in the country. The Fund is set to be managed under ARCEP that supervises all projects on infrastructure and services deployment.

Rights of persons living with disabilities

As of 2025, persons with disabilities (PWDs) in the Central African Republic remain severely digitally excluded, facing high costs, limited device access, poor infrastructure, and low digital literacy. Despite rising awareness, they are less likely to use mobile internet or assistive tech, worsening inequality due to scarce data and weak regulations.[36] Although citizens in CAR face similar issues, PWDs situation is worse. In CAR, a general absence of regulations, binding technical standards, and inclusive design knowledge among developers limits accessible options.

34. Centrafrique : vers la mise en œuvre du fonds du service universel : https://www.agenceecofin.com/actualites-numerique/1107-130013-centrafrique-vers-la-mise-en-uvre-du-fonds-du-service-universel (accessed on December 3, 2025)
35. ARCEP Centrafrique : https://www.facebook.com/ArcepCentrafrique/posts/pfbid0vuhvjaHcuSLqFjovXvpcK3L-w9hdqBPw6v3rRqBXBAjEVaW15GMR5x25tCpkBxFZel (accessed on December 3, 2025)
36. Digital Transformation and Social Inclusion in Public Services: A Qualitative Analysis of E-Government Adoption for Marginalized Communities in Sustainable Governance: https://www.mdpi.com/2071-1050/17/7/2908 (accessed on February 5, 2026)

Conclusion

The Central African Republic has improved on many fronts since last year's report such as with efforts in operationalising optic fiber for better connectivity as well as efforts in the legislative front with the new Press Freedom Bill that was passed by Parliament. However, the State needs to take urgent action in some other sectors that could support the nation's growth, hence our specific recommendations.

Recommendations

The following recommendations are therefore presented to the various stakeholders for action:

The Government should :

- Leverage the availability of optic fiber and work with telecom operators to provide competitive connectivity offers to customers.
- Work at empowering the Committee set to manage the Universal Service Fund, an important mechanism as per national laws, to support the deployment of technology infrastructures and connectivity to remote areas.
- Consider adopting implementation measures (such as the creation of the National Cybersecurity Agency) and join the Malabo Convention.
- Aim at considering targeted actions for Persons With Disabilities in order to be more inclusive through initiatives such as public-private partnerships with entities specialised in service providing for this category of internet users.

The Regulator should:

- Ensure the interests of end-users prevail against commercial interests of operators when deploying their services.
- Consider updating its public sources of information (such as its website) to allow researchers to access data on the evolution of the telecommunications market as it used to be the practice. The available data is outdated.
- Work with the Government in promoting innovative and attractive measures that will attract investors in support of connectivity growth.

Civil Society Organisations should:

- Play the role of watchdog, ensuring the various government-led or announced projects in the digital area are implemented, especially those directed by available national laws and regulations.
- Consider funding opportunities such as through international donors and partnering with the government to develop digital literacy programs that will increase technology uptake in the country and therefore digital inclusion.
- Increase activities such as those related to digital literacy programs, with a special focus on people living with disabilities who are often left behind.
- Keep pressuring the Government for the review of the Press Freedom Bill before this is signed into law by the President.

Citizens should:

- Be creative and active in leveraging the current developments in the ICT sector (such as the optic fiber) to launch innovation, test entrepreneurship opportunities, etc.

Private sector:

- Telecommunications companies should support the government in its efforts to develop and operationalise the Universal Service Fund to help deploy connectivity to underserved and unserved areas.
- Private entities operating in the technology space should comply with the law and international standards to protect the private communications and personal data of their users.
- Telecommunications operators should leverage on the deployed optic fiber to increase capacity and provide broadband connectivity to citizens by considering tariffs that are affordable for the low-income users.
- Business actors should leverage the availability of the fiber connection to request and use the various licenses to provide digital services to CAR citizens.

The Score Index

Central African Republic, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet outages	P38(2)	5	5	The state has not condoned any network disruptions (such as internet shutdowns)
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	2	2	The State has shown efforts and good practices to ensure the availability of meaningful access to the Internet for marginalized groups (such as the operationalisation of the fiber) but efforts need to be made, especially by making sure there are laws to back government efforts in support for meaningful connectivity.
False News Criminalization	P22 (2)	2	2	On sanctions, the law on Freedom of Communication refers to the Penal Code and speaks of a fine and jail for anyone who is found guilty of having authored or spread fake news and defamation. But there are no reports of this being applied in 2025. The State needs to look at this and stop criminalisation of fake news to be fully compliant.
Sedition Legislation	P22 (2)	3	2	Sedition (or similar actions such as defamation or rebellion) is somewhat mentioned in CAR's legislation. Specifically, authors are sentenced under the Penal Code. Like in 2024, there were no reports of these penalties being applied in 2025. Yet, such provisions in the law should be repealed to ensure they are not hanging as a threat to freedom of expression.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20 (1) & (2)	4	3	The same score remains as 2024 but the new controversial bill, passed in Parliament on freedom of communication could lead to a drop, if the president happens to pass it into a law.
Data Protection Legislation.	P42	3	3	The law has been in place since 2024, but no implementing measures have been recorded in 2025 (such as the appointment of a DPA). The score drops by one point.
States interfere and require the removal of online content by internet intermediaries	P38 and P39 (4)	4	3	As in 2024, data on this indicator is not readily accessible from the government but according to the various transparency reports such as with Meta platforms or Google, CAR has made no such request for the last few years. It is, however, important that the Government be proactive in disclosing compliance with due process to be fully compliant.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Invasion of Privacy of Communications	P41	2	4	The 2018 Electronic Communication law provides for judicial oversight with provisions on how best practices should be enforced. No readily available data presents evidence of acts of invasion on people's communication privacy.
AI and Emerging Technologies national strategies	P39 (6)	1	2	There is no national strategy on AI, but the government announced to train at least 30000 citizens on the use of AI, in partnership with Japan.
Failure by the government to disclose or proactively disclose and disseminate information through digital technologies.	P29 (3)	2	1	There is no law on access to information in CAR, there is no up-to-date data on government-related websites platforms that disclose information, other than the mentioned Facebook page of the Ministry of communication and media for which this score is given as a starting point. But there is a lot that needs to be done for CAR to be fully compliant.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	1	1	There is no improvement on this point from last year, we keep the same score.
Digital Inclusion	P37 (3)	2	2	Positive steps to implement the USF have been seen in 2025. The 2024 fiber has increased connectivity, and young people can now deploy their creativity. A new operator has been mentioned to connect remote regions.
Total (out of 60):	2024: **31**	2025 **30**		



DEMOCRATIC REPUBLIC OF CONGO

By Noël Kabeya

Executive Summary

For several years, the Democratic Republic of Congo has placed its successful transition to a high-tech society at the heart of its government action. This has led to legislative and institutional reforms aimed at filling legal gaps and strengthening the institutional framework to foster the digital economy in all aspects.

This annual report draws on quantitative and qualitative research, document analysis (public policies and legal instruments) and interviews with key players in the Congolese digital ecosystem. These resources enabled the monitoring of digital rights protection and inclusion in the country. This assessment focused on internet access, freedom of expression online, personal data protection, content censorship and moderation, access to information, AI and emerging technologies, digital inclusion and the Universal Service Fund.

This report examines the digital, legal and institutional frameworks through the lens of legislation harmonisation and the establishment of various independent administrative bodies tasked with regulating and managing the digital sector, as stipulated by the Digital Code. It then addressed the implementation of the National Digital Plan, assessing its progress as it reached its 2025 deadline and is now being replaced by a more ambitious one.

From another perspective, the report highlighted some progress in promoting and protecting digital rights in the country. It also identified initiatives undertaken to foster digital inclusion and the proper administration of justice. However, the monitoring revealed certain weaknesses in the framework protecting digital rights. The greatest concerns relate to freedom of expression online, particularly in a context marked by the armed conflict in the east of the country. Based on the research findings, this report concludes that the framework protecting digital rights and inclusion is generally deficient in the Democratic Republic of Congo.

Faced with this deficit, the report makes recommendations to the government, parliament, civil society actors, the media, universities, telecommunications companies, and citizens, with the hope of contributing to better protection of digital rights in the Democratic Republic of Congo.

Introduction

The Democratic Republic of Congo (DRC) is the second-largest country in Africa, with an area of 2,345,000 km^2. Its population is approximately 115,403,027,000 inhabitants, according to estimates by The World Factbook[1]. The country has a relatively low mobile internet penetration rate compared to the continental average.
Following the general elections of December 20 2023, and after the Constitutional Court confirmed his re-election on January 9 2024, with 73.47% of the vote, the incumbent president, Félix Antoine Tshisekedi, was sworn in on January 20 2024, for a second five-year term.

The first government of President Tshisekedi's second term, led for the first time in the country's political history by a woman, Judith Siminwa, was approved by the National Assembly on June 11 2024, based on a programme that included several initiatives aimed at promoting digital rights and inclusion.

Framework for Digital Regulation

The Telecommunications Law and the Digital Code are the two main legal documents that make up the DRC's regulatory framework for digital technologies.

1. Law No. 20/017 of November 25, 2020, which addresses information and communication technologies and telecommunications.

This law is regarded as the most significant framework law governing the nation's ICT and telecoms industries[2]. In contrast to the 2002 framework law, which it repeals, it addresses concerns pertaining to information and communication technology in addition to telecoms. In this regard, it provides the Democratic Republic of the Congo with a more thorough and contemporary approach to regulation[3].

2. The Digital Code

The promulgation of Ordinance-Law No. 23/010 concerning the Digital Code was hailed as a significant step in the development of digital sector regulation in the country. The Digital Code is considered the legal lever for the DRC's digital transformation, as it positions itself as an instrument for the development and diversification of the national economy[4]. In fact, at least in theory, it seeks to advance a rights-based digital transformation. This law aims to close the legal gap and open the door for improved digital rights protection in the nation[5].

However, the many obstacles to the Digital Code's successful implementation should not be overshadowed by its applicability, innovations, and declared commitment to strengthening the framework for defending digital rights and inclusion in the DRC[6]. This is also the case for various implementing measures not yet in effect (taken), as well as for the various institutions and regulatory authorities it establishes. This includes, in particular, the National Digital Council, the Digital Regulatory Authority, the National Electronic Certification Authority, the Data Protection Authority, the National Cybersecurity Agency, and the DRC Digital Portal.

1. Congo, Democratic Republic of the - The World Fact Book
2. Paradigm Initiative, LONDA 2023 REPORT ON DIGITAL RIGHTS AND INCLUSION IN AFRICA SUMMARY Democratic Republic of Congo DRC-Londa-Report-FR.pdf
3. Jordy PANZA and Brozeck KANDOLO, The history of digital technology and its regulatory challenges in the Democratic Republic of Factbook
4. Paradigm Initiative, LONDA 2023 REPORT ON DIGITAL RIGHTS AND INCLUSION IN AFRICA SUMMARY Democratic Republic of Congo DRC-Londa-Report-FR.pdf, Op.cit.
5. The Protection of Digital Rights in Light of the New Digital Code in the DRC (Analysis by Michèle CALENGA TSHASEKELA and Hortense NINDA MUHIMUZI/ICDH) – Deep Congo
6. Paradigm Initiative, Protecting digital rights at the dawn of the new digital code in the Democratic Republic of Congo - Paradigm Initiative

Government commitments to digital rights and inclusion

The Congolese government's biggest commitment in 2025 was the simultaneous launch of the National Digital Plan 2026-2030 and the first National Artificial Intelligence Strategy.

Internet Access

In 2025, the number of mobile subscriptions increased from roughly 56.26 million in 2024 to roughly 60.3 million, or 54.3% of the total population[7]. The digital divide is still substantial even if both the number of subscribers and the penetration rate have been rising substantially in recent years. According to the regulatory authority (ARTPC), the mobile penetration rate is close to 30% while the overall penetration rate rose to 61.8%[8]. However, inequalities in internet availability and usage between urban and rural areas continue to be a defining feature of the DRC.

The Democratic Republic of Congo (DRC) is among the countries targeted by the new Global Coalition for Mobile Phone Affordability. Launched in July by the GSMA (Global System for Mobile Communications Association), this initiative aims to facilitate mobile phone ownership among people in low - and middle-income countries (LMICs), generally located in sub-Saharan Africa and South Asia, in order to promote internet usage.

In Africa, mobile phones are currently the primary, and often the only, means of accessing the Internet, according to

7. With 60.3 million active mobile connections, the DRC is projected to reach a penetration rate of 54.3% by 2025 - LePoint.cd
8. T2-25 Rapport ARPTC 29-OCT-2025.pdf

GSMA. In the DRC, 29.98 million people have mobile internet access compared to 16,000 for fixed internet, representing penetration rates of 31.5% and 0.017%, respectively, according to the Congolese Regulatory Authority for Information and Communication Technologies (ARPTIC). In a country where the Government considers the digital economy an asset for development, promoting mobile access can increase internet usage and generate revenue growth for internet service providers (ISPs).[9]

On March 14 2025, a major project, co-financed by the French Development Agency (AFD) and the World Bank to the tune of US$500 million, to strengthen internet connectivity across the country was launched[10]. This project aims to provide internet access to 30 million Congolese people, thus making the service more financially accessible[11].

The project is yet to be successfully executed in order to fully assess how this project will affect the nation's efforts to safeguard and advance digital rights.

Internet shutdowns

The United Nations reports that when the Rwandan-backed M23 armed movement took control of the cities of Goma and Bukavu in North and South Kivu[12], there were frequent internet outages brought on by both the Kinshasa government and the movement's leaders[13].

On January 25 2025, as the M23 attacked and advanced on Goma, authorities reportedly ordered the Internet to be shut down[14]. According to the #KeepItOn coalition and media outlets, the social media platforms X and TikTok were scheduled to be blocked beginning February 1 2025.

9. [Muriel EDJO, Mobile Internet in the DRC: a global coalition to change the game https://www.agenceecofin.com/internet/1307-120283]
10. DRC – France: Two loan agreements signed to finance digital transformation - Rtnc (accessed February 14, 2026)
11. The French Development Agency (AFD) grants a $500 million loan to modernize digital infrastructure in the DRC - LePoint.cd (accessed February 15, 2026)
12. UN report: Rwanda deploys up to 7,000 troops in support of the M23 in eastern DRC
13. https://paradigmhq.org/communique-de-presse-la-net-rights-coalition-condamne-la-coupure-dinternet-a-goma-en-rdc/?lang=fr; Statement from the Internet Society Chapter of the Democratic Republic of Congo on the Internet shutdown in Goma - ISOCRDC
14. Escalation of the conflict in eastern DRC: censorship, internet shutdowns and attacks against journalists and human rights defenders - Civicus Monitor

On February 3 2025, NetBlocks reported that based on its data, access to the Google Play Store had been restricted, presumably to prevent users from downloading VPN services to circumvent the restrictions on X and TikTok[15].

In January, internet outages caused by the M23 persisted for over six weeks in places under its occupancy,[16] especially the city of Goma and its environs.[17]

According to both international human rights legislation and the Declaration of Principles on Freedom of Expression in Africa,[18] these internet shutdowns violate the right to free speech.[19]

Digitalisation

By decree, the Prime Minister established, in March 2025, the implementation of a computerised and digitised management of judicial procedures for the benefit of commercial courts[20].

The Decree provides for the implementation of an integrated, computerised, and digitised system for managing judicial procedures, covering the entire judicial process from the opening of cases to their archiving.

This system consists of a set of tools and applications enabling the paperless management of judicial files, from opening to closing[21].

15. https://www.isocrdc.org/Declaration-ISOC-RDC-coupure-internet-au-Nord-Kivu.php
16. https://beroyafm.net/goma-la-coupure-dinternet-a-paralyse-les-medias-freine-le-commerce-et-isole-la-population-en-pleine-crise-securitaire/
17. https://rtvh.net/nord-kivu-la-societe-civile-denonce-la-coupure-des-reseaux-de-telecommunications-par-le-m23-a-masisi/
18. African Charter on Human and Peoples' Rights (ACHPR), Declaration of Principles on Freedom of Expression in Africa DECLARATION OF PRINCIPLES ON FREEDOM OF EXPRESSION French 2020.fm
19. Article 19 of The Universal Declaration of Human Rights; Article 19 of the International Covenant on Civil and Political Rights International Covenant on Civil and Political Rights | OHCHR
20. Decree No. 25/12 of March 24, 2025, establishing a computerized and digitized system for managing judicial procedures for the benefit of commercial courts | Leganews Pro
21. Article 2, paragraph 4, Decree No. 25/12 of March 24, 2025, states that the functionalities of this system include: the digitization of the judicial case management process; the computerized and digital communication of procedural documents (court writs, orders, communication of documents and pleadings, notifications, service of process, etc.); the automated and random allocation of cases to judges and/or chambers, based on objective criteria (workload, specialisation, etc.); the use of digital tools for case tracking and the management of hearings and deadlines; secure access for stakeholders to the online interface for information on their cases; the payment of court fees and the online publication of decisions; and the archiving of case files.

This represents a significant step in the modernisation of the Congolese judicial system, introducing computerised and digitised procedure management within commercial courts.

One of the innovations of this decree is the creation of the Permanent Monitoring and Evaluation Unit (CPSE) for the implementation of computerised and digitised judicial procedure management in commercial courts. This is a major advancement, as this Unit, if it functions effectively, will ensure the sustainability of the system. Its role will be crucial in identifying shortcomings and proposing necessary adjustments to the computerised and digitised management of judicial procedures.

Freedom of expression online

In 2025, in a context marked by the intensification of the armed conflict in the eastern part of the country, freedom of expression and opinion, including online freedom, has suffered several violations, both in the part under government control and in the areas occupied by the AFC/M23.

After prohibiting media outlets from broadcasting debates on Congolese army operations without the presence of at least one "expert on the subject"[22] and advising against open-phone broadcasts on military operations, the High Council for Audiovisual and Communication (CSAC), the media regulatory authority, suspended Al Jazeera from broadcasting for 90 days as a precautionary measure due to content deemed "subversive".[23]

Following the same logic, the CSAC recommended that media outlets no longer "broadcast information related to the rebellion in eastern DRC without referring to official "government" sources."[24]

In addition, the CSAC prohibited any media coverage of former President Joseph Kabila or his party for 90 days due to his remarks regarding the unrest in the country's east[25] [26].

Subsequently, the CSAC changed this prohibition into a "general recommendation" for all media organisations, asking them to act professionally by not airing or publishing stories that would undermine the DRC's military[27].

A recommendation like this shows that the Congolese government intends to limit freedom of the press, freedom of expression, and freedom of opinion. It violates both international [28] and regional standards[29][30] on freedom of expression that the DRC has adopted, as well as constitutional safeguards.

Further, in the occupied areas, journalists and activists[31], civil society,[32] and human rights defenders [33] have been subjected to intimidation and threats, including death threats and several other violations of their rights, in the context of the escalating conflict in eastern DRC[34].

According to Reporters Without Borders (RSF), from January 2024 to January 2025, RSF recorded 52 violations of press freedom in North Kivu alone, the most affected province. These included the looting of at least 26 community radio stations, at least 10 of which were directly attacked by the M23. Often, before the armed group arrives, radio stations close their doors, either by force or as a precaution,

22. Press release No. CSAC/002/B/02/2024 of February 23, 2024 Security crisis in eastern DRC: CSAC calls on Congolese media to demonstrate patriotism
23. CSAC Decision of January 13, 2025 Al Jazeera suspended in the DRC for subversive content: the CSAC takes strong action
24. Recommendation from the CSAC Plenary Session of April 4, 2024

25. Joseph Kabila and the PPRD banned from DRC media | Radio Okapi
26. Lewis Mudge, A refusal of media coverage that is damaging to the former president of the DRC | Human Rights Watch
27. Media in the DRC: The ban on covering the activities of Kabila and his party has been converted into a "recommendation" - RFI
28. In the Democratic Republic of Congo, freedom of expression in the digital sphere is governed by several legal texts, including the constitution (Articles 23 and 24). The 2023 press law regulates online content and freedom of expression. Furthermore, the Digital Code reinforces these provisions by adding sanctions against disinformation and sexist remarks online.
29. African Charter on Human and Peoples' Rights (ACHPR), Declaration of Principles on Freedom of Expression in Africa DECLARATION OF PRINCIPLES ON FREEDOM OF EXPRESSION French 2020.fm
30. International human rights instruments ratified by the Democratic Republic of Congo, Official Gazette of the DRC, Special Issue, April 1999
31. DR Congo: Rwanda-backed M23 targets journalists and activists | Human Rights Watch, See also DRC: Alarming repression against journalists and activists - AfrikActus
32. Carole Assignon, critical voices in the crosshairs of the AFC/M23 DRC: Critical voices in the crosshairs of the AFC/M23
33. DRC. Endemic human rights violations attributable to the M23 armed group call for concerted international action - Amnesty International
34. Press freedom in peril: repression intensifies in areas occupied by the M23/AFC – B-one television

and journalists receive threatening messages or calls.

According to figures from the National Union of Congolese Press (UNPC), approximately 90 journalists were forced to flee the region, and some were even pursued by the M23[35].

We can also mention the imposition of a blackout on all information coming from territories under government control and the prohibition on all media outlets from relaying negative comments or statements about the M23 movement.[36]

Digital Identity

The Congolese government has signed an agreement with Tridentity Digital Tech Holdings Ltd for the deployment of the National Digital Identification System. This is a preliminary agreement intended to operationalise the comprehensive digital identification and authentication platform project in the DRC.[37]

The partial implementation of the National Digital Plan "Horizon 2025" and the launch of the National Digital Plan "Horizon 2026-2030"

The National Digital Plan "Horizon 2025" has come to an end with an estimated execution rate of 60%.[38]

While its performance remains unsatisfactory,[39] the National Digital Plan "Horizon 2026-2030" has been launched, with more ambitious objectives than the previous plan.[40] Its stated goal is to improve internet access, modernise public services, and develop local technological talent. Beyond the enthusiasm it has generated, however, implementation is still necessary to assess whether it achieves its objectives[41].

Data protection and privacy

In the DRC, personal data protection is characterised by a disorganised regulatory framework and a deficient institutional framework[42]. To date, the Data Protection Authority stipulated by the Digital Code has not yet been established[43].

Meanwhile, the responsibilities of this authority have been assigned to ARPTIC[44]. A year and a half after this transfer, it is difficult to objectively assess ARPTIC's work in the area of personal data protection.

Furthermore, the ratification by the Democratic Republic of Congo of the African Union (AU) Convention on Cybersecurity and Personal Data Protection (Malabo Convention) on June 27 2025, deserves to be highlighted[45]. Through this ratification, the DRC, like other states participating in this convention, has committed itself to a regulatory approach to securing the digital space and protecting personal data[46].

Regulatory authority

While the Digital Code provides for the creation of several independent administrative authorities responsible for regulating the digital sector, the supervising minister, by decree of the Prime Minister[47], transferred the responsibilities of three of these entities to ARPTIC. These are the Digital Regulatory Authority, the National Electronic Certification Authority, and the Data Protection Authority.

This decision, although temporary, raises some concerns regarding the institutional autonomy of these bodies.

35. Escalation of the conflict in eastern DRC: censorship, internet shutdowns and attacks against journalists and human rights defenders - Civicus Monitor
36. JED, Eastern DRC: War Crimes Committed Against the Press, 2025 Report RAPPORT-JED-2025-en-RDC_V1-1.pdf
37. Trident Digital Tech Holdings Ltd Signs Agreement with DRC Ministry for National Digital Identity System Deployment | Nasdaq
38. Evaluation Report on the Implementation of the National Digital Plan "Horizon 2025" (PNN): Progress and Challenges in Laying the Foundations for a Digital Economy in the Democratic Republic of Congo – ADN
39. See Paradigm Initiative, LONDA DRC 2024 Report, page 5 Londa-24-DRC-FR.pdf
40. DRC DIGITAL NATION 2030: President Tshisekedi announces a new digital plan and mobilizes key players in the sector – ADN
41. The National Digital Plan "Horizon 2026-2030" is based on 4 pillars (Infrastructure and connectivity, Digital platforms and public services, Human capital and digital inclusion, Cybersecurity and digital trust)
42. See Paradigm Initiative, LONDA DRC 2024 Report on page 6 Londa-24-DRC-FR.pdf
43. Data protection laws in the Democratic Republic of Congo - Data Protection Laws of the World (Accessed February 6, 2026)
44. Article 1 of Ministerial Decree No. CAB/MIN/PT&N/AKIM/KL/KBS/051/2024 of August 17, 2024, harmonizing the implementation procedures of Ordinance-Law No. 023/010 of March 13, 2023, establishing the Digital Code, and Law No. 20/017 of November 25, 2020, relating to telecommunications and information and communication technologies in the Democratic Republic of Congo, Official Gazette – Special Issue – September 18, 2024
45. Prosper Ntetika Mbakata, 5 things to know about the DRC's ratification of the African Union Convention on Cybersecurity and Personal Data Protection - CIOMAG (accessed February 15, 2026)
46. Enoch BULONZA, "DRC: the National Assembly ratifies the law order authorizing the ratification of the Malabo Convention", CIOMAG, April 6, 2023, online https://cio-mag.com/rdc-lassemblee-nationale-ratifie lordonnance-loi-autorisant-la-ratification-de-la-convention-de-malabo/ (Accessed February 14, 2026)

On the one hand, one can also question whether ARPTIC has the necessary resources and expertise to fully assume all these responsibilities[48]

Conversely, the question of the institutional independence of the Data Protection Authority (DPA) is particularly pressing. Based on Article 11 of the Malabo Convention, this authority must enjoy effective institutional independence and have its own powers of investigation, control and sanction.[49]

Consequently, transferring the prerogatives of this regulatory authority, known as the Regulatory Authority for Posts, Telecommunications, and Information and Communication Technologies (ARPTIC), raises whether national practices comply with international standards[50]. More specifically, this situation risks impacting the independence and institutional autonomy of this authority.

Therefore, given the risks of ineffectiveness and/or functional paralysis of ARPTIC in its role as the Data Protection Authority, the requirement for regulatory consistency would be reflected in the establishment of regulatory authorities under the conditions stipulated by the Digital Code.

Another noteworthy innovation of the Digital Code is the appropriation of systems and new technologies by the Central Bank of Congo and the High Council of the Judiciary, in accordance with the relevant legislation.

Access to information

A bill aimed at guaranteeing "access to information and transparency in public life" in the Democratic Republic of Congo was tabled in the National Assembly on October 30 2024.[51]

To date, this proposal has not yet been adopted, and the law has not been promulgated. The absence of this law creates a legal vacuum regarding access to information, which is detrimental to the rule of law in the Democratic Republic of Congo.[52]

Artificial Intelligence and Emerging Technologies

The regulatory framework for artificial intelligence (AI) remains relatively underdeveloped[53].

First, with technical support from UNESCO, a national report on artificial intelligence, considered a strategic reference framework for the country, was validated.[54] This report constitutes the first global regulatory framework on the ethics of artificial intelligence[55].

Second, the Ministry of National Education introduced AI into the State Examination marking process to enhance the reliability and efficiency of exam marking[56]. This system is presented as being based on technology that allows for the automatic marking of exams while maintaining a high level of human oversight by experts from the Inspectorate General. However, its relevance and viability have been met with mixed reviews[57].

Digital Inclusion

The implementation of the Universal Service Fund (USF) is not effective in the DRC. Even though it has initiated some partnerships[58] and begun operationalis-

47. Articles 7 and 9 of the Congolese Digital Code 971.03.23-Ordonnance-loi-du-12-mars-2023_Code-du-numerique.pdf
48. Article 1 of Ministerial Decree No. CAB/MIN/PT&N/AKIM/KL/KBS/051/2024 of August 17, 2024, concerning the harmonization of the implementation procedures of the regimes of Ordinance-Law No. 023/010 of March 13, 2023, Official Gazette – Special Issue – September 18, 2024,
49. Article 11 of the African Union (AU) Convention on Cybersecurity and Personal Data Protection African Union Convention on Cyber Security and Personal Data Protection | Union africaine
50. BROZECK KANDOLO, The DRC's ratification of the Malabo Convention: legal progress or a step backward? NEWS-JURITECH LEGAL WATCH - No. 11 - June 28, 2025, online Copy of N°10 I NEWS-JURITECH
51. Bill submitted to the President of the National Assembly by MP Jacques NDJOLI ENSEG'EKELI in his correspondence referenced N°081/AN/RAPP/DEJ/SECAB/ELG/2024 on October 30, 2024
52. Access to information in the DRC: a long-awaited law, a suspended democracy - Collective 24
53. Londa-24-DRC-FR.pdf
54. The DRC validates its national report on artificial intelligence and opts for an inclusive strategy - DRC - LIVE
55. The DRC validates its national report on artificial intelligence
56. DRC: Artificial Intelligence to be used for marking the 2025 State Exam - Stay informed - UNE.CD
57. What are the advantages and disadvantages of using AI to grade the main session of the State Exams? | Radio Okapi;Mobeka Ekabela, Exétat 2025 against the backdrop of AI-assisted grading. What ethical issues need to be considered? | Droit-Numérique.cd NEWS-JURITECH – N°13 – AUGUST 05, 2025
58. The FDSU has entered into a partnership with Airtel aimed at accelerating the deployment of telecom services and reducing the digital divide across the entire Congolese territory (September 25, 2025) A New Era for Digital Inclusion in the DRC: The FDSU-Airtel Strategic Partnership and began discussions for a strategic partnership with Starlink (September 2025) Major strategic partnership: the FDSU - Starlink DRC..

ing its roaming and site acquisition strategy,[59] the Universal Service Development Fund (UDDF), responsible for managing the USF, is still not functioning optimally. In fact, telecom firms failed to make all the legally required contributions in 2025[60]. Neither the Unified Social Development Fund (FDSU)nor the Congolese government has released a report on the precise amount that these businesses have paid.

The fact that the decree forming, organising, and administering the FDSU does not identify the consequences these corporations face for failing to pay their payments makes this lack of transparency even more concerning.

However, the price of the nation's most popular mobile internet bundles (gigabytes) is still thought to be excessive.

Conclusion

The guarantee of digital rights in the DRC is generally deficient, primarily due to regulatory gaps, an incomplete institutional framework, and dysfunctions that weaken the protective framework. It is therefore necessary to harmonise legislation and develop measures to implement the digital code.

Thus, the various regulatory authorities will be established and provided with the necessary resources to complete the reform in the areas of digital identity, electronic certification, data protection, and cybersecurity. Given the widespread lack of awareness and recurring violations, particularly in the context of armed conflict, legal awareness and digital literacy training are strongly encouraged.

59. Pilot phase of roaming and site acquisition in Kongo Centralhas
60. Article 33.2 of Decree No. 22/51 of December 30, 2022, establishing, organising and operating a public institution called the Universal Service Development Fund (FDSU), stipulates that the FDSU's financial resources consist primarily of a 3% levy on the turnover of operators in the telecommunications and information and communication technology sector. Decree No. 22/51 of December 30, 2022, establishing, organising, and governing a public institution called the Universal Service Development Fund, abbreviated as FDSU.

It is also the government's responsibility to promote inclusion by taking the necessary measures to facilitate internet access for people living in rural areas.Furthermore, the ratification of the African Union (AU) Convention on Cybersecurity and the Protection of Personal Data is an indication of the Congolese authorities' commitment to contributing to the emergence of a regional ecosystem that protects digital rights and freedoms.

Recommendations

The Government should:

- Accelerate the implementation of measures to enforce the Digital Code.
- Publish the implementation report of the National Digital Plan "Horizon 2025".
- Promote digital skills training.
- Take measures to protect freedom of expression online.
- Invest in expanding telecommunications infrastructure to improve internet access.

Parliament should:

- Accelerate the adoption and promulgation of the law on access to information.
- Legislate on artificial intelligence.
- Implement laws to protect consumers of telecommunications services, especially citizens living in rural and isolated areas.

The private sector should:

- Telecommunications companies must pay their legal contributions to the FSU, amounting to 3% of their revenue.
- Strengthen partnerships with the public sector to implement innovative initiatives aimed at bridging the digital divide.
- Invest in infrastructure tailored to the needs of disadvantaged communities.
- Participate in digital skills training.

Civil society organisations should:

- Advocate for the adoption and promulgation of the law on access to information
- Advocate for each telecommunications company to make 3% of its revenue available to the FDSU
- Work with the media to raise awareness against hate speech in the digital public sphere, including during armed conflicts
- Investigate violations of digital rights

Civil society organisations should:

- Initiate awareness-raising activities, digital training, and digital capacity building.
- Launch awareness campaigns on tolerance and hate speech in the digital public sphere, including during armed conflicts.
- Respect professional ethics and standards and press laws, and demonstrate professionalism to avoid disseminating misinformation and spreading hate speech in the digital public sphere, including during armed conflicts.

The Score Index

Democratic Republic of Congo, 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 outages	P38(2)	3	1	In 2025, there were internet outages during the capture of the cities of Goma and Bukavu by the AFC/M23, on the sidelines of the armed conflict in eastern DRC.
Existing laws, policies and other measures aimed at promoting universal, equitable, affordable and meaningful access to the Internet	P37	3	3	There are some policies and initiatives to promote universal, equitable, affordable and meaningful access to the Internet, but they are incomplete, deficient, and require several enforcement measures and political will. In 2025, with a view to ensuring connectivity in rural areas, the Universal Service Development Fund (UDDF) continued to operationalise its roaming strategy and site acquisition in the provinces and territories.
Criminalizing fake news	P22(2)	1	1	The Penal Code (Art. 199) and the Digital Code (Art. 360) cover false news and false rumours, including when committed through social networks, computer systems, electronic communication networks, or any form of electronic media.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Sedition legislation	P22(2)	1	1	Confusing and inconsistent legislation. The activists' penal code addresses the detention of persons for sale as slaves (Art. 68), while the military penal code deals with insurrection and rebellion.
Arbitrary arrests and harassment of the media, human rights defenders and citizens	P20(1) & (2)	1	1	Despite the promulgation of the law relating to the protection and responsibility of human rights defenders in the Democratic Republic on June 15 2023, the year 2025 saw several arbitrary arrests and detentions of human rights defenders, journalists, and pro-democracy activists, according to the United Nations and human rights NGOs. This situation is exacerbated by the armed conflict in eastern Congo. Arbitrary arrests have taken place in areas occupied by the M23 and in areas under government authority.
Data protection legislation.	P42	3	3	Protection exists because the digital code contains an entire section of 78 articles dedicated to data protection. However, efforts must be made to ensure the effective application of this legislation.
States intervene and demand the removal of online content by internet intermediaries.	P38 and P39(4)	3	1	Lack of a national digital awareness policy
Invasion of the confidentiality of communication	P41	2	2	Intelligence services and the police violated the confidentiality of communications to justify legal proceedings against journalists, human rights defenders, and political opponents.
The government's failure to proactively disclose and disseminate information on digital technologies.	P29(3)	2	2	There are laws, policies, and government initiatives in place to raise awareness and disseminate information about digital technologies. The Digital Code, the National Digital Plan 2026-2030 (PNN2), and the Digital Strategy 2030, currently being finalised, include provisions dedicated to disseminating information about digital technologies.
National strategies on artificial intelligence and emerging technologies	P39(6)	2	2	Embryonic initiatives and a first national strategy are currently being developed
Adoption of laws, policies and measures specifically for children promoting digital safety and children's online privacy	P37 (5)	3	2	The legislation exists. However, there is a lack of specific measures promoting digital safety and children's online privacy.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Digital inclusion	P37(3)	1	1	The new National Digital Plan 2026 - 2030 aims to reduce the digital divide. For its part, the FDSU has made progress by extending universal service to some rural and peri-urban areas in order to guarantee equitable access to the internet.
Total (out of 60):	2024: **26**		2025 **21**	



Egypt

By Mohamed Farahat

Executive Summary

This report is an evaluation of the state of digital rights in Egypt in 2025 and serves as an update to the Londa Egypt report published in 2024.[1] The year 2025 witnessed five main changes which affect digital rights positively and negatively. In early 2025, the Egyptian government released the second edition of the National Strategy on AI (2025-2030)[2]. In mid of 2025, Egypt was subjected to a Readiness Assessment Methodology (RAM) by UNESCO in collaboration with

1. Mohamed Farahat, Egypt Digital Rights And Inclusion 2024 Report, Londa, Paradigm Initiative, pp.202-217. https://paradigmhq.org/wp-content/uploads/2025/04/Londa-2024-2.pdf
2. .Egypt Artificial Intelligence Strategy ,2025-2023. https://ai.gov.eg/SynchedFiles/en/Resources/AIstrategy%20English%2016-1-2025-1.pdf

the Ministry of Communication and Information Technology, which completed Egypt's AI readiness assessment in accordance with UNESCO's Readiness Assessment Methodology (RAM)[3] and the final report officially has been published.[4] In the reporting year, the National Council for Artificial Intelligence (NCAI) approved and released the Open Data Policy[5]. Late 2025 witnessed one of the most significant overdue steps, which is issuing the executive regulation on the personal data protection law five years after the law was passed in 2020. This step has completed the personal data protection legislation and regulation framework and made the law effective. Finally and adversely, in November 2025 the new criminal procedures law was issued, which gives prosecutors the authority to issue surveillance orders for communications, including social media, for an indefinite period. This new development constitutes a clear abuse of digital rights and promotes closing of the civic space.

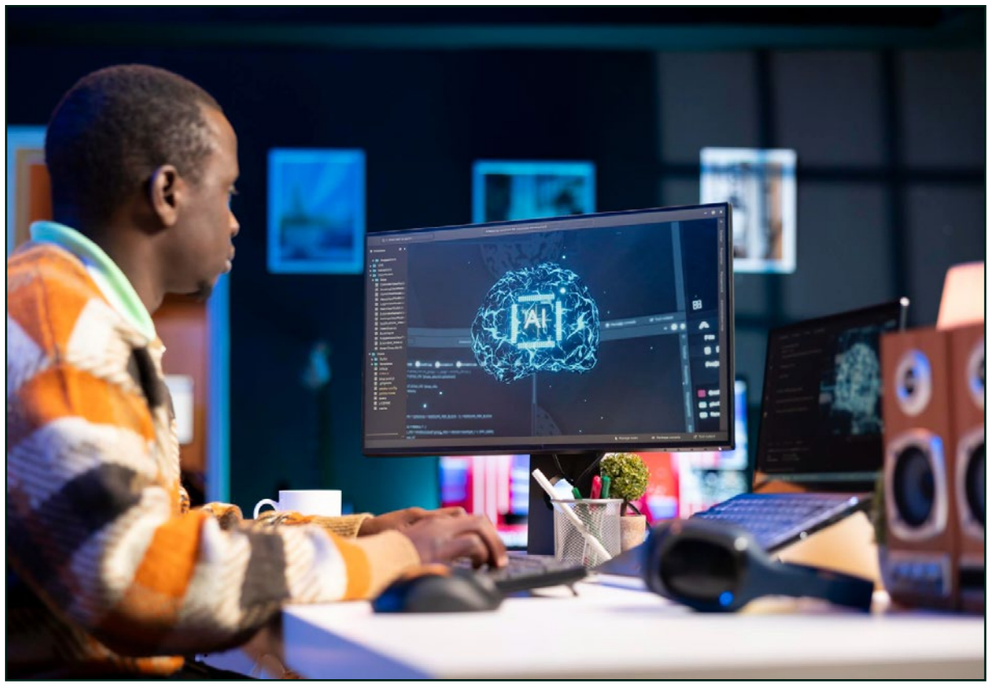
This report reflects the continuous practices that contribute to the narrowing of the digital civic space in Egypt. The Londa report 2025 highlights the use of different legal tools as justification to abuse digital rights and affirms the inefficiency of adopted safeguards. The focal points of this assessment encompass themes such as internet accessibility and interruptions, freedom of expression in online spaces, privacy and surveillance issues, data protection, cybersecurity, the Universal Service Fund, and advancements in Information and Communication Technologies (ICTs), along with emerging technologies.

The report findings highlight that while some of the current legal frameworks safeguard the digital rights of internet users, paradoxically, some provisions enable digital rights abuses and are a means to restrict the digital civic space.

The report employed both analytical and qualitative research methodologies.

3. RAM is is a key tool to support Member States in their implementation of the UNESCO Recommendation on the Ethics of AI
4. Egypt: artificial intelligence readiness assessment report https://unesdoc.unesco.org/ark:/48223/pf0000395173?posInSet=1&queryId=39fff3b8-75bb-433c-a655-aef57bffb73d
5. The National Council for Artificial Intelligence - Egypt. Open Data Policy Arab Republic of Egypt 2025 https://ai.gov.eg/

Secondary data was gathered through an extensive literature review. The proposed recommendations call for the implementation of dedicated legislation governing the creation and utilisation of artificial intelligence (AI) systems, focusing on adopting approaches that prioritise human rights in the digital age. It is also imperative to formulate executive regulations (by laws) to streamline the enforcement of data protection laws. Additionally, introducing access to information law is essential to foster governance that is both transparent and accountable. The report uses Paradigm Initiative's TheScore Index, a digital rights index to evaluate compliance of Egypt with regard to key human rights elements and is inspired by the African Commission on Human and Peoples' Rights' Declaration of Principles on Freedom of Expression and Access to Information.[6]



6. https://achpr.au.int/en/node/902

Introduction

Egypt is a North African country with an estimated population of 119,134,103 by end of November 2025[7] in comparison with 117,406,765 by December 2024[8]. In 2025, 41.91% of the total population lived in urban areas[9] compared with 41% in 2024, while 58.9% of the total population reside in rural areas, in 2025[10]. The country is party to several international human rights treaties that emphasise and guarantee internet freedoms and digital rights, such as the International Covenant on Civil and Political Rights (ICCPR), the African Charter on Human and Peoples' Rights, and the Arab Convention of Anti-Information Technology Crimes (Cybercrimes). Egypt is yet to ratify the 2014 African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention). It is therefore envisaged that Egyptian domestic laws need to be aligned with existing international human rights laws and standards.

Since 2018, Egypt has been enacting legislation that significantly shapes the landscape of digital rights. Laws that govern internet freedoms include the Personal Data Protection Law No. 151 of 2020 and the Law no. 175 of 2018 combating information technology crimes.[11] Egypt also enacted national security and anti-terrorism laws. Recently, Egypt enacted the criminal procedures law no.174 of 2025. These recent legislative frameworks have often been utilised to restrict the civic space. Regrettably, the implementation of these measures has also had adverse consequences on media freedoms.[12]

Moreover, in the aftermath of the COVID-19 pandemic, Egypt continues to grapple with the dissemination of false information in its various manifestations, such as misinformation and disinformation.[13] It is, therefore, evidently imperative to adopt access to information legislation to guarantee the proactive dissemination of credible information to the public by relevant stakeholders and to prevent spreading false information. Generally, there was no significant improvement in the digital rights situation in Egypt in 2024, juxtaposed with the developments observed over the preceding five years. According to Freedom House, Egypt's score for internet freedom was 26 out of 100 in 2019, 27 out of 100 in 2020, and 28 out of 100 in 2023 and 2024.[14] Throughout the five-year period, Egypt was classified as "not free" in the category of internet freedom. The subsequent sections of this report explore the reasons behind the low rate of internet freedoms, examining whether the root cause lies in legislation or its execution.

Internet Access

As reported by the Egyptian Ministry of Communication and Information Technology (MCIT), in the period from July through September 2025, mobile subscriptions stood at 120.85 million - which constitutes 100% of the total population - compared to 111.12 million in the same period in 2024, with a r 8.75 % rate of annual growth.[15] From July through September 2025, the fixed line subscriptions stood at 13.86 million, growing 7.12% from 12.94 million in the same period in 2024.

At the beginning of 2025, there were 96.3 million internet users in Egypt[16], while it was 82.01 million in the beginning of 2024[17]. Internet penetration was 81.9%[18]

7. Worldometers, Egypt ,https://www.worldometers.info/world-population/egypt-population/
8. Worldometers, Egypt , https://www.worldometers.info/world-population/egypt-population/
9. Worldometers, Egypt ,https://www.worldometers.info/world-population/egypt-population/
10. Worldometers, Egypt, https://www.worldometers.info/demographics/egypt-demographics/#urb
11. Mohamed Farahat, (2021). Egypt Digital Rights And Inclusion, LONDA, Paradigm Initiative,. https://paradigmhq.org/wp-content/uploads/2021/05/lr-Egypt-Digital-Rights-Inclusion-2020-Report.pdf, Mohamed Farahat (2021) , Egypt Digital Rights Landscape Report, in T. Roberts (ed.), Digital Rights in Closing Civic Space: Lessons from Ten African Countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.014. AND, Miral Sabry AlAshry, op,cit.,
12. Miral Sabry AlAshry (2022) A critical assessment of the impact of Egyptian laws on information access and dissemination by journalists, Cogent Arts & Humanities. P. 1. DOI: 10.1080/23311983.2022.2115
13. Mohamed Farahat, Coronavirus Trials in Egypt: Blurring the Lines Between Fake News and Freedom of Expression, SMEX.
14. Freedom House, "Freedom On The Net 2024, Egypt", https://freedomhouse.org/country/egypt/freedom-net/2024#B Accessed 20/12/2024.
15. Ministry of Communications and Information TechnologyICT Indicators Bulletin, September 2025 Quarterly Issue, p.2. https://mcit.gov.eg/Upcont/Documents/Publications_4112025000_ICT_Indicators_in_Brief_September_2025.pdf
16. Data Reportal , Egypt 2025, https://datareportal.com/reports/digital-2025-egypt.Accessed 23 February 2026
17. Data Reportal , Egypt 2024, https://datareportal.com/reports/digital-2024-egypt?rq=egypt. Accessed 23 February

in 2025, up from 72.2%[19] in 2024. In 2023, only 72.2% of the population was connected[20]. According to the Speedtest Global Index, the speed of fixed broadband in Egypt in October 2025 was 91.25 Mbps, ranking 73rd globally out of 156 countries[21], while it was 76.67 Mbps, ranking 81st globally out of 154 countries in November 2024[22]. In October 2023, it was 61.22 Mbps, ranking 83rd globally[23]. In terms of mobile speed, it was 44.51 Mbps, ranking 83rd globally out of 104 countries by December 2025[24], while it was 38.29 Mbps, ranking 86th globally out of 110 countries by December 2024[25]. According to Kepios, internet users in Egypt increased by 12 million (+14.6%) between January 2024 and January 2025.[26] In 2024,[27] 99.89% of the population was covered by 3G mobile network, while 99.62% was covered by 4G mobile network.[28] Egypt is one of 14 countries in Africa where 5G networks are being tested and widely deployed.[29] Other African countries, including North African countries, still invest in 4G networks.[30] Egypt has achieved remarkable strides in connectivity and is among the leading countries on the continent in this regard.

In the context of social media users, there were 50.7 million social media users in Egypt in January 2025, or 43.1% of the total population.[31] There were 45.40 million social media users in January 2024, representing 40% of the total population[32]. According to Statcounter, in the period from January 2025 to January 2026, 90.94% of the population was using Facebook[33], compared to 63.96% in November 2024[34]. 2.7941% using Instagram by December 2025, while it was 21.3% in August in the same year.[35], and 18.57% in November 2024[36]. By December 2025, 6.12% were using YouTube[37], down from 9.7% in November 2024[38]. 1.07% used Twitter in 2025[39], down from 4.17% in 2024[40]. It is very clear that there is a significant decrease between 2024 and 2025 in the use of social media, particularly Instagram, Twitter, and YouTube. There were no reported cases of internet shutdowns in 2025, but Freedom House reported that "the Brussels-based independent Egyptian media outlet, Zawia3, was blocked."[41]

Privacy and Surveillance

As mentioned earlier, Egypt is a party to most of the international human rights binding treaties which emphasise and guarantee the rights to privacy and prohibit unlawful surveillance practices.

2026

18. Data Reportal , Egypt 2025,https://datareportal.com/reports/digital-2025-egypt. Accessed 23 February 2026
19. Data Reportal , Egypt 2024, https://datareportal.com/reports/digital-2024-egypt?rq=egypt.Accessed 23 February 2026
20. Data Reportal , Egypt 2023,https://datareportal.com/reports/digital-2023-egypt.Accessed 23 February 2026
21. Speedtest Global Index , https://www.speedtest.net/global-index, October 2025.Accessed October 2025
22. Speedtest Global Index. Egypt's Mobile and Broadband Internet Speeds - Speedtest Global Index.Accessed October 2025
23. Speedtest Global Index. https://www.speedtest.net/global-index/egypt#mobile.Accessed October 2025
24. Speedtest Global Index, https://www.speedtest.net/global-index/egypt#mobile.Accessed October 2025
25. Speedtest Global Index. Egypt's Mobile and Broadband Internet Speeds - Speedtest Global Index.Accessed October 2025
26. Data Reportal , Egypt 2025, https://datareportal.com/reports/digital-2025-egypt.Accessed 23 February 2026
27. Figures of 2023 were not available during the time of writing this report.
28. Stasista, Digital & Connectivity Indicators – Egypt. https://www.statista.com/outlook/co/digital-connectivity-indicators/egypt#:~:text=The%204G%20network%20coverage%20in,to%20amount%2099.89%25%20in%202024.
29. Diplo Foundation , Status of internet access and connectivity in Africa. URL: https://www.diplomacy.edu/wp-content/uploads/2023/01/African-digital-foreign-policy_En.pdf. P,56 and 57.
30. Diplo Foundation , Status of internet access and connectivity in Africa, https://www.diplomacy.edu/wp-content/uploads/2023/01/African-digital-foreign-policy_En.pdf
31. Data Reportal , Egypt 20254, https://datareportal.com/reports/digital-2025-egypt.Accessed 23 February 2026
32. Data portal https://datareportal.com/reports/digital-2024-egypt?rq=egypt.Accessed 23 February 2026
33. StateCounter, Global State, Social Media Stats Egypt ,Jan 2025 - Jan 2026, https://gs.statcounter.com/social-media-stats/all/egypt. Accessed 23 February 2026.
34. StateCounter, Global State, Social Media Stats Egypt , Nov 2023 - Nov 2024 https://gs.statcounter.com/social-media-stats/all/egypt.Accessed 23 February 2026
35. StateCounter, Global State, Social Media Stats Egypt ,Jan 2025 - Jan 2026, https://gs.statcounter.com/social-media-stats/all/egypt. Accessed 23 February 2026
36. StateCounter, Global State, Social Media Stats Egypt , Nov 2023 - Nov 2024 https://gs.statcounter.com/social-media-stats/all/egypt.Accessed 23 February 2026
37. StateCounter, Global State, Social Media Stats Egypt ,Jan 2025 - Jan 2026Jan 2025 - Jan 2026, https://gs.statcounter.com/social-media-stats/all/egypt. Accessed 23 February 2026
38. StateCounter, Global State, Social Media Stats Egypt , Nov 2023 - Nov 2024 https://gs.statcounter.com/social-media-stats/all/egypt
39. StateCounter, Global State, Social Media Stats Egypt ,Jan 2025 - Jan 2026Jan 2025 - Jan 2026, https://gs.statcounter.com/social-media-stats/all/egypt. Accessed 23 February 2026
40. StateCounter, Global State, Social Media Stats Egypt , Nov 2023 - Nov 2024 https://gs.statcounter.com/social-media-stats/all/egypt.Accessed 23 February 2026
41. Freedom House,FFreedom on the Net 2025, Egypt. URL:https://freedomhouse.org/country/egypt/free-

Principle 40 of the African Commission on Human and Peoples' Rights' (ACHPR) 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa (the Declaration) states that "Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information and everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies". [42]
On October 25 2025, Egypt was one of North African States that signed the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes[43] (United Nations Convention against Cybercrime). Only four North African States out of seven states signed the convention: Algeria, Morocco, Libya, and Egypt. It is worth mentioning that only 21 African countries out of 54 signed the convention. [44]

Article 57 of the Constitution provides the protection to the right to privacy and this provision aligns with Principle 40 of the ACHPR 2019 Declaration and other international human rights treaties and standards. Article 57 states that "the right to privacy may not be violated, shall be protected and may not be infringed upon. Postal, telegraphic, and electronic correspondence, telephone conversations, and other means of communication are inviolable, their confidentiality is guaranteed, and they may not be confiscated, viewed, or monitored except by a reasoned judicial order for a specific period and in the circumstances specified by law."[45] The State is also committed to protecting citizens' right to use public means of communication in all its forms. It is not permissible to disrupt, stop, or deprive citizens of these rights arbitrarily. While this is regulated by law, other laws have provisions that undermine the right to privacy, as expounded later in this report.
In terms of promoting children's digital safety and privacy online, Egypt adopted different laws seeking to protect children in general including in digital sphere such as children law no 12 of year 1996, Penal Code, cybercrimes law, data protection law, and law no 64 of year 2010 focused on combatting trafficking in persons.

In addition, Article 99 of the Constitution establishes the right to remedies and compensation for damage resulting from abuse of privacy: "any violation of personal freedom, or the sanctity of the private life of citizens, or any other public rights and freedoms which are guaranteed by the Constitution and the Law is a crime. The criminal and civil lawsuit arising from such crime shall not abate by prescription. The affected party shall have the right to bring a direct criminal action."[46] The right to remedy and compensation are guaranteed by the Constitution and also guaranteed under Article 163 of civil law. In particular, there are many compensation claims submitted to Egyptian courts for breach of privacy with final judgement in favour of affected persons.
Article 25 of Law No. 175 of 2018 on Combating Information Technology Crimes criminalises the breach of the family's principles and values of Egyptian society and the violation of the inviolability of private life. It is punished by imprisonment for a period of not less than six months and a fine of not less than EGP50,000 (US$1,600) and not exceeding EGP100,000 (US$3,200).

The same Article includes some actions that constitute a breach of privacy, such as sending a large number of messages electronically to a specific person without their consent, granting data to a system or website to promote goods or services without their consent, or publishing, via the information network or by any means of information technology, information, news, pictures, and the like, that violate the privacy of any person without his consent, whether the published information is correct or incorrect. Article 26 of the same law added that "anyone who intentionally uses an information

dom-net/2025#A , Accessed 23/2/206.

42. African Commission on Human and Peoples' Rights ,the Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019.
43. United Nations , Treaty collection.https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=X-VIII-16&chapter=18&clang=_en
44. United Nations , Treaty collection.https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=X-VIII-16&chapter=18&clang=_en
45. Egypt , Constitution 2014 article 57

program or information technology to process personal data of others in order to link it to content that is contrary to public morals or to display it in a way that would infringe on his character or honour." In the same context, Article 20 of Law No. 180 of 2018 regarding Regulating the Press, Media, and the Supreme Council for Media Regulation stipulated that "it is prohibited in any means of publication or broadcast to breach the private lives of citizens".

In terms of surveillance practices in Egypt[47] according to Principle 41 of the ACHPR 2019 Declaration, states shall rely on it if it is "authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim".[48] In the Egyptian context, community standards and ensuring national security are always used as justification for undertaking surveillance.[49] Under the regime of Hosni Mubarak, surveillance practices were primarily focused on monitoring terrorist activities. However, the dynamics have transformed significantly in the aftermath of the 2011 revolution and subsequent political events, emanating from the pivotal role that social media played. Surveillance measures have expanded beyond tracking terrorist activities. Rigorous steps were implemented to regulate internet access and scrutinise online content. Legislation is used to ban websites, obtain personal data, abuse citizens' right to privacy, and criminalise the right to freedom of expression through allegations of disseminating false news.[50]

As already stated, Article 57 of the Constitution prohibits surveillance except when authorised by a judicial order, strictly for a defined duration, and in cases specified by the law. Article 71 of the Constitution stipulates that "it is prohibited to censor, confiscate, suspend or shut down Egyptian newspapers

46. Constitution article 99
47. For detailed information about surveillance practices and related framework refer to Mohamed Farahat (2021), Egypt country report, in Surveillance Law in Africa: a Review of Six Countries, Brighton: Institute of Development Studies, pp.48-70. DOI: 10.19088/IDS.2021.059
48. African Commission on Human and Peoples' Rights, The Declaration of Principles of Freedom of Expression and Access to Information in Africa 2019.
49. OpenNet Initiative (September 2004). A Starting Point: Legal Implications Of Internet Filtering.
50. Mohamed Farahat (2021), Egypt country report, in Surveillance Law in Africa: a Review of Six Countries, Brighton: Institute of Development Studies, p.48. DOI: 10.19088/IDS.2021.059 p.48.
51. Constitution article 71
52. The Chapters from I to IV in Book Two of the Penal Code of Egypt address offences directed against persons and nature, beginning with crimes of Homicide, Wounding, and Battery/Assault (Chapter I), followed by Intentional Arson (Chapter II). This is succeeded by offenses such as Causing Abortion (or Inducing Miscarriage) and Manufacturing Substances Injurious to Health (Chapter III), and finally, Indecent Assault and Corruption of Morals

and media in any way. In exceptional circumstances, they may be subject to limited censorship in times of war or general mobilisation".[51] However, the same laws contain specific provisions that grant powers to the authorities to block websites that are deemed a threat to national security.

November 2025 witnessed the emergence of a new criminal procedures law no 174 of 2025 as a new legal tool to close the civic space in Egypt and promote surveillance practices. The law gives prosecutors the authority to issue surveillance orders for communication services, including social media, for an indefinite period. The law will enter into force on October 1 2026, in accordance with Article (Sixth) of promulgating provisions of the law. This new development constitutes a clear abuse of digital rights and promotes closure of the civic space.

Article 80 of the above-mentioned law clearly states the following: "A member of the Public Prosecution (Prosecutor) - after permission from the judge - has the power to order the interception of wired and wireless communications, social media accounts and applications (including their various non-public content), electronic mail (email), text, audio, or video messages on phones, devices, or any other technological means, and to seize the containing media/devices; or make recordings of conversations that took place in a private location, whenever such action is deemed beneficial for the discovery of the truth in a felony or a misdemeanor punishable by imprisonment for a period exceeding three months. The order must be for a period not exceeding 30 days. The order may renew it for one or more similar periods". The new law reinforces surveillance for an indefinite period even in cases of not serious crimes.

Article 117 of the same law added that "Chief Prosecutor (Ra'ees Niyaba) or higher, shall have the authority, in the investigation of felonies stipulated in Chapters I, II, II bis, III, and IV of Book Two of the Penal Code[52], in addition to the powers prescribed for the Public

Prosecution, to issue a reasoned order for a period not exceeding 30 days, to:

Intercept and monitor wired and wireless communications, social media accounts and their various non-public content, electronic mail (email), text, audio, or video messages on phones, devices, or any other technological means;

1. Seize the containing media/devices;
2. Or make recordings of conversations that took place in a private location, whenever such action is beneficial for the discovery of the truth

The order referred to in the first paragraph of this Article may be renewed for one or more similar periods".

Article 80 and 117 of new criminal procedures law no 174 of 2025 legally establishes a provision for surveillance for an indefinite period of time, not only for published content but also for private conversation, without clear safeguards to avoid abuse of privacy rights.

Article 1 of the Cybercrimes Law No. 175 of 2018 defines national security as everything related to the independence, stability, and security of the homeland and anything linked to affairs of the Presidency, the Ministry of Defense and General Intelligence. The term 'national security' is vague and shrouded in ambiguity. The lack of clarity in defining national security bestows unfettered discretionary powers upon the authorities, allowing them to decide which actions may pose a threat to national security. Although the Constitution prohibits surveillance practices without a judicial order, the different laws provide the legal basis for surveillance, such as Telecommunications Regulation Law No. 10 of 2003, Personal Data Protection Law No. 151 of 2020, Anti-Terrorism Law No. 94 of 2015, Anti-Cyber and Information Technology Crimes no. 175 of 2018, and Emergency Law no. 162 of 1958.[53] On the basis of the information already provided, it can be asserted that the existing laws exhibit a partial alignment with international human rights standards at a superficial level. However, the same laws contain provisions that undermine digital rights.

(Chapter IV). These Chapters pertain to direct aggressions/offences against individuals and their public and private property.

53. Mohamed Farahat (2021), Egypt country report, in Surveillance Law in Africa: a Review of Six Countries, Brighton: Institute of Development Studies, pp.53-56. DOI: 10.19088/IDS.2021.059 And , Mohamed Farahat ,Mohamed Farahat, Egypt Digital Rights and Inclusion 2020 report, LONDA, Paradigm Initiative https://paradigmhq.org/wp-content/uploads/2021/05/lr-Egypt-Digital-Rights-Inclusion-2020-Report.pdf

Irrespective of the Egyptian legal framework, which to some extent protects the right to privacy, the actual practice witnessed served as abuse to this fundamental right, and demonstrates that the existing legal framework was used to justify the digital surveillance. For instance, according to Thomson Reuters Foundation, 6,000 surveillance cameras were deployed in the new administrative capital[54]. According to People in Need, "Digital censorship was evident, in the period between May 2023 and May 1 2024, there were five instances where digital platforms were blocked, further restricting access to information and limiting journalistic freedom.[55]" In the same context, and according to Freedom House, "Egyptian governments use Sandvine devices to block websites and monitor, prevent, or tamper with connections"[56]. The flagship product of Sandvine "is deep packet inspection (DPI) which is a common tool used by ISPs and telecom companies to monitor traffic and prioritize certain types of content, however it is also used to divert traffic away from sites or social media platforms and into dead ends, effectively censoring them.[57]" According to WIRED, "In February 2024, the US Department of Commerce added Sandvine to its Entity List, effectively blacklisting it from doing business with American partners due to the fact that the company's technology was used in mass web monitoring and censorship in Egypt contrary to the national security and foreign policy interests of the United States.[58]"

Online Freedom of Expression

The ACHPR 2019 Declaration stresses the importance of both rights and states that "[t]he respect, protection and

54. Thomson Reuters Foundation, CCTV cameras will watch over Egyptians in new high-tech capital,4 January 2023.
55. People in Need, Report: Violations of journalist and media rights in Egypt (May 2023 - May 2024), Published: Sep 20, 2024. https://www.peopleinneed.net/report-violations-of-journalist-and-media-rights-in-egypt-may-2023-may-2024-11862gp
56. Freedom House, Key Developments, June 1, 2023 - May 31, 2024. https://freedomhouse.org/country/egypt/free-domnet/2024#footnoteref15_SkY8W4xsgQfWO6slCXHW5-YXwAktvCYGYMgBYfXwANI_nhebWdJe4puP
57. WIRED, Dictators Used Sandvine Tech to Censor the Internet. The US Finally Did Something About It, Feb,2024. https://www.wired.com/story/sandvine-us-sanctions-egypt-internet-censorship/

fulfilment of these rights is crucial and indispensable for the free development of the human person, the creation and nurturing of democratic societies and for enabling the exercise of other rights". This segment of the report underscores the correlation between freedom of expression and the right to access information. When both rights are guaranteed without undue restrictions, it contributes to combating the spreading of false news while promoting freedom of expression, including the right to engage in constructive criticism of government policies.

Despite the surveillance practices outlined earlier, it is essential to underscore the constitutional assurance of freedom of expression. Article 65 guarantees freedom of thought and opinion and all individuals have the right to express their opinions through various means of expression and publication, including digital platforms. However, Article 102 (Bis) of the Penal Code criminalises broadcasting false news, statements, or rumours, particularly if such actions are considered to potentially disturb public security, spread terror among people, or jeopardise public interest. While the legitimacy of criminalising the publication of false news is acknowledged, the existing legal framework does not define the parameters of what constitutes harm to public security and interest. Moreover, article 19 of Law No. 180 of 2018, regulating the Press, Media, and the Supreme Council for Media Regulation, prohibits the publication of false news, incitements of violations of the law, promotion of violence or hatred, and discrimination between citizens. It also forbids publication of content that endorses racism or includes an abuse of the honour of individuals, cursing or slandering them, or insulting religions. Article 4 of this law also restricts the publication of content that contradicts the Constitution. In this regard, it explicitly prohibits the promotion of activities that encourage legal violations, contravene the professional code of honour, disrupt public order, or undermine public morals. The Article also prohibits the propagation of content that fosters discrimination, violence, racism, or hatred. Evidently, the aforementioned provision exhibits legal deficiencies characterised by the utilisation of ambiguous terms like "public order" and "public morality." It also fails to specify actions deemed as detrimental to the honour of individuals. The lack of precision raises concerns regarding the clarity and enforceability of the provision, warranting a careful reassessment to enhance its legal robustness and effectiveness. Also, the absence of a well-defined legal framework that distinguishes between misinformation and the lawful dissemination and unrestricted flow of information poses a significant challenge to the preservation of freedom of expression that is constitutionally guaranteed. The country's 2021 National Human Rights strategy that was developed by the government acknowledges "the lack of a legal framework regulating access to and circulation of official information, data, and statistics, albeit being a constitutional right".[60]

Egypt is yet to enact an access to information law, a situation which is contrary to the aspiration enshrined under Principle 26 of the ACHPR 2019 Declaration. Therefore, dissemination of information that deviates from official government publications is consistently deemed a violation, constituting the offence of disseminating false information.

New Open Data Policy

In October 2025, the National Council for Artificial Intelligence (AI) released the first "Open data policy[61]" in the country. According to this policy, open data refers to the data maintained by the government and its goal is to establish the general framework for data openness in public institutions by defining the principles, guidelines, and responsibilities that ensure the consistent, secure, and effective sharing, management, and reuse of data, prior to the issuance of the Data Governance Law, its implementing regulations, and the accompanying data classification framework. This step may open the door to adopt access to information law. One of the important principles adopted by the policy is "availability, affordability, and ease of use." According to the policy, data should be available and easily accessible to the average citizen, regardless of their technical skills or geographical location; and data should be discoverable and machine-readable. In addition to that,

58. WIRED, Dictators Used Sandvine Tech to Censor the Internet. The US Finally Did Something About It, Feb,2024. https://www.wired.com/story/sandvine-us-sanctions-egypt-internet-censorship/

59. African Commission on Human and Peoples' Rights, The Declaration of Principles of Freedom of Expression and Access to Information in Africa 2019 Principle 1

60. Egypt, SupremeStanding Committee for Human Rights, National Human Rights Strategy (2021) p31 https://sschr.

the policy establishes an "Interim Joint Committee for Data Accessibility" as a central body responsible for data governance ensuring the protection of data by reviewing it and coordinating the disclosure process across ministries and public entities.

2025 witnessed several actions taken based on the above-mentioned laws which target content creators and 'Online Opinion Expressers' (OOE). For instance, "On Tuesday, July 22 2025, Al-Azhar's official Facebook page published a statement by Sheikh Ahmed Al-Tayeb, the Grand Imam of Al-Azhar, strongly condemning Israeli attacks on the Gaza Strip and calling for urgent action to save residents of the Strip from starvation. The statement was mysteriously deleted minutes later. Multiple sources confirmed the deletion came under political pressure from powerful state agencies[62]".

Data Protection

The Data Protection Law (DPL) No 151 of 2020 was enacted in 2020. In November 2025, the Minister of Communication and Information Technology issued the law's executive regulation[63], five years after the law was adopted, to complete the personal data protection legal and regulation framework in compliance with the provisions outlined in the legislation. The executive regulations of this law specify the policies, procedures, controls and standards for collecting, processing, preserving and securing this data. Data minimisation regulation in the law ensures that organisations collect, process, and retain only the personal data that is strictly necessary for the purpose for which it was collected. This provision is aligned with Article 22 of the African Union, African Convention on Cybersecurity and Personal Data Protection 2014 (Malabo Convention), which permits the retention of personal data until the fulfilment of the intended purpose for which the data were originally collected and processed.[64] However, Article 2 of the Cybercrimes Law No 175 of 2018 grants permission to service providers to retain and store user data for 180 days. This provision for data retention contradicts the Data Protection Law. The Cybercrime Law does not include a provision that justifies personal data retention for that timeframe. The law should be amended to enhance transparency and incorporate a clear justification for data retention.

The Data Protection Law has provisions that regulate the processing of sensitive personal data. Article 12 prohibits the collection, transfer, storage, retention, processing, or disclosure of sensitive personal data except with authorisation from the "personal data protection centre".[65] Except in cases authorised by law, written and explicit consent is required from the person concerned. Additionally, when processing children's personal data, the consent of the guardian must be secured. Participation of a child in activities such as games, competitions, or any other engagements should not be contingent upon the provision of personal data beyond what is strictly essential for their involvement. Article 1 of the law defines sensitive data as data that discloses psychological, mental, physical or genetic health, biometric data, financial data, religious beliefs, political opinions, or security status. In all cases, children's data is considered sensitive personal data. Article 41 of the law states that "Any holder, controller, or processor who collects, makes available, circulates, processes, discloses, stores, transmits or saves sensitive personal data shall be punished by imprisonment for a period of not less than three months and a fine of not less than EGP500,000 (approximately US$10) and not exceeding EGP five million (approximately US$100000), or by one of these two penalties, without the consent of the data subject or in cases other than those legally authorised".

In February 2025, the Economic Court of Alexandria ordered Orange Egypt to pay EGP 10 million in compensation to a woman whose personal data had been unlawfully compromised. The judgment arose after the company replaced the claimant's SIM card without her consent, which led the court to award compensation for both material and moral damages[66]

gov.eg/media/gapb5bq4/national-human-rights-strategy.pdf

61. The National Council for Artificial Intelligence, Open Data Policy- Arab Republic of Egypt https://ai.gov.eg/
62. Law and Democracy Support Foundation e.V.,Egypt: Escalating Hostility Toward Freedom of Expression Now Targets Regime Insiders,July 23, 2025.URL: https://ldsf.info/blog/2025/07/23/23-07-25-1/
63. Minister of CIT, Ministerial decree No.816 of 2025 on 1 November, 2025. Al Wqaa El Masrya issue 244 Bis (A).
64. African Union, African convention on Cybersecurity and personal data protection 2014.
65. According to article 1 of personal data protection law No 151 of 2020, centre refers to the personal data protection centre.
66. Shehta and Partners, Legal Alert: Egyptian Court Judgment Tightens Enforcement of Privacy and Data Protection

Universal Service Fund (USF)

According to GSMA Intelligence,[67] a Universal Service Fund (USF) is based on three principles: availability, affordability, and accessibility.[68] Egypt allocated a specific fund for accessing universal services, regulated by the Telecom Regulation Law no.10 of 200. Article 2 of that law stipulates that Telecommunication Services shall comply with the following rules:

1. Publicity of information;
2. Protection of free competition;
3. Provision of Universal Service; and
4. Protection of Users' rights.

Article 9 stipulates that the National Telecommunications Regulatory Authority (NTRA) is entitled to maintain an autonomous budget, adhering to the guidelines outlined in its internal regulations and in conformity with the Unified Accounting System. This autonomy extends without any restrictions imposed by governmental rules or regulations. In 2005, the National Telecom Regulatory Authority (NTRA) established the USF.[69] The USF strives to provide essential telecommunication services to every citizen at reasonable rates.[70] There is no publicly available official record about the value of the USF in Egypt. According to some media reports, the USF started with an initial budget of EGP50 million, approximately US$1 million.[71] Moreover, the National Telecommunications Regulatory Authority (NTRA) has proposed and financed projects to establish, operate, and provide mobile phone services to 54 urban areas and 22 strategic roads throughout the Republic, with a total length of 3,100 km, and a total cost of EGP1,668,000,000 (US$ 54 million).[72] Furthermore, the National Telecommunications Regulatory Authority (NTRA) has initiated measures to enhance the efficacy of fundamental communication services within the Sinai Peninsula. The initiative involves the funding, construction, and operation of mobile phone stations across 30 urban areas and along four critical roads with a total distance of 112 kilometres. This initiative will reportedly cost EGP513 million (US$16,000,000), reflecting NTRA's commitment to advancing connectivity and infrastructure.[73]

Available media reports indicate that in a meeting held in January 2023, with the Parliamentary committee responsible for telecommunication and information technology, the Chairperson of NTRA said that "[t]he Universal Service Fund bears three billion Egyptian pounds to provide telecommunications services in deprived areas and new roads at a cost of 1.8 billion Egyptian pounds, in addition to 1.2 billion to establish 592 stations in the first phase for a decent life Project (مشروع حياة كريمة/ Decent life).[74] The aforementioned initiatives and allocated funds, aimed at addressing telecommunication and connectivity challenges, illustrate that the USF in Egypt is used to narrow the digital divide between urban and rural areas. Concurrently, these initiatives are focused on enhancing the affordability, accessibility, universality and availability of internet and telecommunication services. This is what is envisaged under Principle 41 of the ACHPR 2019 Declaration which requires States, in collaboration with other stakeholders, to adopt measures to ensure universal, equitable, affordable, and meaningful access to the internet without discrimination. [75]

USF initiatives include upgrading existing road infrastructure linked to providing telecommunication services[76]; the El Million Fadan Project which aims

Laws, URL:https://shehatalaw.com/law-update/legal-alert-egyptian-court-judgment-tightens-enforcement-of-privacy-and-data-protection-laws/ Accessed in 24/3/2026.

67. GSMA Intelligence is the global home of mobile market information, driven by our team of expert analysts and is the definitive source of mobile industry insights, forecasts, and research, used around the world.https://www.gsmaintelligence.com.
68. GSMA, (2023). Universal service funds in Africa Policy reforms to enhance effectiveness, p.14. https://www.gsma.com/subsaharanafrica/wp-content/uploads/2023/10/USF-Africa.pdf.
69. National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.3. https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf
70. National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.8. https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf
71. https://muhtwaplus.com/49705/2020/07/25/ما-هو-صندوق-الاتصالات-المصري-لمدخل-ا/
72. El Youm El Sabaa, accessed 13 /2/2024. https://www.youm7.com/story/2021/12/8/وزير-الاتصالات-يعرض-مشروع-مد-شبكات-المحمول-لـ-54-منطقة-نائية-بتكلفة-1-668-مليون-جنيه/5571579
73. El Youm El Sabaa, accessed 13 /2/2024. https://www.youm7.com/story/2021/12/8/وزير-الاتصالات-يعرض-مشروع-مد-شبكات-المحمول-لـ-54-منطقة-نائية-بتكلفة-1-668-مليون-جنيه/5571579
74. Sada El-Balad news , https://www.elbalad.news/5594448
75. ACHPR 2019 Declaration principle 41

to expand the agricultural sector by improving mobile coverage[77] and other national telecommunications and information plan projects such as public educational institutions and libraries, funding for Health Care Centers, services provided to the disabled, infrastructure of digital society and digital architecture, and a broadband project to increase the deployment of high-speed internet in Egypt to create jobs.[78] While acknowledging that the USF regulations focus on digital transformation to a considerable extent, it is imperative to propose recommendations to amend the existing framework so that it explicitly provides for regulating funds for digital literacy and awareness. The abovementioned initiatives contribute to filling the digital gap in Egypt, promoting economic development, and ensuring connectivity in urban and rural areas. As ICT is one of the core services of the government, it is always keen to allocate financial sources to improve.

Developments in ICT and Emerging Technologies

In 2025, Egypt ranked 51st globally in the Government AI Readiness Index, which places it as the first in Africa and North Africa sub-region, and third in the MENA region after Kingdom of Saudi of Arabia and United Arab of Emirates, and before Qatar[79]. Its rank was 65th globally in 2024[80], which means Egypt moved up fourteen places between 2024 and 2025. The country was ranked seventh in the MENA region in the same year and moved up four positions in 2025. This reflects the progress Egypt has achieved in the context of AI integration.

In November 2019, the Egyptian Cabinet approved the establishment of the National Council for Artificial Intelligence (NCAI).[81] At its inception, the primary task of the NCAI was the adoption of a National AI Strategy (NAIS). Subsequently, in July 2021, the NCAI adopted the Egypt AI strategy.[82] At the point of adoption, it was envisaged that the strategy would be implemented in a phased approach until the end of 2022. In 2024, the strategy's execution remained in its initial stage, primarily attributable to the postponed launch. The goal of the initial phase is "to prove the value of AI in the different domains and build the foundations upon which to build AI at scale".[83] Although the Egyptian government adopted the national AI strategy[84] and established the NCAI, binding legislation on AI is yet to be enacted.

Regarding the influence of AI on privacy, Egypt enacted the previously stated cybercrimes and data protection laws in 2018 and 2022 respectively, providing a framework that could be utilised, to some degree, for AI regulation, particularly in terms of privacy, combating arbitrary actions, unlawful surveillance and personal data protection. However, both laws are inadequate to completely regulate AI in Egypt as both laws tackle human acts and do not touch on actions committed by AI systems.

In 2023, the NCAI adopted the Egyptian Charter for Responsible AI (the Charter).[85] The main aim of the Charter is to ensure the ethical use, deployment and management of AI systems in Egypt.[86] The Charter also incorporates overarching principles such as fairness, transparency, a focus on human-centeredness, accountability, and the assurance of security and safety[87]. In addition, the strategy acknowledges that "the existence of policies, regulations, and legislation to mitigate potential

76. National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.17. https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf
77. National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.17. https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf.
78. National Telecom Regulatory Authority (NTRA), Universal Service Policy, pp.17-19.. https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf, pp. 17-19.
79. Oxford Insights, Government AI Readiness Index,2025.p.61.
80. Oxford Insights, Government AI Readiness 2024, https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Foxfordinsights.com%2Fwp-content%2Fuploads%2F2024%2F12%2F2024-GAIRI-data.xlsx&wdOrigin=BROWSELINK
81. https://ai.gov.eg
82. Egypt , AI strategy, https://ai.gov.eg/Egypt National AI Strategy (6-4-2021)4.pdf
83. Egypt AI strategy , p. 60.
84. Egypt , Egypt Artificial Intelligence Strategy. https://ai.gov.eg/Egypt National AI Strategy (6-4-2021)4.pdf
85. Egypt ,Egyptian Charter For Responsible AI https://aicm.ai.gov.eg/en/Resources/EgyptianCharterForResponsibleAIEnglish-v1.0.pdf
86. Egypt ,Egyptian Charter For Responsible AI. p.1. https://aicm.ai.gov.eg/en/Resources/EgyptianCharterForResponsibleAIEnglish-v1.0.pdf
87. Egypt ,Egyptian Charter For Responsible AI. pp..2-3. https://aicm.ai.gov.eg/en/Resources/EgyptianCharterForResponsibleAIEnglish-v1.0.pdf

misuse, whether ethical, legal, or socio-economic, can promote and enable the widespread adoption of AI solutions”[88]. This is not yet the case. Egypt’s ethical use and deployment of AI systems is undermined by the lack of a national legal framework on AI.

One of the recommendations proposed in the strategy is to “communicate and coordinate with appropriate government bodies to issue laws and regulations when and where needed.”[89] This recommendation may be considered a call for the adoption of a regulation where the need arises. The question of adopting independent and specific AI laws and regulations may need more time because Egypt has recently commenced regulating AI by adopting a national strategy and Charter for responsible AI. In this stage, AI may be regulated by adding specific provisions to existing laws. In the same vein, as per media reports, the Parliamentary Committee on Communication and Technology has commenced deliberations on the adoption of AI-related regulations. The Committee Chairperson indicated that the proposed regulation will not be a separate law. Instead, the plan is to introduce AI-specific provisions to the Cybercrimes Law No. 175 for 2018. This approach is the first step towards the establishment of precise regulations governing various facets of AI within the Cybercrimes Law. The imperative to regulate the utilisation of AI systems is strongly advocated for, whether achieved through the enactment of an independent law or the incorporation of targeted provisions into existing legal frameworks.

In January 2025, due to the rapid development of AI technology, the Egyptian government launched the second edition of the NAIS (2025-2030)[90]. According to this Strategy, there are six strategic objectives the Egyptian State seeks to achieve by 2030:Ensure ethical and responsible AI use by establishing a comprehensive AI regulatory system, activate the ethical framework, and put a nucleus for a clear regulatory body, actively contributing to global efforts and playing an active role in AI different international fora;

1. Enhance quality of life and sectoral efficiency through AI applications;
2. Ensure data accessibility and sharing by developing frameworks for national data governance and strengthening life cycle management of domestic data;
3. 4. Build a robust scalable AI infrastructure and cloud services, innovate business models, and create a good digital foundation for the development of the AI industry with the support of infrastructure development;
4. 5. Create a healthy AI ecosystem by supporting local startups, small and medium enterprises, and innovation efforts, and strengthening the investment of venture capital institutions in Egypt;
5. 6. Strengthen the quantity and quality of local AI talents and experts.

In the reporting year, Egypt was subjected to the Readiness Assessment Methodology by UNESCO to check the readiness of Egypt to adopt AI in an ethical way.

Conclusion

While Egypt’s current legal frameworks contain provisions aimed at safeguarding digital rights, their efficacy in upholding citizens’ right to privacy is questionable. The absence of a precise definition outlining legitimate aims and reasonable grounds for surveillance poses a significant threat to digital rights. Moreover, the lack of clear criteria for identifying false news not only undermines freedom of expression but also opens the door to potential abuse. Addressing these gaps is crucial to fortifying the protection of digital rights and privacy for the citizens of Egypt. Therefore, in light of the identified gaps, stakeholders must consider the recommendations proposed in this report.

88. Egypt , AI strategy, p.47. https://ai.gov.eg/Egypt National AI Strategy (6-4-2021)4.pdf
89. Egypt , AI strategy, p.47. https://ai.gov.eg/Egypt National AI Strategy (6-4-2021)4.pdf
90. National AI Strategy, 2nd edition, 2025URL: URL: https://ai.gov.eg/

Recommendations

Parliament should:

- Enact an access-to-information law and adopt human rights-based approaches to combat the publication of false information.
- Amend the Telecommunications Regulation Law and ensure the legitimacy of surveillance practices.
- Amend Article 2 of Cybercrimes Law No. 175 of 2018 requiring service providers to retain and store data for 180 days by including justifications for the six-month data retention period.
- Amend article 80 and 177 of Criminal Procedures Code no 174 of 2025 before it enters into force to ensure respect of the right to privacy, In particular, it is strongly needed to determine definite periods for surveillance practice for the purpose of investigation. Furthermore, to determine specific crimes which may be subject to surveillance practice for legitimate purposes.
- Enact laws regulating the use of AI systems and their deployment in alignment with the AI strategy.
- Introduce explicit regulations through a standalone law or as an integral component within existing legislation to strengthen the legal framework on privacy rights and their protection. A proposed adjustment involves amending the title of the personal data protection law to: “Privacy and personal data protection”. Additionally, emphasis should be placed on including a dedicated and comprehensive chapter solely focused on delineating the rights to privacy and the corresponding safeguards within the legal framework. This nuanced approach ensures a more robust and distinct coverage of privacy concerns, enhancing the overall efficacy of the regulatory measures.

The Government should:

- Incorporate digital rights explicitly into the National Human Rights Strategy.
- Refrain from infringing on digital rights like privacy and cease engaging in unauthorised surveillance.
- Enact legislation that promotes the ethical utilisation of artificial intelligence.
- Ratify the Malabo Convention.
- Facilitate access to Universal Service Fund information through official government websites.
- Enhance transparency and accountability by annually publishing comprehensive reports on the Universal Fund’s activities and funded projects.
- Craft the USF reports to vividly highlight the significant progress achieved by the USF in narrowing the digital gap and addressing the digital divide. Illustrate the impactful strides made in fostering digital inclusion and reducing disparities.

The National Human Rights Council should:

- Engage in continuous monitoring of digital rights violations, document and propose policies and practices that uphold human rights.
- Aligning with their mandate, investigate all digital rights violations and, where necessary, refer violations for further investigation and judicial oversight.

Civil Society Organisations should:

- Enhance the skills of various stakeholders through comprehensive training programs.
- Strengthen the capability of legal professionals, with a particular focus on strategic litigation and the utilisation of international human rights standards in national court proceedings.
- Report any privacy breaches to the National Human Rights Council and other relevant judicial entities.
- Advocacy campaigns and activities against the new Criminal procedures law before its enter into force in October 2026.

Civil Society Organisations should:

- Enhance the skills of various stakeholders through comprehensive training programs.
- Strengthen the capability of legal professionals, with a particular focus on strategic litigation and the utilisation of international human rights standards in national court proceedings.
- Report any privacy breaches to the National Human Rights Council and other relevant judicial entities.
- Advocacy campaigns and activities against the new Criminal procedures law before its enter into force in October 2026.

Private Sector should:

- Ensure AI systems deployied for hiring or credit scoring, companies should audit these systems to ensure they don't discriminate against marginalized groups or specific geographic areas in Egypt.
- Adopt internal responsible AI guidelines.
- Ensure risk assessment took place before using AI systems.
- Raise awareness of their staff about the ethics of using AI systems and associated harm and risks and how to avoid and mitigate them..
- For companies using CCTV or employee monitoring software, provide clear "Privacy Notices" to staff.
- Ensure surveillance is used only for legitimate security purposes and is not intrusive to personal privacy.
- Adhere to data protection law and regulation and respect the privacy of employees and beneficiaries.
- Adhere to the transparency principle in using AI systems, cyber attacks which lead to breach the personal data and privacy of the staff and beneficiaries.

The Score Index

Egypt, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	4	4	Although Egyptian authorities resort to blocking some media websites, the Egyptian government did not disrupt access to the Internet and other digital technologies for segments of the public or an entire population.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	4	5	All laws,measures, and policies did not exclude some groups or include discriminatory provisions on gender or geographic bases. All existing policies and laws ensure the inclusion of all groups of society without any discrimination.
False News Criminalisation	P22(2)	1	1	False news is criminalised by different laws without clear criteria of what to consider as false news
Sedition Legislation	P22(2)	1	1	Sedition is criminalised by different laws, without criteria of what is considered sedition.
				Importantly, criminalisation of sedition is acceptable as long it is associated by specific criteria and clear definition. Neither declaration or other international instruments include clear criteria.
Data Protection Legislation.	P42	3	4	Data protection law and its executive regulation were a adopted, the institutional framework was completed. As , in 2025 data protection authority has been established.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	2	2	Different legislation give rights to the government to request the regulatory authority to remove online content or entirely or block the website
Invasion of Privacy of Communications	P41	1	1	Although surveillance is prohibited by the Constitution and other laws, there are laws allowing the surveillance of communication and in practice there is evidence of surveillance being used to close civic spaces as articulated in the report. In 2025, a new law has been passed furthering surveillance practices: Criminal procedures law no 174 of 2025

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	3	4	In 2025 Egypt adopted "Open Data Policy" to make all governmental data available for citizens, and the government considers it as a pre-step before issuing data governance law, and data classification framework. In addition, the Egyptian government established several platforms to disseminate information.
AI and Emerging Technologies national strategies	P29(3)	5	5	Since 2021, Egypt has had an AI national strategy and issued the Egyptian charter for responsible AI in 2023. Data Protection law, Cybercrimes law and other laws include some safeguards in case of misuse of AI
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	3	4	Egypt adopted different laws to protect children in general including in the digital sphere such as Children Law no 12 of 1996, penal code, cybercrimes law, data protection law, and law no 64 of 2010 to combat human trafficking
Digital Inclusion	P37(3)	4	5	The Universal Service Funds are addressing the digital divide and there are different government initiatives to address this gap
Total (out of 60):	2024: **32**		**2025 38**	

Ethiopia

By Anonymous

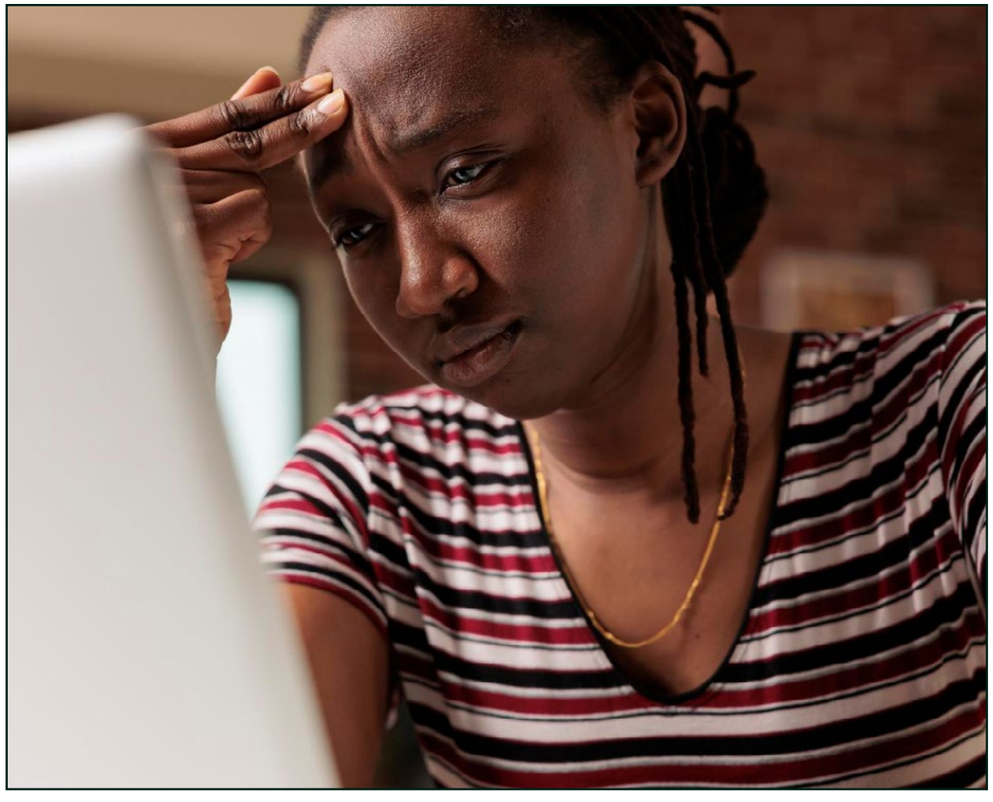
Executive Summary

This report highlights recurring internet shutdowns that cause economic and social disruptions, as well as the enactment of Ethiopia's Personal Data Protection Proclamation amid concerns about enforcement. Recommendations stress the need for robust enforcement of digital rights laws, targeted interventions to bridge the digital gender gap, and alignment with international human rights standards to foster a more inclusive and equitable digital landscape.

Thematic areas include internet access and affordability, freedom of expression, gender-based digital violence, data protection, and regulatory frameworks. The report employs a desk research methodology, synthesising data from government, civil society, media, and topic-specific sources to provide a comprehensive analysis of the digital rights landscape in Ethiopia in 2024. In addition, this report uses Paradigm Initiative's (PIN's) The Score Index

to assess digital rights in Ethiopia. Key sources of information include government websites, which provide official data and policy documents essential for understanding the regulatory and institutional framework. Different reports from civil society organisations offer insights into this report, showing ground-level realities and challenges. Additionally, media articles serve as a rich repository of events, trends, and public opinion, further enriching the report's analysis. Finally, websites relevant to the specific topics under investigation were thoroughly examined to gather supplementary information and contextual background.

By combining data from these diverse sources, the report's findings and recommendations are well-informed and also rooted in a robust evidentiary base, ensuring their reliability and relevance.



Introduction

Ethiopia is located in the Horn of Africa, and as of 2025, the country's population is estimated at approximately 135.4 million.[1] In recent years, Ethiopia has faced a turbulent political and social landscape marked by conflict in different parts of the country. These challenges have significantly impacted the digital rights environment, contributing to recurring internet shutdowns, restrictions on freedom of expression, limited access to information, and patterns of online censorship. Since 2016, Ethiopia's digital rights landscape has undergone major shifts shaped by political transition, insecurity, and telecom sector reform. Internet governance for much of this period was defined by heavy state control, limited access, and frequent restrictions on online expression. Periodic shutdowns during protests and political unrest became a recurring feature, reinforcing concerns about the use of connectivity restrictions as a tool for security and political management. At the same time, access remained largely urban-centred, with rural communities, women, and low-income groups facing structural exclusion from meaningful internet use.[2]

From 2018 onward, Ethiopia experienced some positive developments following the appointment of Prime Minister Abiy Ahmed (Ph.D), including amendments to restrictive laws and a broader opening of civic space during the early reform period from 2018 - 2020.[3] Digital engagement expanded, and the gradual modernisation of the communications sector accelerated. The establishment of the Ethiopian Communications Authority (ECA) and the partial liberalisation of the telecom market marked important progress toward expanding infrastructure, competition, and service delivery. More

1. Population of Ethiopia: https://www.populationpyramid.net/ethiopia/2025/BOCRA (2025) https://www.bocra.org.bw/sites/default/files/sites/default/files/documents/BOCRA2025_ANNUAL_REPORT_(WEB)_compressed.pdf (accessed on 10 January 2026)
2. Country report for Ethiopia - Internet Society Pulse: https://pulse.internetsociety.org/en/reports/ET/ nectivity-2025-understanding-mobile-internet-use-in-low-and-middle-income-countries (accessed on 09 January 2026)
3. Ethiopia: Freedom in the World 2025 Country Report: https://freedomhouse.org/country/ethiopia/freedom-world/2025

recently, the adoption of a Personal Data Protection Proclamation in 2024 and the approval of a National AI Policy, alongside the establishment of institutions such as the AI Institute, and the development of an AI strategy, signal growing recognition of privacy, innovation, and emerging technology governance as national priorities.

However, despite these reforms, persistent and in some cases, worsening challenges remain. Internet disruptions and targeted social media restrictions have continued during conflict and instability, undermining access to information and economic activity. The broader civic space has also shown signs of contraction. On December 25, 2024, the Authority for Civil Society Organizations (ACSO), the government agency responsible for regulating CSOs in Ethiopia, suspended two prominent human rights organisations, the Ethiopian Human Rights Council (EHRCo) and the Ethiopian Human Rights Defenders Center (EHRDC), along with the other previously suspended CSOs (CARD, LHR, AHRE) accusing them of engaging in activities deemed "not politically neutral" and "acting against national interests." The three-month suspension raised serious concerns about shrinking civic space and the increasing pressure on independent human rights actors.[4] In 2025, Ethiopia's digital rights environment remained characterised by both advancements and ongoing systemic challenges. While reforms aimed at increasing internet penetration and mobile coverage continue, barriers such as affordability, weak oversight, surveillance risks, and security-driven restrictions still limit Ethiopia's compliance with regional and international human rights standards on freedom of expression, privacy, and digital inclusion.

Internet Access

Between July 2024 and June 2025 (one Ethiopian fiscal year), the State-owned telecom operator, Ethio Telecom, continued to expand its network and digital services. The company reported a total customer base of 83.2 million. Mobile and broadband coverage

4. Ethiopia: alarming rise in the cases of suspension of civil society organizations at the end of 2024: https://srde-fenders.org/ethiopia-alarming-rise-in-the-cases-of-suspension-of-civil-society-organizations-at-the-end-of-2024-joint-communication/

expanded substantially, with 1,683 new mobile sites launched during the year, nearly half in rural areas, bringing mobile connectivity to an estimated 5.9 million new rural residents. 4G LTE service was extended to 512 new locations, increasing the total 4G-covered cities and districts to 936 and raising national 4G population coverage from 37.5% to 70.8%. The number of 5G-enabled cities rose from 10 to 26. Network capacity increased from 86.1 million to 104.8 million users, providing 99.4% population coverage and 86.5% geographic coverage nationwide.[5]

In addition to network expansion, Ethio Telecom's telebirr mobile payment platform strengthened digital financial inclusion. It reached 54.84 million users and processed over 2.38 trillion birr in transactions during the fiscal year, including 13.22 billion birr in microloans and 11.24 billion birr in digital savings.[6] Mobile ownership in Ethiopia rose from 57% to 65% in 2025, reflecting progress in overall connectivity. However, the mobile gender gap remains evident, with women still less likely to own or use mobile devices. The gap narrowed to 24% for general mobile ownership, but the disparity in smartphone access widened slightly; 42% of men own internet-enabled phones compared to only 24% of women. Beyond ownership, both men and women exhibit relatively low levels of daily mobile internet use, indicating that affordability, digital literacy, and socio-cultural barriers persist in limiting meaningful connectivity, particularly for women.[7]

Internet accessibility is also important for upholding the principles outlined in the Universal Declaration of Human Rights (UDHR),[8] especially Article 19, which guarantees freedom of opinion and expression, and Article 27, which ensures cultural rights. The Internet provides a critical platform for exercising these rights by enabling the free exchange of information and participation in cultural activities. Furthermore, the Sustainable

5. Ethio Telecom. 2024/25 Fiscal Year Performance Report (released July 2025): https://www.ethiotelecom.et/2024-25-fiscal-year-annual-performance-and-three-year-lead-growth-strategy-performance/
6. Ethio Telecom. 2024/25 Fiscal Year Performance Report (released July 2025): https://www.ethiotelecom.et/2024-25-fiscal-year-annual-performance-and-three-year-lead-growth-strategy-performance/
7. GSMA– Mobile Gender Gap Report 2025: https://www.gsma.com/gender-gap/
8. Universal Declaration of Human Rights: https://www.ohchr.org/en/UDHR/Documents/UDHR_Translations/eng.pdf; Date accessed October 20, 2024

Development Goals (SDGs)[9] emphasise the importance of internet access, particularly SDG 5 on gender equality, SDG 9 on industry, innovation, and infrastructure, and SDG 10 on reducing inequalities, highlighting the internet's role in achieving these global goals.

Since 2016, no country in Sub-Saharan Africa has experienced as severe internet shutdowns as Ethiopia over the years.[10][11] Since 2016, there have been at least 26 incidents of shutdowns in response to conflict, communal violence, and political turmoil.[12] There are no official records of internet shutdowns in 2025 in Ethiopia.

Freedom of Expression

The Ethiopian Constitution,[13] under Article 29, asserts the Right of Thought, Opinion, and Expression, and Article 30 guarantees the Right of Assembly, Demonstration, and Petition as democratic rights. These rights align with Article 19 of both the International Covenant on Civil and Political Rights (ICCPR)[14] and the African Charter,[15] which focus on freedom of expression.

Beyond the Londa 2024 Ethiopia report, [16] the detention of journalists and activists continued into 2025. In 2025, restrictions on media freedom intensified across

9. Sustainable Development Goals: https://sdgs.un.org/goals
10. Addis Standard news: https://addisstandard.com/ethiopia-tops-sub-saharan-africa-in-economic-losses-from-internet-shutdowns-new-study/ ; Date accessed Feb 6, 2025
11. The 5 Longest & Costliest Internet Shutdowns Recorded In Africa: https://weetracker.com/2025/11/03/longest-internet-shutdowns-africa/
12. Access Now: Shrinking Democracy, Growing Violence, May 2024, 2023-KIO-Report.pdf; Date accessed October 26, 2024
13. Constitution of Federal Democratic Republic of Ethiopia, 1995, https://www.fsc.gov.et/Digital-Law-Library/Federal-Laws/ArtMID/1179/ArticleID/152/Constitution-of-the-Federal-Democratic-Republic-of-Ethiopia-Proclamation-no-11995-%E1%8B%A8%E1%8A%A2%E1%89%B5%E1%8B%AE%E1%8C%B5%E1%8B%AB-%E1%8D%8C%E1%8B%B4%E1%88%AB%E1%88%8B%E1%8B%8A-%E1%8B%B2%E1%88%9E%E1%8A%AD%E1%88%AB%E1%88%B2%E1%8B%AB%E1%8B%8A-%E1%88%AA%E1%8D%90%E1%89%A5%E1%88%8A%E1%8A%AD-%E1%88%95%E1%8C%88-%E1%88%98%E1%8A%95%E1%8C%8D%E1%88%A5%E1%89%B5-%E1%8A%A0%E1%8B%8B%E1%8C%85-%E1%89%81-11987; Date accessed October 28, 2025
14. International Covenant on Civil and Political Rights, 1966, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights; Date accessed October 28, 2024
15. African Charter on Human and Peoples' Rights, 1981, https://achpr.au.int/en/charter/african-charter-human-and-peoples-rights/; Date accessed October 28, 2025
16. Londa report, 2024: https://paradigmhq.org/londa-24/; Date accessed on October 6 2025

several regions. In September 2025, the Tigray People's Liberation Front (TPLF) announced a "zero tolerance" stance against media outlets it accused of promoting division and serving the interests of "enemies," sparking alarm among journalists and media owners. Media professionals in the region described the rhetoric as an alarming escalation against press freedom and independent reporting.[17]

Beyond the Tigray region, journalists faced a series of detentions and harassment throughout the year. In Addis Ababa, three Sheger FM 102.1 journalists, Tigist Zerihun, Mintamir Tsegaw, and Eshete Assefa, were arrested after the station aired a report on health workers, despite complying with an Ethiopian Media Authority order to remove the broadcast. While Eshete was released the same day, the 2 journalists were released after more than 20 days in detention.[18]

Additional incidents include the August 5 detention of Somali Regional TV journalist Khadar Mohamed Ismail, who remains held without charge; the incommunicado detention of radio host Abdulsemed Mohammed until his release on August 22; and the abduction of The Reporter's senior editor, Yonas Amare, who was held for eight days by masked men before being freed.[19]

The clampdown reflects a broader pattern of intimidation observed in 2025. In March, 7 Ethiopian Broadcasting Service (EBS) journalists were charged with terrorism after airing allegations of sexual violence by government soldiers. [20] In April, Addis Ababa police raided the offices of Addis Standard, a private news station, seizing equipment that the outlet later claimed had been returned with surveillance software installed. In June, Tesfalem Woldeyes, editor-in-chief of Ethiopia Insider, was detained on accusations of "disseminating false information" and later released on bail

17. Londa report, 2024: https://paradigmhq.org/londa-24/; Date accessed on October 6 2025
18. Sheger FM journalists released after more than 20 days in detainment: https://addisstandard.com/news-sheger-fm-journalists-released-after-more-than-20-days-in-detention/
19. HRW: Surge in Arrests of Journalists, Media Workers: https://www.hrw.org/news/2025/09/22/ethiopia-surge-in-arrests-of-journalists-media-workers
20. Ethiopian Media Authority suspends EBS TV program over "false information", "misleading the public": https://addisstandard.com/ethiopian-media-authority-suspends-ebs-tv-program-over-false-information-misleading-the-public/
21. IFJ: Journalist released after six days in custody: https://www.ifj.org/media-centre/news/detail/article/ethiopia-journalist-released-after-six-days-in-custody

after 6 days in custody.[21]

Some of these actions followed the April 17 amendments to the 2021 media law, which transferred key regulatory powers to the Prime Minister–appointed Director General of the Ethiopian Media Authority, reducing the role of civil society and professional associations in media oversight. Additionally, non-governmental organisations advocating for media freedom have faced increasing pressure, including surveillance, suspension, and intimidation of activists.[22]

Technology Facilitated Gender Based Violence (TFGBV) remains a significant issue in Ethiopia, forcing women to withdraw from public spaces and limiting their participation in public life, both online and offline. Numerous women have recounted experiences of physical assaults, detention, and having to flee the country following threats of TFGBV.[23],[24] Women and girls are subjected to more hate speech, including gendered stereotypes and mockery, than men and boys.[25]

In 2025, technology-facilitated gender-based violence (TGBV) continued to escalate, with feminist activists facing some of the most severe attacks. One of the most alarming cases involved Yordanos "Jordin" Bezabih, a feminist advocate and co-founder of Setaset Power. After her laptop was stolen, her private accounts were hacked, and intimate photos, videos, and voice recordings were leaked online. The material was then used to create deepfake content accompanied by coordinated calls for violence against her.[26]

Jordin's case reflects a broader trend of targeted online violence against women who speak publicly about gender equality. In the past year, another feminist figure, Lella "Emama Fishka" Misikir, also left Ethiopia after facing sustained death threats and online abuse. In both instances, attackers framed feminism as a threat to religious and cultural norms, often linking it to fabricated claims about promoting same-sex relationships.[27] These narratives have fuelled digital harassment campaigns that silence women's voices and push them out of public life both online and offline.[28]

In Ethiopia, the LGBTQIA+ community endures significant challenges, including institutionalised persecution and societal violence. Even minor nonconformities, such as wearing skinny jeans or having colored hair, can lead to false perceptions of being gay, resulting in social ostracisation and physical violence. Many individuals face doxxing, where their identities are exposed online through disinformation rumours, leading to home invasions and assaults, forcing some to flee for their safety[29,30].

22. HRW: Proposed Legal Changes Threaten Civil Society: https://www.hrw.org/news/2025/07/29/ethiopia-proposed-legal-changes-threaten-civil-society
23. France 24, 'Normalised and invisible': online abuse targets Ethiopian women: https://www.france24.com/en/live-news/20240529-normalised-and-invisible-online-abuse-targets-ethiopian-women; Date accessed January 19, 2025
24. GenderIT, Technology Facilitate Violence: The Fourth Battlefield Amid the Escalation in Ethiopia, https://genderit.org/feminist-talk/technology-facilitate-violence-fourth-battlefield-amid-escalation-ethiopia? ; Date accessed January 9, 2025
25. The Centre for Information Resilience (CIR), Research on Technology-Facilitated Gender-Based Violence in Ethiopia Summary Document, May 2024, https://www.info-res.org/_files/ugd/587f01_849a90c2a17d4526b0fc69b-049b8946a.pdf ; Date accessed October 30, 2024
26. Amnesty International: Ethiopia WHRDs targeted with digital violence: https://www.amnesty.org/en/latest/news/2025/02/ethiopia-woman-human-rights-defender-targeted-with-digital-violence/

Data Protection and Privacy

In April 2024, the House of Peoples' Representatives (HoPR) of the Federal Democratic Republic of Ethiopia ratified the Personal Data Protection Proclamation, 2024.[31] Despite this legislative milestone, several human rights and media institutions raised concerns regarding the appointment of the Ethiopian Communications Authority (ECA) as the regulatory body responsible for overseeing data protection, but it may lack the necessary independence and expertise to effectively enforce the new regulations.

ECA conducted awareness creation sessions in 2025 with different entities, such as Telecom service providers and the National ID Ethiopia.

27. The Continent: https://www.thecontinent.org/_files/ugd/287178_8f2ba983303e42faa70d0f49a9ad7212.pdf?index=true
28. Digital gender-based violence is putting Ethiopian women under siege https://www.geeska.com/en/digital-gender-based-violence-putting-ethiopian-women-under-siege
29. Sifter Newsletter: https://sifter.substack.com/p/how-many-salaries-can-you-afford?r=38rapq&triedRedirect=true November, 12, 2024; Date accessed November 14, 2024
30. Sifter Newsletter: https://sifter.substack.com/p/how-many-salaries-can-you-afford?r=38rapq&triedRedirect=true November, 12, 2024; Date accessed November 14, 2024
31. Fana Broadcasting Corporate, House endorses personal data protection bill, April 4, 2024, https://www.fanabc.com/english/amp/house-endorses-personal-data-protection-bill/ ; Date accessed October 27, 2024

Digital Inclusion

Ethiotelecom announced a comprehensive strategy for the 2024/25 fiscal year, focusing on significantly enhancing telecom coverage and capacity. The plan includes constructing 1,298 new mobile sites, expanding 4G service to 500 additional cities, and introducing 5G service to 15 more cities. To bridge the digital divide, 331 rural connectivity solutions and 165 mobile network sites will be established, totaling 496 sites, to improve network coverage in 1,000 rural kebeles. Ethio Telecom aims to increase its subscriber base by six per cent, targeting 83 million customers, and boost revenue by 74.7% to 163.7 billion birr by the end of the fiscal year.[32]

In 2023, Ethiopia enacted the Ethiopian Digital Identification Proclamation No. 1284/2023[33]. The National Identity (ID) Program (NIDP) is responsible for implementing this foundational national identification system. The program issues a 12-digit unique identifier, known as the Fayda ID, to all residents of Ethiopia. This ID serves as a tool for service delivery and Know Your Customer (KYC) processes in both the public and private sectors. The NIDP ensures the quality of its enrollment through biometrics and authentication services, aiming to register 90 million residents by 2028.[34] Exclusion of service for people without a national ID is announced by various service providers. For instance, Ethio Djibouti Railway SC has announced the launch of its online booking platform for public passenger transport services, starting in February 2025, where all travel bookings will now require Fayda, the national ID[35]. Additionally, beginning January 1, Ethiopians must present a Fayda national digital ID to open a bank account at branches in the capital, and banks nationwide must comply with Fayda standards by January 2026, while those in major cities face an earlier deadline of July 1, 2025.[36]

Ethio telecom has launched high-speed 4G LTE mobile services across 93 cities nationwide, substantially extending digital connectivity infrastructure across Ethiopia's diverse geography[37]. The Universal Service Fund (USF) is soon to be implemented[38], yet the Ethiopian Communications Authority enacted the universal access and service framework in 2022

32. Ethiotelecom press statement: https://www.ethiotelecom.et/%E1%8B%A8%E1%8A%A2%E1%89%B5%E1%8B%AE-%E1%89%B4%E1%88%8C%E1%8A%AE%E1%88%9D-%E1%8B%A82017-%E1%89%A0%E1%8C%80%E1%89%B5-%E1%8B%93%E1%88%98%E1%89%B5-%E1%8A%A0%E1%88%98%E1%89%B3%E1%8B%8A-%E1%8B%A8%E1%89%A2/?lang=am ; Date accessed February 6, 2025
33. Ethiopian Digital Identification Proclamation (2023) https://ethiodata.et/wp-content/uploads/2023/09/Ethiopian-Digital-Identification-Proclamation-No.-1284_2023-1.pdf, Date accessed November 03, 2024
34. https://id.gov.et/worldbank
35. Birrmetrics News: https://birrmetrics.com/ethio-djibouti-railway-launches-passenger-service-requires-national-id/

Conclusion

Ethiopia's policy efforts, data protection proclamation, AI policy, regulatory frameworks and private sector activity are setting the stage for a modern digital economy. Yet the gains are shadowed by shrinking civic space, uneven implementation capacity, uncertain USF transparency, and lingering risks from surveillance technologies and weak oversight mechanisms. If Ethiopia strengthens institutional oversight, ensures transparent USF management, operationalises the data protection law with an independent regulator, embeds human rights safeguards in AI and cybersecurity policies, and invests in affordability and accessibility programs, the trajectory can shift towards inclusive, rights-respecting digital transformation

36. Capital Market Ethiopia, National Bank of Ethiopia Mandates National ID for Banking, https://www.capitalmarketethiopia.com/national-id-must-for-banking-ethiopia/ ; Date accessed January 10, 2025
37. https://ethicalbusiness.africa/2025/12/16/ethio-telecom-expands-4g-coverage-to-93-cities-in-nationwide-connectivity-push/
38. Universal Service Funds in Africa, GSMA, October 2023 https://www.gsma.com/about-us/regions/sub-saharan-africa/wp-content/uploads/2023/10/USF-Africa.pdf; date accessed on January 8, 2025

Recommendations

The Government:

- Prioritise the protection of digital rights by ceasing the use of internet shutdowns during conflicts, which undermine freedoms of expression and access to information. It should adopt transparent policies regarding internet governance.
- Though Ethio-Telecom is implementing different initiatives to curtail internet accessibility of rural and women communities, authorities should implement subsidy programs for smartphones and internet access targeting women and marginalised groups. This should be coupled with digital literacy campaigns to empower women and address socio-cultural barriers.
- Review and amend laws like the Hate Speech and Disinformation Prevention Proclamation of 2020 to ensure they align with international human rights standards.
- End arbitrary detentions of journalists and activists and provide robust protections for free speech.
- Establish an independent and adequately resourced data protection authority to oversee compliance with the Personal Data Protection Proclamation of 2024, investigate violations, and hold perpetrators accountable.
- Expedite the operationalisation of the USF through policy to expand connectivity in underserved areas, ensuring equitable access to digital services for all.
- Proactively disclose information on policies affecting digital rights and technologies, fostering public understanding and participation in digital governance.

Civil Society Organisations should:

- Civil society organisations should focus on litigation and advocacy to challenge internet shutdowns, freedom of expression violations, and weak data protection measures.
- Produce evidence-based research to support their campaigns.
- Form coalitions at the local level and join regional and international coalitions to amplify advocacy efforts, access resources, and promote accountability for digital rights violations.
- Civil society should advocate for the establishment of an independent Personal Data Protection Commission to ensure the impartial enforcement of data protection laws.

The Private Sector should:

- Telecommunications and social media companies should partner with stakeholders to enhance digital literacy, particularly in underserved regions, while ensuring safe online spaces through effective content moderation in local languages.
- Telecommunications operators should actively contribute to the USF and work towards expanding coverage to unconnected regions.
- Telecommunications companies should let service seekers know the reason for internet shutdowns.

The Score Index

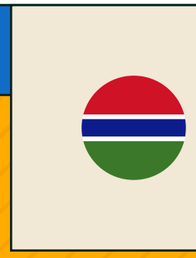
Ethiopia, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	1	4	Though there was no OFFICIAL internet shutdown in Ethiopia, the government needs to be transparent regarding who shuts down the internet and for what purpose
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	2	2	Minimal reforms are needed in terms of law around AI, data protection law, and USF
False News Criminalisation	P22(2)	1	1	Journalists were detained and charged under Ethiopia's hate speech and disinformation law. Authorities accused many journalists of false news.
Sedition Legislation	P22(2)	2	2	Ethiopia does not have a specific sedition law; however, provisions within the Criminal Code, and Hate Speech and Disinformation Proclamation function as de facto restrictions on speech. These laws contain broadly defined offences that have, in practice, been used to regulate dissent and online expression.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	Different media personnel and HRDs, were imprisoned arbitrarily
Data Protection Legislation.	P42	3	3	The proclamation was enacted in 2024, though there are limitations in the proclamation's implementation because of the capacity of regulatory body.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	2	2	TikTok received 2 requests from January to June 2025 from Ethiopia government and Meta has also received a request and stated it in its transparency report.
Invasion of Privacy of Communications	P41	2	2	HRDs and HROs staff, as well as media institutions, were targeted, and their office and devices were confiscated.[39]

39. https://addisstandard.com/cpj-warns-of-sensitive-data-misuse-amid-polices-continued-seizure-of-multiple-electronic-devices-confiscated-in-raid-on-addis-standard/

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Failure by the government to proactively disclose and disseminate information digital technologies	P29(3)	1	1	Citizens were unaware when internet shutdowns happened and who imposed them.
AI and Emerging Technologies national strategies	P39(6)	2	3	The state is using emerging technologies and AI for different purposes, including establishing an AI institution and introducing the plan for the AI University. Yet proclamation that is guiding it is missing.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	3	3	Though there are no specific laws to promote children's digital safety, the data protection proclamation gives greater emphasis to children's data privacy
Digital Inclusion	P37(3)	2	3	State-owned telecom company, Ethiotelecom, has expanded unconnected regions to promote digital inclusion.
Total (out of 60):	2024: **21**		2025 **26**	



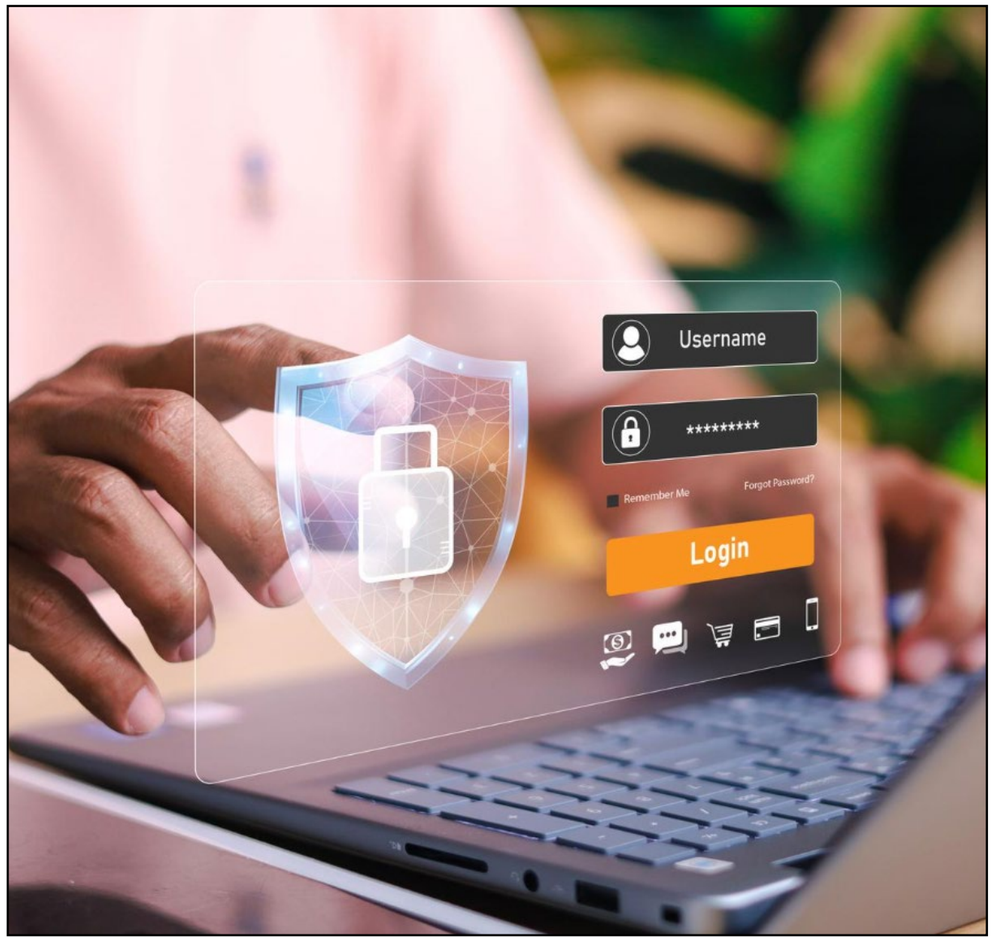
Gambia

By Muhammed B. Sowe

Executive Summary

This report gathered evidence from diverse sources including newspaper articles, court decisions, press statements and reports from media rights organisations. It covers thematic areas such as internet access and disruptions; online freedom of expression and access to information; data protection and cybersecurity; privacy and surveillance; developments in ICT and emerging technologies; digital inclusion. The country's score for TheScore Index puts it at 34 out of 60, moderately compliant for 2025. Key highlights include enactment of the Personal Data Protection and Privacy Act 2025 which makes provision for the protection of digital rights. Although the Personal Data Protection and Privacy Act 2025 was enacted during the reporting period, its institutional and enforcement mechanisms remain at an early stage of implementation. The validation of the Access to Information Regulations 2025, which seeks to give

effect to the full implementation of the Access to Information Act 2021, is another key highlight. While the Act is formally operational, it has not yet been fully implemented in practice. The report shows that The Gambia continues to experience slow internet connectivity, coupled with unaffordable internet services. Also, The Gambia still maintains laws on sedition and false news. These implementation gaps, particularly in access to information, freedom of expression, and affordable connectivity continue to limit The Gambia's full compliance with the ACHPR Declaration.



Introduction

The 2024 Londa Report highlighted that The Gambia made considerable progress in the areas of digital rights and internet freedom since 2017, coupled with persistent challenges.[1] While there has been an increase in the number of internet users and the enactment of the data protection law to protect digital rights, The Gambia continues to experience slow and poor internet connection, internet disruptions and high cost of internet data due to poor ICT infrastructure. Limited public investment in ICT infrastructure continues to constrain meaningful access. The Gambia also maintains laws that threaten digital rights and internet freedom. These laws are contained in the newly enacted Criminal Offences Act 2025, which maintains the criminalisation of sedition and false news, despite the decision of the ECOWAS Court of Justice decision in the case of Federation of African Journalist & 4 Ords v The Gambia ECW/CCJ/JUD/04/18 delivered in 2018. The Access to Information Act 2021 is not fully implemented, thus there is absence of proactive disclosure of information by public institutions. These unresolved challenges directly informed The Gambia's 'moderately compliant' score under TheScore Index. This is as a result of the existence of the unresolved challenges referred to above, which continued into 2025.

Internet Access

The Gambia's telecommunications services regulatory body, Gambia Public Utilities Regulatory Authority (PURA) has no complete data on internet coverage, quality and disruptions for the year 2025. The lack of complete internet data by PURA reveals a troubling account of poor infrastructure leading to weak enforcement. The fact that PURA as the internet service regulatory authority does not have readily available data on the state of internet

1. Paradigm Initiative, Muhammed B. Sowe 'Londa 2024 Digital Rights and Inclusion in Africa Report-The Gambia' (2024) https://paradigmhq.org/wp-content/uploads/2024/06/The-Gambia-Country-Report.pdf (accessed 5 November 2025).

accessibility, quality and disruptions in The Gambia clearly shows absence of the required infrastructure to enable effective and efficient regulation of the telecommunication sector. This regulatory data gap underscores structural weaknesses in sector oversight and limits PURA's ability to ensure universal affordable, and reliable internet access.

DataReportal's 'Digital 2025' report shows that The Gambia's internet penetration rate stood at 45.9% of the population (1.28 million people) at the start of 2025.[2] This is a decrease of 8.3% from January 2024 to January 2025. The report also shows that there are 3.15 million cellular mobile internet connections by the start of January 2025 representing an equivalent of 113% of the total population, with an increase of 5.5% compared to 2024. The report noted that many people make use of more than one mobile connection, and as such the mobile connection users significantly exceeded the total population. Also, the number of social media users in The Gambia at the start of 2025 stood at 449,000 active users, equating to 16.1% of the total population.[3] This reflects an increase of 45,000 users from the year 2024. Despite the increase in internet users in 2025, the fastest internet connection speed in The Gambia recorded in the third quarter of 2025 was provided by Netpage with an average download speed of 17.2 Mb/s.[4]

The Gambia is among the 10 countries with the slowest broadband connection and network qualities for citizens. This is associated with the country's lack of investment in ICT infrastructure and technology which ensures faster internet speed. For example, the budget of the Government of The Gambia for 2025 shows that the Ministry of Communications and Digital Economy (MoCDE) was allocated the sum of GMD96,212,260 (US$1,355,102.25),[5] representing 0.25% of the national budget.[6] This is evidence of the lack of prioritisation of ICT development in order to enhance access and inclusion of all people, including children and vulnerable groups. The absence of targeted budget lines for rural communities, women, or persons with disabilities further undermines equitable digital inclusion. This shows the lack of commitment of the Government of The Gambia to develop the ICT sector with a view to ensuring accessibility and affordability to the people, including vulnerable groups. The allocation of less than 1% of the total national budget to the ICT sector explains the reason for the poor telecommunication infrastructure in The Gambia. This has a great impact on the country's socio-economic advancement, thus limiting the participation of Gambians in the global digital economy.

The Gambia suffers from unstable and slow internet connection coupled with exorbitantly high cost of mobile data, making the Internet unaffordable for many Gambians.[7] On August 22 2025, a coalition of civil society organisations including the Edward Francis Small Centre for Rights and Justice (EFSCRJ), Gambians Against Looted Assets (GALA), and Team Gom Sa Bopa organised a peaceful protest against the decision of PURA to enforce a minimum data tariff of D50 (US$0.69) per 1GB for GSM operators. The coalition condemned PURA's new policy as "anti-competitive" and a direct assault on affordable internet access, a critical lifeline for education, employment, and civic engagement in Gambia. The D50 per gigabyte minimum tariff marks a staggering 243% increase from promotional data bundles previously offered by GSM operators

2. DataReportal 'Digital 2025: The Gambia' (2025) https://datareportal.com/reports/digital-2025-gambia (accessed 9 November 2025).
3. DataReportal 'Digital 2025: The Gambia' (2025) https://datareportal.com/reports/digital-2025-gambia (accessed 9 November 2025).
4. Speedgeo 'Internet Speed in Gambia' (2025) https://www.speedgeo.net/statistics/gambia (2025) (Accessed 9 November 2025).
5. Carbri 'Approved Estimates of Revenue and Expenditures 2025'. (2025) Available at: https://www.cabri-sbo.org/en/documents/estimates-of-revenue-and-expenditure-5 (Accessed 12 November 2025).
6. Ministry of Finance and Economic Affairs 'Citizens' Budget: Budget of the Government of The Gambia 2025'(2025). Available at: https://mofea.gov.gm/wp-content/uploads/2025/04/2025-Approved-Budget-Citizens-Version.pdf (Accessed 12 November 2025). The National Budget for 2025 also shows that the sum of D12,320, 000 (USD173, 521) has been allocated for Information Communication Technology (ICT) research and development.
7. The Point Newspaper 'GCCI, consumers slam PURA's halt on cheap internet bundles' (2025) https://thepoint.gm/africa/gambia/headlines/gcci-consumers-slam-puras-halt-on-cheap-internet-bundles#google_vignette (Accessed 19 November 2025).

at rates as low as D13.33 (equivalent to US$0.18) per gigabyte.[8] Following a peaceful protest, the police arrested 19 protesters and charged them with unlawful assembly,[9] a move that caused outrage and condemnation by civil society organisations including Article 19.[10] The arrest of protesters advocating for affordable internet access raises concerns under Principle 37 of the ACHPR Declaration, which obliges states to promote universal, affordable, and meaningful access to the internet.

Reports continue to show that The Gambia has one of the most expensive internet charges in the world and ranked 8th in the African countries with the most expensive mobile data.[11] Internet connectivity in rural Gambia is poorer than in the urban areas because of the absence of adequate communication infrastructure. The public outrage and peaceful protests by civil society organisations are evidence of people's frustration with the high cost of the internet coupled with slow internet services across the country. The GSM operators are accused of exploiting users with high tariffs and poor services, while PURA is accused of failing to ensure affordable and reliable internet service.

Although the Government started engaging Starlink Services for the provision of satellite internet services to diversify internet access options in the country,[12] in 2024, there were no new developments regarding the operations of Starlink services in The Gambia in 2025. Starlink has submitted an application for a license to operate internet services in The Gambia and it is awaiting the approval of the Minister for Communication and Digital Economy.[13] As of November 26 2025, Starlink services are not available. Starlink's internet service is expected to bridge the digital divide; offer high-speed internet access; enhance rural internet access; end monopolies enjoyed by local ISPs and ensure competition. Notwithstanding, concerns remain about the potential implications, including national security and localization of data.

Internet disruption

In May 2025, The Gambia's national telecommunications provider, Gamtel, reported internet disruption to its fibre optic networks due to fibre cable cuts through vandalism.[14] The internet disruption, which lasted for about four hours, caused internet black out in Banjul, Kanifing and the West Coast Region. It affected both residential and commercial entities in these regions. Gamtel's fibre cable cut remains a major source of internet disruptions in The Gambia. Despite these challenges, there appears to be no deliberate internet shutdowns occasioned by the State during the reporting period, a sign of compliance with international standards.

Online Freedom of Expression and Access to Information

Section 25(1) of the Constitution of The Gambia, 1997, guarantees the right to freedom of speech and expression, which includes freedom of the media. Even though The Gambia has registered significant progress in freedom of expression and of the media between 2017 and 2024,[15], the events in 2025 suggest a retrogression. The Gambia enacted the Criminal Offences Act 2025 which criminalises false publication and broadcasting, sedition,

8. The Alkamba Times '19 Protesters arrested in clash with the police over PURA's data price hike' (2025). https://alkambatimes.com/19-protesters-arrested-in-clash-with-police-over-puras-data-price-hike/ (accessed 9 November 2025).
9. The Alkamba Times '19 Protesters arrested in clash with the police over PURA's data price hike' (2025). https://alkambatimes.com/19-protesters-arrested-in-clash-with-police-over-puras-data-price-hike/ (accessed 9 November 2025).
10. Article 19 'The Gambia: Authorities must release protesters and protect their rights' (2025) https://www.article19.org/resources/the-gambia-authorities-must-release-protesters-and-protect-their-rights/ (accessed 9 November 2025).
11. Gambiana 'GDC calls for affordable and reliable internet in The Gambia' (2025) https://gambiana.com/gdc-calls-for-affordable-and-reliable-internet-in-the-gambia/ (accessed 9 November 2025);
12. Foroyaa Newspaper 'Gambia Explores Possible Launch of Starlink Services' (2024) https://foroyaa.net/gambia-explores-possible-launch-of-starlink-services/ (accessed 9 November 2025).
13. African Press 'gov't Taking Due Diligence Amid US Pressure for Starlink' (2025) https://www.africa-press.net/gambia/all-news/govt-taking-due-diligence-amid-u-s-pressure-for-starlink (Accessed 9 November 2025)
14. Gambiana 'Gamtel investigates sabotage after major internet disruption' (2025) https://gambiana.com/gamtel-investigates-sabotage-after-major-internet-disruption/ (Accessed 9 November 2025)
15. Reporters Without Borders 'Gambia' (2025) https://rsf.org/en/country/gambia (Accessed 9 November 2025)

and parental insult of public officials. This is notwithstanding the decision of the Community Court of Justice of ECOWAS in 2018 that The Gambia's criminalisation of sedition and false publication and broadcasting is not in line with international human rights.[16] Civil Society organisations condemned the National Assembly for passing the Criminal Offences Act 2025 with repressive provisions against freedom of expression and of the press.[17] They called on the National Assembly to repeal the said provisions. Members of the public also raised concerns about the provisions being discriminatory,[18] legally absurd[19] and that they pose a threat to Gambia's democracy.[20] The sedition law was applied within months of its enactment. On August 21 2025, sedition charges were brought against Abdoulie Sanyang over comments made on West Coast Radio where he accused President Adama Barrow of electoral malpractices in the 2021 Presidential elections.[21]

The Gambia introduced the Cyber Crime Bill in the National Assembly, which contains provisions that impede freedom of speech and expression,

16. Federation of African Journalist & 4 Ords v The Gambia ECW/CCJ/JUD/04/18 http://www.courtecowas.org/wp-content/uploads/2019/02/ECW_CCJ_JUD_04_18.pdf (accessed 10 November 2024).
17. Kerr Fatou 'EFSCRJ Raises Issues and Concerns about the Criminal Offences Act 2025' (2025) https://www.kerrfatou.com/efscrj-raises-issues-and-concerns-about-the-criminal-offenses-act-2025/ (Accessed 9 November 2025); The Media Foundation for West Africa ' Gambia Press Union challenges government over laws limiting press freedom' (2025) https://mfwa.org/partner-highlights/gambia-gpu-press-freedom-laws-2025-2/ (Accessed 9 November 2025); The Point Newspaper 'RSF asks Gambia to repeal draconian media laws' (2025) https://thepoint.gm/africa/gambia/headlines/rsf-asks-gambia-to-repeal-draconian-media-laws (Accessed 9 November 2025).
18. Askanwi Gambia Radio and Newspaper 'Gambia: The New Criminal Offence Act 2025 is discriminatory' (2025) https://askanigambia.com/gambia-the-new-crmininal-offence-act-2025-is-discriminatory/ (Accessed 9 November 2025).
19. The Point Newspaper 'Section 113 of the Criminal Offences Act 2025 is legally absurd and must be repealed' (2025) https://thepoint.gm/africa/gambia/opinion/section-113-of-the-criminal-offences-act-2025-is-legally-absurd-and-must-be-repealed (Accessed 9 November 2025).
20. The Voice Newspaper 'Critics Slam Gambia's New Criminal Code as Threat to Democracy' (2025) https://www.voicegambia.com/2025/06/12/critics-slam-gambias-new-criminal-code-as-threat-to-democracy/ (Accessed 9 November 2025).
21. The Alkamba Times 'Former Soldier Remanded in Arson and Sedition Charges, Case moved to High Court' (2025) https://alkambatimes.com/former-soldier-remanded-on-arson-and-sedition-charges-case-moved-to-high-court/ (Accessed 9 November 2025).

including digital rights. Furthermore, 2025 witnessed the return of intimidation of journalists by Government officials, including the Minister of Information. These events evidence erosion of freedom of speech and expression as well as freedom of the media. On March 27 2025, the Minister of Information, Dr Ismaila Ceesay, summoned the Editor in Chief of The Voice Newspaper; the Media Council; and the Newspaper Publishers Association. The summon was in connection to a report in The Voice Newspaper, titled "Survey reveals corruption at the Presidency, National Assembly," which looked at corruption in the public sector. The Minister of Information claimed that the headline was misleading and damaged the image of the Government of The Gambia. This move by the Minister of Information was condemned by human rights organisations.[22] and showcased intimidation of the media over their reports.

> **Survey reveals corruption at the Presidency, National Assembly,**
>
> Key Informant A

All these actions continue to affect The Gambia's ranking on the freedom of press index, with a decline from 10th to 11th position out of 54 African countries.[23] The Gambia maintained 58th position out of 180 countries in the global press freedom index, the same position as 2024.[24] The Gambia's drop in ranking for the year 2025 is linked to Government exerting pressure

22. The Media Foundation for West Africa 'The Gambia: Minister summons newspaper editor, media stakeholders over newspaper headline' (2025) https://mfwa.org/country-highlights/gambia-minister-summons-editor-over-newspaper-headline/ (Accessed 9 November 2025); Askani Gambia 'Gambia: Forcing the Media to Apologize is intimidation' (2025) https://askanigambia.com/gambia-forcing-the-media-to-apologize-is-intimidation/ (Accessed 9 November 2025)
23. Askanwi 'Sierra Leone and Liberia Overtake The Gambia in African Press Freedom Index' (2025) https://www.askanwi.com/news/sierra-leone-and-liberia-overtake-the-gambia-in-african-press-freedom-index#:~:text=-Folder:%20About%20Us-,Sierra%20Leone%20and%20Liberia%20Overtake%20The%20Gambia%20in%20African%20Press,%E2%80%9Csatisfactory%E2%80%9D%20press%20freedom%20environment (Accessed 9 November 2025)

on media outlets at times; hostility towards journalists, particularly from comments by the President accusing the media of reporting false news and having the intent of promoting conflict and instability; enactment of repressive laws against freedom of express and of the press, including laws on parental insult of certain government officials and false publication and broadcasting.[25]

With regards to content moderation, there have been no reports of blocking or filtering of websites or apps by the Government from 2017 to 2025. However, concerns have been raised about the Cybercrime Bill 2024, currently before the National Assembly, containing provisions which have the potential future restrictions of websites, thus impacting digital rights.[26]

Access to Information

Since the enactment of the Access to Information Act, 2021 (ATI 2021), it is yet to be fully implemented.[27] The lack of implementation of the ATI 2021 extends to the period under review. The following key elements of the ATI are yet to be fully implemented:

(a) While the ATI 2021 requires the head of every public body, in consultation with the Minister of Information, to designate a suitable officer as information officer to receive requests for information, this has not been complied with.[28] On November 12 2025, the Access to Information Commission issued a press release urging Ministries, Departments and Agencies to designate information officers in compliance with the ATI

24. Reporters Without Borders 'Gambia' (2025) https://rsf.org/en/country/gambia (Accessed 9 November 2025)
25. Ibid.
26. Civicus 'New Criminal Law and Draft Cybercrime Bill in The Gambia threatens Press Freedom, Freedom of Expression and Digital Rights'(2025) https://monitor.civicus.org/explore/new-criminal-law-and-draft-cyber-crime-bill-in-the-gambia-threatens-press-freedom-freedom-of-expression-and-digital-rights/#:~:text=On%2024th%20March%202025%2C%20The,the%20draft%20bill)%20for%20adoption. (Accessed 9 November 2025)
27. Reporters Without Borders 'Gambia' (2025) https://rsf.org/en/country/gambia (Accessed 9 November 2025).
28. The Point Newspaper 'Public institutions urged to designate information officers' (2025) https://thepoint.gm/africa/gambia/headlines/public-institutions-urged-to-designate-information-officers (Accessed 31st December 2025).

2021.[29] The implication of the absence of an information officer is that the people do not know whom to contact to request information. This denies them the right to request and access information from public bodies.

(b) Section 12 of the ATI 2021 provides that a request for information shall be accompanied by such a reproduction fee as prescribed in a regulation made by the Minister of Information. No such regulation has been made by the Minister so as to prescribe the reproduction fees. The absence of a regulation on reproduction fee allows for potential and unpredictable excessive cost of reproduction, which may render information inaccessible to the public.

(c) Public bodies do not respond to requests for information within the prescribed time frame of 21 days for response. For example, the author of this report on October 27 2025 made a request via email for information to the PURA and MoCDE as regards data on state of internet access in The Gambia in 2025; the number of reported internet disruptions from January 2025 to October 2025; the state of implementation of the Universal Service Fund in The Gambia in 2025; and the state of digital inclusion of persons with disabilities in 2025. Even though PURA acknowledged receipt of the request, it only responded to the request for information on 31 December 2025. This is64 days after the request. MoCDE is the ministry responsible for communications, and is supposed to have this information, neither acknowledged nor responded to the request.

(d) Section 61 of the ATI 2021 requires public bodies and relevant private bodies to submit implementation plans to the Access to Information Commission within 6 months of the establishment of the Commission. The implementation plan should outline the institution's operational plan to implement its obligations under the ATI 2021 and information publication plan in respect of its proactive disclosure responsibilities under the Act. The Access to Information Commission was established on 5 September 2024, when the five Commissioners were sworn into office by the Vice President. It has been over a year since the establishment of the Access to Information Commission and none of the public bodies and relevant private bodies has submitted their

29. Ibid.

implementation plan to the Access to Information Commission.

(e) The Access to Information Commission takes a considerable amount of time to determine appeals arising from refusals or denials to grant access to information by public bodies. For example, The Republic, an investigative media outlet, has submitted six appeals with the Access to Information Commission against government institutions since February 2025. As at November 26 2025, the Access to Information Commission has not determined these appeals. It claimed that it could not determine the said appeals in the absence of regulations, which it is already developing. This is in the light of the fact that the Act is silent on the timelines for the determination of appeals by the Access to Information Commission. The proposed regulations will hopefully address the time limit. The absence of implementing regulations continues to stall the effective enforcement of the ATI 2021 as appeals against decisions of heads of public bodies cannot be determined.

Notwithstanding the above, the Gambia has taken some commendable steps in 2025 in the implementation of the ATI law of 2021. The Access to Information Commission has been fully established after the swearing of the Commissioners in September 2024.[30] On January 27 2025, the stakeholders validated the Access to Information Roadmap,[31] which outlines the roles and responsibilities of stakeholders, including the process and timelines for the full implementation of the ATI 2021.

Between January 2025 to October 2025, the Ministry of Information, the Access to Information Commission and civil society organisations, organised a series of training workshops on access to information law, in line with the provisions of the Roadmap. These training workshops targeted senior Government officials, Information Officers,[32] journalists[33] and members of civil society organisations.[34] The purpose of these training workshops was to raise awareness among government officials, members of the civil society organisations and members of the public on the Access to Information Act, particularly on the use of the law, for effective implementation and enforcement. On August 26 2025, the stakeholders validated the Access to Information Regulations 2025.[35] The Regulations were made in furtherance of the provisions of the ATI 2021. It seeks to operationalise the provisions of the Act, particularly on matters of reproduction fees; forms used to request information from public bodies; mode of transferring request for information, among other matters. The validation of the Regulations is a step towards the enactment of the same after Cabinet and parliamentary approvals.

Despite the developments registered in 2025, there is failure by the government to proactively disclose and disseminate information using digital technologies. During the course of this research, it was noted that most government institutions do not have functional websites. This includes the government printing house, Gambia Printing Publishing Corporation. Even those institutions that have functional websites do not proactively disclose and disseminate the information required to be published under Section 7 of the ATI 2021. For example, the website of PURA does not have information on the number of reported internet disruptions from January to December 2025; the cost of internet data, among others. This is also the case for MoCDE. Government institutions also fail to respond to access

30. Paradigm Initiative, Muhammed B. Sowe 'Londa 2024 Digital Rights and Inclusion in Africa Report-The Gambia' (2025) https://paradigmhq.org/wp-content/uploads/2025/09/Londa-24-Gambia.pdf (accessed 9 November 2025).
31. The Gambia News Agency 'Access to Information Law Implementation Roadmap Validated' (2025) https://gamna.gov.gm/access-information-law-implementation-roadmap-validated (Accessed 9 November 2025).
32. Gambia Press Union 'GPU engages Government Information Officers on ATI, Document Management Practices' (2025) https://gpu.gm/gpu-engages-government-information-officers-on-ati-document-management-practices/ (Accessed 9 November 2025).
33. Gambia Press Union 'GPU Concludes Training of 100 Journalists on Open Space Investigations, Use of ATI law' (2025) https://gpu.gm/gpu-concludes-training-of-100-journalists-on-open-source-investigations-use-of-ati-law/#:~:text=GPU%20Concludes%20Training%20of%20100,Investigations%2C%20Use%20of%20ATI%20Law (Accessed 9 November 2025).
34. The Point Newspaper 'Civil Society organisations trained on Access to Information Law' (2025) https://thepoint.gm/africa/gambia/national-news/civil-society-organisations-trained-on-access-to-information-law#google_vignette (Accessed 9 November 2025).
35. Paradise TV 'The Ministry of Information, Media and Broadcasting Services in The Gambia recently organized a validation workshop to validate draft regulations for Access to Information Law, implementation Plan and Roadmap'(2025) https://www.facebook.com/watch/?v=1424154218876081&_rdc=1&_rdr# (Accessed 9 November 2025)

to information requests, and even when they responded, they did well outside of the 21 days prescribed period in the Act. Furthermore, the Access to Information Commission also takes a considerable amount of time to determine appeals arising from access to information requests. These defects highlight the need for a comprehensive implementation of the ATI 2021. It also requires the government to put in place the necessary structure and infrastructure to facilitate timely disclosure and dissemination of information to the public. Collectively, these failures indicate that access to information in The Gambia remains largely reactive rather than proactive, undermining Principle 29 of the Declaration.

Censorship and Content Removal; self-censorship and arrest and prosecution

There are no publicly reported incidents of censorship and content removal by the State during the period under review. Notwithstanding, in March 2025, the Gambia enacted the Criminal Offenses Act 2025 with provisions on sedition and false publication and broadcasting that have already been used to harass and intimidate journalists into self-censorship.[36] This is because these laws pressure individuals, journalists and activists to avoid publishing information that might be critical of the authorities or deemed controversial, for fear of legal penalties, imprisonment, or financial ruin.

As regards the arrest and prosecution for online speeches, Abdoulie Sanyang, an ex-soldier, was arrested on August 17 2025 at the Banjul International Airport as he was boarding to leave for Switzerland.[37] Mr. Sanyang was arrested over comments he made on August 14 2025, over West Coast Radio when he accused President Adama Barrow of electoral malpractices in the 2021 Presidential elections. Video and audio excerpts of Mr. Sanyang's interview were amplified online, especially on Facebook and WhatsApp platforms. The wide circulation of the audio and videos appears to have triggered the State to arrest Mr. Sanyang. The arrest was met with outrage by Gambians on Facebook. There was a public debate online that the electoral malpractices in the 2021 Presidential elections was no secret as members of President Barrow's political party have themselves admitted these facts. It has been also argued that members of the opposition, particularly the United Democratic Party, have talked about the electoral malpractices when they filed a case before the Supreme Court of The Gambia, albeit dismissed on a technical ground. The majority of the views shows that the arrest, detention and subsequent prosecution of Mr. Sanyang for sedition is in violation of the constitutional right to freedom of expression enshrined in Section 25 of the Constitution of The Gambia 1997. The Government is accused of using repressive and draconian laws to silence citizens, including journalists, activists and social and political commentators .

Gendered Disinformation

Gendered disinformation remains a persistent issue in The Gambia.[38] During the period under review, gendered disinformation was prevalent in public debates and discussions on women's rights issues, particularly on their political participation and Female Genital Mutilation (FGM).

36. Media Foundation for West Africa 'Gambia Press Union challenges government over laws limiting press freedom' (2025) https://mfwa.org/partner-highlights/gambia-gpu-press-freedom-laws-2025-2/ (Accessed 13 November 2025).

37. The Fatu Network 'Ex-Soldier Abdoulie Sanyang Arrested After Controversial Claims on Coup and Elections' (2025) https://fatunetwork.net/ex-soldier-abdoulie-sanyang-arrested-after-controversial-claims-on-coup-and-elections/ (Accessed 31 December 2025).

38. The Point Newspaper 'Study exposes, fear, harassment as barriers facing women in politics' (2025) https://thepoint.gm/africa/gambia/headlines/study-exposes-fear-harassment-as-barriers-facing-women-in-politics (Accessed 31st December 2025).

These issues attract disinformation because of strong cultural and religious resistance where traditional values and religious interpretations are used to restrict women's roles in the society. This results in resistance to women's advancement. Thus, disinformation is used as a tool of technology-facilitated gender-based violence against women to enforce their silence on matters of public importance. This is done with a view to discourage women from partaking in political and public life of the country. For example, there was an increased online violence against women, journalists and human rights activists who raised their opposition to FGM.[39] Even though FGM is banned in The Gambia as stated in the Women's' Act 2010, the practice remains highly prevalent. Recent statistics shows that 72.6% of women aged 15-49 have undergone FMG, while 45.7% of the same age group supports the continuation of the practice despite the ban.[40] A section of the Muslim population who believe that FMG is a religious obligation, continue to challenge the authorities and remain defiant to carry on the practice. According to the BBC, online bullying, harassment and violence intensified against women and women organisations that advocate against FMG after the death of a one-month-old baby girl because of FGM.[41] It is observed that comments on social media platforms, including Facebook and X, contained attacks against women, journalists and human rights activists who spoke against FGM. Also observed was the prevalence of disinformation about FGM, particularly by the supporters of the practice.

In the political arena, women continue to face bullying and targeted online harassment. This is often the case for women who wish to vie for political positions. This researcher has observed that on social media platforms, particularly Facebook and X, negative and damaging comments were made to target those who declared their intentions to contest for political offices, particularly for the offices of the Presidential and National Assembly. These statements are made to discourage women from taking political positions and eventually get them to withdraw from the race.

Civil society organisations, international bodies and the Government have taken considerable steps to fight against gendered disinformation.[42] This includes the Ministry of Information, InfoCheck and International IDEA. Training and workshops were organized in February, April, August, September, October and December 2025 on matters of disinformation and encouraging women political participation. Nationwide campaigns were undertaken with a view to talk to members of the community about the dangers of disinformation.[43] These trainings addressed disinformation that occurs in online spaces.

Data Protection and Cybersecurity

On September 29 2025, the National Assembly passed the Personal Data Protection and Privacy Bill 2025.[44] In a press release, the Ministry of

39. Askani Gambia 'EFSCRJ Statement on 16 Days of Activism against Gender-Based Violence 2025' (2025) https://askanigambia.com/gambia-efscrj-statement-on-16-days-of-activism-against-gender-based-violence-2025/ (Acessed 31 December 2025).
40. Orchid Project ' Data Updated: FGM/C in The Gambia April 2025' (2025) https://www.fgmcri.org/media/uploads/Country%20Research%20and%20Resources/The%20Gambia/the_gambia_data_update_v1_(april_2025).pdf (Accessed 31 December 2025).
41. British Broadcasting Corporation 'Outrage as baby dies after genital mutilation in The Gambia' (2025) https://www.bbc.com/news/articles/c6200g5d4jlo (Accessed 19 November 2025).
42. The Alkamba Times 'Infocheck Unveils Ambitious 2026-2030 Plan To Combat Disinformation And Empower Gambians https://alkambatimes.com/infocheck-unveils-ambitious-2026-2030-plan-to-combat-disinformation-and-empower-gambians/ (Accessed 19 November 2025); Gambia Daily 'Regional Media Training Launched in Gambia to Tackle Misinformation, Disinformation' (2025) https://gambiadaily.gov.gm/regional-media-training-launched-gambia-tackle-misinformation-disinformation (Accessed 19 November 2025); UNESCO 'Journalists from Gambia, Guinea Bissau trained on open-source intelligence to combat disinformation ' (2025) https://www.unesco.org/en/articles/journalists-gambia-guinea-bissau-trained-open-source-intelligence-combat-disinformation (Accessed 19 November 2025); International IDEA 'National Conference on Women's Political Participation and Representation in The Gambia (2025). https://www.idea.int/events/national-conference-womens-political-participation-and-representation-gambia (Accessed 30 December 2025)
43. Gambia Daily 'Nationwide Campaign against Misinformation, Disinformation Begins' (2025) https://gambiadaily.gov.gm/nationwide-campaign-against-misinformation-disinformation-begins (Accessed 19 November 2025).
44. Block TV News ' National Assembly passes Data Protection and Privacy Bill' (2025) https://blocktvgambia.com/2025/09/30/national-assembly-passes-data-protection-and-privacy-bill/ (Accessed 12 November 2025).

Information, Media and Broadcasting Services described the passing of the law as a "... a major step forward in strengthening the protection of personal data, safeguarding the privacy of citizens, and building trust in The Gambia's digital transformation journey. For the first time, it establishes a comprehensive legal framework dedicated to protecting the personal data and privacy rights of all Gambians."[45] On November 7 2025, the President assented to the Bill. Following the President's assent, the Act was published in The Gambia Gazette contained in G.N. No. 160/2025 dated November 13 2025. It is designated as Act No. 11 of 2025. In terms of Gambian law, the Act came into effect from the date of publication in the Gazette. Although the Personal Data Protection and Privacy Act 2025 entered into force upon gazetting, its enforcement architecture—particulalry staffing, regulations, and public awareness—remains nascent.

The Act establishes core data principles, defines data subject rights, and creates enforcement mechanisms. The provision of the basic principles in the Personal Data Protection and Privacy Act 2025 are important as they form the foundation for data rights. It enables the enforcement of data rights by individuals. They also ensure that individuals have control over data as well as protect their data from misuse. It also creates trust in the people as their data is handled with clear legal bases underpinning all activities. It also ensures accountability for data processors and controllers.

Part 4 of the Act deals with offences. The offences include unlawful processing of personal data; selling personal data; impersonating or falsely pretending to be a data subject; re-identification of personal data; alteration of personal data to prevent disclosure to a data subject; concealment of a personal data security breach; false statements made in response to a notice requesting information; and destruction or falsification of information requested by the Data Commission. The average penalty for violation of the above provisions by an individual is a minimum term of imprisonment of three years, and a minimum fine equivalent to US$6,800. For corporate bodies, the minimum fine is equivalent to US$6,800. The courts are to impose penalties for violation in line with the minimum penalties stated above. Also, the penalties show that the above acts constitute serious offences under Gambia law (felonies) which attract severe penalties. Thus, the purpose of the severity of the penalties is to ensure deterrence.

The Act, in terms of Section 38, empowers the Access to Information Commission to administer the Act and serve as the Data Commissioner. As an independent regulatory body, the Access to Information Commission has the mandate to monitor and ensure compliance with the Act and any regulations and statutory guidance made under it, among other functions. It has the power to investigate, intervene, and enforce the provisions of the Act, as well as impose penalties and fines for non-compliance. The Access to Information Commission was already established under the ATI 2021 prior to the coming into force of the Personal Data Protection and Privacy Act 2025.

From the above, the Personal Data Protection and Privacy Act 2025 contains the key elements of what a data protection law must contain, as outlined in the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention). The Malabo Convention was adopted on June 27 2014, and entered into force in 2023. Although The Gambia signed the Malabo Convention on December 2 2022, it is yet to ratify the same for its domestication. Notwithstanding the non-ratification of the Malabo Convention, The Gambia has, through the Personal Data Protection and Privacy Act 2025, incorporated the basic and core principles of data processing; established the rights of data subjects; obligations of the controllers and processors; established an independent regulatory body that monitors and enforces the law, with powers to impose sanctions for non-compliance, among other matters. Thus, The Gambia made substantial strides in 2025 when it passed into law the Personal Data Protection and Privacy Act 2025, which came into force on November 13 2025.

Cyber security

As stated in the 2024 report, the Cyber

45. Askanwi ' Information Ministry Lauds Parliamentary Approval of Personal Data Protection and Privacy Bill' (2025) https://www.askanwi.com/news/information-ministry-lauds-parliamentry-approval-of-personal-data-protection-and-privacy-bill (Accessed 12 November 2025

Crime Bill 2023 was committed by the Plenary of the National Assembly to the National Assembly Select Committee on Education and Information Communication and Technology (Select Committee) for consideration and scrutiny.[46] Following the referral of the bill to it by the Plenary, the Select Committee undertook consultations with respective stakeholders. The stakeholders include government institutions, civil society organisations and individuals with expertise in cyber security.[47] Some of the key recommendations of the Select Committee include confiscation of the proceeds of crimes relating to child pornography; deletion of vague computer crimes by specifying the acts; judicial oversight for interception of content by law enforcement institutions; extension of the period of preservation of data; criminalisation of child grooming, child solicitation and online human trafficking; criminalisation of recording of private conversation without prior notice; criminalization of cyber extortion.

The above indicates that the Cyber Crime Bill 2023 has gone through thorough consultations with stakeholders. The Select Committee has endeavoured to take into account the views of the civil society organisations and individuals experts on cyber security. This is evidence of the collaboration between the National Assembly and civil society organisations in the law making process. Even though some civil society organisations have initially raised concerns about some of the provisions of the bill as having the potential to freedom of expression and digital,[48] the Select Committee has taken into account these concerns in their scrutiny. It has recommended for judicial oversight in the case of interception of data by law enforcement, and the deletion of controversial provisions that have an impact on press freedom, freedom of expression and digital rights. These recommendations have been adopted by the Plenary of the National Assembly. There were strong indications that the bill will be passed into law in December 2025. However, it did not happen by the end of December 2025.

On September 19 2025, the Communication Bill 2025 was published in the Gazette No. 43 GN No. 133/2025 Vol. 142. The Gazetting is the first process in the legislation-making process, and serves as a notice to the public about the intention of the Government to introduce a legislative proposal. This bill seeks to repeal the Information and Communications Act 2009, and provide for the development, effective functioning and regulation of the electronic communications sector, information, media broadcasting and electronic commerce in The Gambia. Sub-part 8 of the Bill deals with cyber security issues. The bill empowers the Minister of Communication and Digital Economy to develop, publish, maintain, and oversee the implementation of a national cybersecurity policy strategy and other related cyber security instruments, as well as develop enforcement measures. The Minister is also mandated to enforce compliance and audit in close cooperation with other stakeholders in the cybersecurity ecosystem. The concentration of cybersecurity powers with the Minister of MoCDE creates several risks, including that decisions of the Minister may align more with political expediency instead of technical best practices. Also, it reduces accountability as overconcentration of power weakens oversight bodies such as the National Assembly from holding the minister accountable for his decisions. Furthermore, ministers as political appointees often have limited expertise on cybersecurity so as to enable them meet with the emerging challenges of the sector.

The Bill proposes the establishment of The Gambia Computer Security and Incident Response Team, tasked with the main responsibility of receiving and assessing reports of cybersecurity incidents and threats from operators of critical infrastructure and other relevant parties. It also proposes the designation and registration of critical information infrastructure essential for national security and the economic and social well-being of citizens. It also outlines duties and obligations of operators of critical information infrastructure, the breach of which is an offence.

46. Paradigm Initiative, Muhammed B Sowe, 'Londa 2024 Digital Rights and Inclusion in Africa Report-The Gambia' (2025) https://paradigmhq.org/wp-content/uploads/2025/09/Londa-24-Gambia.pdf (accessed 9 November 2025).
47. National Assembly of The Gambia 'Draft Report of the National Assembly Select Committee on Education and Information Communication and Technology on the Cyber Crime Bill 2023" (2025).
48. Paradigm Initiative Muhammed B Sowe,'Londa 2024 Digital Rights and Inclusion in Africa Report-The Gambia' (2025) https://paradigmhq.org/wp-content/uploads/2025/09/Londa-24-Gambia.pdf (accessed 9 November 2025).

The Gambia's Digital ID System

The Gambia is part of the ECOWAS National Biometric ID Card scheme for cross-border use meant to promote inter-regional trade and integration.[49] The biometric system in The Gambia extends to passports, alien cards, non-Gambian IDs, residence permits and driving licences. In October 2018, The Gambia initiated the issuance of biometric ID Cards.[50] As a result, the Government has adopted a policy to stop producing and issuing non-biometric ID cards and other documents. The rights implication of The Gambia's policy on biometric ID includes significant privacy and data protection risks; potential for mass surveillance; threat of exclusion; and discrimination.

On March 29 2025, QTV reported that it received information from credible sources that the Government of The Gambia through the Ministry of Interior awarded the National Identity Document Systems and Digital ID Project contract to Margin's ID Group of Ghana.[51] Margins ID Group is contracted to carry out the production of ID cards and other national documents in The Gambia. To date, the Ministry of Interior has not come out to inform the public about the details of the contract signed with Margins ID Group. Like the previous ID Card contracts with Simplex Group, the contract with Margins ID Group is shrouded with secrecy causing civil society organisations to call for transparency.[52] Despite the award of the contract for the production of ID cards and other national documents, Gambians continued to show their displeasure over the slow process of the issuance of ID Cards.

On January 30 2025, The Gambia Immigration Department (GID) announced resumption of the production and issuance of Machine Readable Passports (MRPs). Throughout December 2024 MRPs were not issued. MRPs are issued to Gambians living abroad who cannot access biometric passports. In March 2025, the production and issuances of MRPs stopped because of undisclosed technical challenges. It was not until May 19 2025 that GID announced that the production of Machine Readable Passports (MRPs) had officially resumed. On August 21 2025, GID announced a regional biometric passport mobile enrolment service across 5 regions of The Gambia to ensure accessibility and remove the need to travel from the regions to Banjul to process a passport. This move has facilitated access to national identification documents to people in provincial Gambia, who struggle to obtain these documents.

The failure of the government to produce ID Cards and other national documents within a reasonable time has caused difficulties for thousands of Gambians and non-Gambians who are without ID cards, driving licenses and resident permits. The lack of ID Cards and other documents constitutes a violation of digital rights. This is because it has a negative impact on people's access to digital and non-digital services and fulfilment of rights, thus depriving them of inclusion. It created a barrier to people's access to public service, financial services, SIM registration, travel, social protection, among others. Given the situation, the Government could have resorted to issuing non-biometric ID cards as a temporary measure or an alternative. The provisions of the National Identity Cards Regulations 1993 anticipate the production and issuance of non-biometric ID cards. Additionally, the said Regulation has not been amended to make provision for the issuance of only biometric ID cards by The Gambia Immigration Department. The issuance of non-biometric ID cards is necessary and reasonable in the light of the unavailability of biometric ID cards. This will ensure accessibility of national identification documents to the people.

In June 2025, the President of The Gambia announced Government's plans to integrate the ID cards with an Electronic Civil Registration and Vital Statistics, passport, and other

49. Paradigm Initiative 'Londa 2024 Digital Rights and Include Report in Africa: The Gambia (2024) https://paradigmhq.org/wp-content/uploads/2025/09/Londa-24-Gambia.pdf (Accessed 12 November 2025)
50. United Nations Economic Commission for Africa 'Gambia National Digital Identity Strategy: Strategy Report' (2023)https://www.uneca.org/sites/default/files/TCND/Digital%20ID%20Transformation%20Strategy%20_Gambia%20V_9.pdf (accessed 13 November 2025).
51. QTV 'Sources have confirmed to QTV that a major government National Identity Document Systems and Digital ID project has been awarded to Margins ID Group of Ghana, following a bidding process' (2025) https://web.facebook.com/watch/?v=1984610305282299 (Accessed 31 December 2025)
52. The Point Newspaper 'EFSCRJ demands transparency on issue of passports, national documents' (2025) https://thepoint.gm/africa/gambia/national-news/efscrj-demands-transparency-on-issue-of-passports-national-documents (Accessed 17 November 2025).

identification databases to create a unified digital ID system that is locally designed, built, operated, and managed by government services.[53] According to the President, the purpose of the initiative is to strengthen internal security, and modernise the national identity card management and national security infrastructure. On November 19 2025, the Civil Registration and Vital Statistics Bill, 2025 was presented to the National Assembly for First Reading.[54] This Bill seeks to create and integrate the ID cards with an Electronic Civil Registration and Vital Statistics, passport, and other identification documents. A key provision in the Bill is the protection of data. Section 14 of the Bill requires the Civil Registration Directorate to protect data in its possession and control against loss, unauthorised destruction, access or disclosure. The Civil Registration Directorate must also process personal data in a manner that ensures appropriate security of the personal data.

Even though the adoption of a digital ID system will enhance security and efficient identification for crime prevention, it has the potential for mass surveillance. A biometric system can enable the Government to monitor the movements and actions of individuals as well as profile them. Also, the storage of biometric data can result in violation of the right to privacy especially when it is not properly done. In the event of a data breach, the passports of biometric information cannot be changed, thus creating a permanent risk of identity theft and fraud. Thus, there is the need for the Government to provide further safeguards for the protection of digital rights of people. There is a need for the National Assembly to undertake consultations with more civil society organisations, particularly those who engage in the promotion of digital rights, before passing the Civil Registration and Vital Statistics Bill, 2025. This is necessary to ensure that the principles of data protection are clearly incorporated in the proposed legislation.

53. The Point Newspaper 'Gov't to integrate ID cards with Electronic Civil Registration' (2025) https://thepoint.gm/africa/gambia/headlines/govt-to-integrate-id-cards-with-electronic-civil-registration (Accessed 17 November 2025).
54. National Assembly of The Gambia (2025) https://web.facebook.com/GambiaAssembly/posts/fourth-ordinary-session-of-the-national-assembly-in-the-2025-legislative-year-or/1162797119377826/?_rdc=1&_rdr# (Accessed 30 December 2025).

Privacy and Surveillance

Section [23] of the Constitution guarantees the right to privacy. This provision states that one's right to privacy can only be interfered with in accordance with the law. In the year [2025], there have been no publicly reported incidents of violations of the right to privacy by the State or its agents. Furthermore, there are no publicly reported incidents of government surveillance on private communications for the period under review.

In June 2025, the Government announced plans to install CCTV systems along the major highways and other strategic locations. These will be linked to a traffic management centre for real-time monitoring and law enforcement. The installation of CCTV systems, although important for law enforcement and traffic management, raises serious concerns about broad surveillance, data retention and potential misuse of advanced features like facial recognition which is foreseeable. This is the case especially in the absence of a law or regulation to govern the use of the CCTV systems in public spaces thereby violating privacy rights. Thus, to mitigate the risks, the Government should adopt a clear, legal framework regulating public surveillance, including strict necessity, proportionality, data retention limits, and independent oversight.

Developments in ICT and Emerging Technologies

The Gambia has no legislation on AI and emerging technologies such as blockchain and quantum computing for the period under review. There is a significant impact associated with the absence of legislation on AI and emerging technologies. This includes creating a vacuum gap in the governance. This has the potential to increase risks of algorithmic bias, discrimination, privacy violations

55. Ibid.

and lack of accountability. It also undermines fundamental rights including privacy and autonomy, while also fostering distrust and hindering responsible innovation by leaving developers and users without clear standards and remedies. The impact of such a gap encourages uncontrolled development, allowing autonomous systems to cause harm in critical areas like justice and defence, necessitating urgent calls for global, human rights-focused frameworks to ensure these technologies benefit humanity rather than harm it. Notwithstanding the above, for the first time, the National Digital Economy Master Plan 2023-2033 recognises the need to develop a policy and strategy for promoting AI research, development, adoption, and application.[56] There have not been any developments in the area of AI for 2025.

Digital Inclusion

Digital inclusion of Persons with disabilities (PWDs), women and children

As stated in the 2024 Report, PWDs continue to be marginalised in the decision-making process, including in the use of ICTs for development. [57]The exclusion of PWDs in the decision-making processes in the ICT sector is due to different factors. This includes stigma as a result of cultural and religious beliefs; weak policy implementation; lack of resources; physical and digital accessibility barriers; insufficient consultation during policy design and implementation, which results in exclusion, among others. Despite the adoption of several Information, Communication and Technology (ICT) policies and strategies, 2025 has not witnessed any progress in terms of the inclusion of PWDs, women and children in the development of the ICT sector. This situation yet again presents the need for the inclusion of vulnerable groups in ICT

56. Ministry of Communications and Digital Economy 'National Digital Economy Master Plan 2023-2033' (2025) https://mocde.gov.gm/wp-content/uploads/2023/10/Final-The-Gambia-Digital-Economy-Master-Plan-2023-20233.pdf (Accessed 19 November 2025)
57. Paradigm Initiative 'Londa 2024 Digital Rights and Inclusion in Africa Report-The Gambia' (2025) https://paradigmhq.org/wp-content/uploads/2025/09/Londa-24-Gambia.pdf (accessed 12 November 2025)

development in The Gambia.

In October and December 2024, the Ministry of Communications and Digital Economy developed and validated[58] the Gambia's National Child and Vulnerable Groups Online Protection Policy.[59] The Policy was made as part of the Western Africa Regional Digital Integration Programme. The purpose of the Policy is to ensure a safe, secure and supportive digital environment for all children and vulnerable groups, including women, persons with disabilities and older persons in The Gambia where their rights are protected, their well-being is prioritised, and they are empowered to leverage the full potential of digital technology for sustainable growth and development. It also aims at inclusion of children, women, persons with disabilities and older persons in the digital landscape of The Gambia. The implementation of the policy commenced in 2025. The Government noted that a proposed new legislation on telecommunications will contain provisions requiring regulatory bodies, service providers, and equipment standards are all guided to ensure safe online access for children, balancing freedom of expression with necessary controls.[60]

Digital Inclusion

As at November 26 2025, The Gambia has not established the Universal Service Fund (USF). While the Information and Communications Act 2009 (the ICA) and the Universal Access and Service Policy 2020[61] envisage the establishment of the

58. The Point Newspaper 'Gov't validates policy to protect child & vulnerable groups online' (2024) https://thepoint.gm/africa/gambia/headlines/govt-validates-policy-to-protect-child-and-vulnerable-groups-online (accessed 19 November 2025).
59. Ministry of Communications and Digital Economy 'The Gambia's National Child and Vulnerable Groups Online Protection Policy' (2024) https://mocde.gov.gm/wp-content/uploads/2024/11/Gambia-CVGOP-Policy.docx#:~:text=Introduction%20and%20Background-,The%20Gambia's%20National%20Child%20and%20Vulnerable%20Groups%20Online%20Protection%20Policy,vulnerable%20groups%20as%20a%20strategic (Accessed 19 November 2025)
60. Ministry of Communications and Digital Economy Facebook account https://web.facebook.com/100070229588702/posts/hon-lamin-jabbiwe-have-validated-an-online-protection-policy-for-children-and-vu/824778166539829/?_rdc=1&_rdr# (Accessed on 31 December 2025)
61. Ministry of Communications and Digital Economy 'Universal Access and Service Policy 2020' https://mocde.gov.gm/wp-content/uploads/2023/10/Universal-Access-Service-Policy-2020.pdf (Accessed 19 November 2025).

USF, the same has not been achieved for 15 years since it was introduced in the ICA. The delay in setting up the USF stems from the lack of political will and commitment from the Government of The Gambia. While policies have been developed around USF, the actual setting up of the fund has not happened. The absence of the USF continues to increase the mobile broadband connectivity gap in The Gambia, like many other African countries.[62] This is because the primary purpose of the USF is to bridge the gap in access to telecommunication connectivity between urban areas with high income and rural areas with low income. This affects access and affordability of telecommunication services by rural areas in The Gambia, as telecommunication service providers do not have access to subsidies provided by USF to provide affordable internet services to the rural population. To close the gap in connectivity in The Gambia, it is important to prioritise the establishment of the USF.

Conclusion

In 2025, The Gambia made some moderate efforts in its digital landscape. The period witnessed considerable increase in the number of internet users by population compared to 2024, as reported by DataReportal's Digital 2025 Report . The data protection law was enacted by the National Assembly, and the Cyber Crime Bill also underwent considerable stakeholders' consultations and scrutiny. The Communications Bill 2025 was introduced to make detailed provisions on cyber security. Despite these efforts, the report highlights the challenges that still exist. The Gambia continues to suffer from internet disruptions occasioned by vandalism, poor speed connectivity and exorbitantly high cost of mobile data due to poor telecommunication infrastructure and technology. Also, The Gambia still maintains laws on sedition and false publication criminalisation despite directions from the ECOWAS Community Court in the case of Federation of African Journalist & 4 Ords v The Gambia ECW/CCJ/JUD/04/18 for these laws to be repealed on the basis that they are a violation of freedom of expression, media freedom and digital rights. The Access to Information Act 2021 is yet to be fully implemented, thus there is absence of proactive disclosure of information by public institutions. These challenges have caused the country to score moderately compliant for the year 2025 based on TheScore Index.

62. GSMA Intelligence 'Universal service funds in Africa Policy reforms to enhance effectiveness' (2023) https://www.gsma.com/about-us/regions/sub-saharan-africa/wp-content/uploads/2023/10/USF-Africa.pdf (Accessed 19 November 2025)

Recommendations

The Government should:

- Invest and develop telecommunication infrastructure so as to enable internet accessibility and limit the cause of internet disruptions and slow internet connection.
- Increase the national budget allocation for ICT research and development in order to meet the need to improve and develop the telecommunication infrastructure
- Establish and operationalise the Universal Service Fund to address affordability gaps, particularly for rural communities and marginalised groups.
- Prioritise the repealing of all laws that impede freedom of expression and the media as directed by the ECOWAS Community Court of Justice in the case of Federation of African Journalist & 4 Ors v The Gambia ECW/CCJ/JUD/04/18.
- Fully implement the Access to Information Act 2021 so as to ensure proactive disclosure and dissemination of information to the public.
- Promote and ensure the inclusion and participation of vulnerable

groups in the formulation of policies and ICT developments.
- Resort to issuing non-biometric ID cards as a temporary measure or an alternative in the event of a breakdown in the issuance of biometric ID cards.
- Adopt laws, regulations and clear guidelines which govern the use of face recognition technologies and surveillance including CCTVs in major public spaces.

The Media should:

- Work with civil society organisations (CSOs) to raise public awareness on digital rights in The Gambia.
- Engage the Government and the National Assembly to repeal all the laws that affect freedom of expression and of the media.
- Engage the Government on the implementation of the Access to Information Act 2021.
- Engage the Government on the harassment and intimidation of journalists and media personnel.
- Undertake public interest litigation on behalf of journalists who are subject to harassment or intimidation by the Government, and/or provide legal support to journalists in conflict with the Government.

The National Assembly should:

- Engage and consider views of members of the media and CSOs on the Cyber Crime Bill 2023 and so as to remove provisions that threaten digital rights and freedom of expression.
- Prioritise passing the Cyber Crime Bill 2023.

Civil Society Organisations should:

- Engage and lobby members of the National Assembly to pass the Cyber Crime Bill 2023 by taking into account the concerns raised by CSOs and to incorporate provisions that meet international standards.
- Undertake public awareness programs on freedom of expression and of the media as well as digital rights.
- Continue to advocate for independence of the media, freedom of expression and digital rights.
- Engage members of the National Assembly and Ministry of Justice for the repealing of laws on sedition and all other laws that hinder freedom of expression and digital rights in the Gambia.

The private section should:

- Comply with data protection standards prescribed in the Personal Data Protection and Privacy Act 2025 by ensuring that data is processed lawfully, transparently and safely.
- Partner with the Government and CSOs to organise digital literacy training and awareness programs.
- Actively participate in digital forum platforms and dialogues with a view to align business practices with human rights standards on data protection and privacy,.
- Invest and promote affordable digital payment systems to enable rural population and small businesses to participate in the formal digital economy.

The Score Index

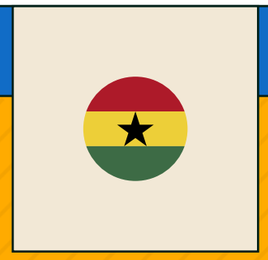
Gambia, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	5	5	Since January 2017, the Government of The Gambia has not shut down any social media platforms.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	4	4	Laws in The Gambia such as Persons with Disabilities Act 2021 that promotes the inclusion of vulnerable groups such as persons with disabilities in national development initiatives including ICT development. Similarly, The Gambia has adopted several policies including the Digital Transformation Strategy for The Gambia 2023-2028 and the National Digital Economy Master Plan 2023-2032 that speak to the promotion of affordability and accessible internet to marginalised and vulnerable groups. Notwithstanding the law and policies, the period under review has not shown any progress in the promotion and inclusion of marginalised groups to affordable internet access.
False News Criminalisation	P22(2)	1	1	Section 152 of the Criminal Offences Act 2025 criminalises false publication and broadcasting
Sedition Legislation	P22(2)	1	1	Sections 45 and 54 of the Criminal Offences Act 2025 criminalises inciting a member of the armed forces or the police force to sedition, and seditious enterprise. August 21 2025, one Abdoulie Sanyang, an ex-member of The Gambia Armed Forces, was charged with seditious intention before the Kanifing Magistrates' Court
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	There was intimidation of journalists particularly when in March 2025 the Minister of Information summoned the Editor in Chief of The Voice Newspaper; the Media Council; and the Newspaper Publishers Association. The summon was in connection to a report in The Voice Newspaper about a survey conducted by a local CSO in The Gambia. Comments by the President accusing the media of reporting false news and having the intention of promoting conflict and instability in the country. On August 21 2025, one Abdoulie Sanyang, was arrested and charged for comments made over a talk show on West Coast Radio when he accused President Adama Barrow of electoral malpractices in the 2021 Presidential elections.
Data Protection Legislation.	P42	2	3	On September 29 2025, the National Assembly enacted the Personal Data Protection and Privacy Act 2025. On November 7 2025, the President as-

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
				sented to the Bill, which comments its entry into force.
Online Content Removal Without Process	P38 and P39(4)	5	5	There is no reported incident in 2025 where the Gambian government interfered and required the removal of online content by internet intermediaries.
Online Content Removal Without Process	P38 and P39(4)	5	5	There is no reported incident in 2025 where the Gambian government interfered and required the removal of online content by internet intermediaries.
Invasion of Privacy of Communications	P41	4	4	There is no reported incident in 2025 where there was invasion of privacy of communications. However, the Cyber Crime Bill 2023, which is currently being considered by the National Assembly, contains provisions that have the potential to enable invasion of privacy of communications.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	2	2	The websites of most government institutions do not comply with the Access to Information Act 2021 by proactively disclosing and disseminating information.
AI and Emerging Technolo	P39(6)	1	2	National Digital Economy Master Plan 2023-2033 recognises the need to develop a policy and strategy for promot

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
gies national strategies				ing AI research, development, adoption, and application. Thus, there is an attempt and recognition to develop policies.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	4	4	The Gambia has developed The Gambia's National Child and Vulnerable Groups Online Protection Policy since October 2024. The aim of this policy is to promote and ensure a safe, secure and supportive digital environment for all children and vulnerable groups including women, persons with disabilities and older persons in The Gambia.
Digital Inclusion	P37(3)	1	2	The Gambia commenced the implementation of the National Child and Vulnerable Groups Online Protection Policy, which seeks the inclusion of children, women, persons with disabilities and older persons in the digital landscape of The Gambia.
Total (out of 60):		2024: **31**	2025 **34**	



Ghana

By Selassie Tay

Executive Summary

This report examines developments within Ghana's communication and mass media subsector in 2025. It focuses on themes that can be broadly classified under digital rights, human rights, and press freedom. Employing a multi-faceted approach, the report evaluates Ghana's performance in digital inclusion, internet access, freedom of expression, data protection and privacy, access to information, censorship and content moderation, and artificial intelligence and emerging technologies. It assesses Ghana's compliance with international standards by utilising The Score Index, a digital rights index developed by Paradigm Initiative, which evaluates state adherence to key human rights principles as outlined in the African Commission on Human and Peoples' Rights' Declaration of Principles on Freedom of Expression and Access to Information in Africa. Effective laws and targeted initiatives have bolstered Ghana's ICT progress over the year, putting the country in good standing on various indices. Challenges, however, remain with press freedom, digital divide, data protection, and cybersecurity. Robust regulatory frameworks, along with strategic collaboration among government entities, civil society organisations, and the private sector, are essential for enhancing technology access and protecting digital rights.

Introduction

Liberalisation of Ghana's ICT sector in 1994 has been key in developing infrastructure and boosting the country's competitiveness among its regional peers. As of 2025, the industry was valued at about 1.5 billion Ghanaian cedis, approximately US$136 million annually, with steady growth expectations.[1] The country now has six subsea cables[2] with a reported cumulative bandwidth capacity of about 7.16 terabytes, positioning Ghana as a potential ICT-enabled Services hub in West Africa.[3] A clear set of laws, policies, and targeted projects focused on specific goals has helped the country achieve significant progress in its ICT sector. The Ghana Digital Acceleration Project, which secured US$15.77 million in disbursements in March 2024,[4] is one of the key infrastructure projects currently ongoing to expand and improve both national and international connectivity. Another noteworthy initiative is the Next Gen InfraCo (NGIC) 5G Network, a public-private partnership launched in mid-2024 to develop Africa's first shared, neutral host 4G/5G mobile broadband infrastructure. This initiative aims for complete digital coverage by 2030, with plans to deploy 4,400 sites and serve 37 million customers by 2028.[5] As of 2025, NGIC has deployed only 16 5G-ready sites and received full NCA approval for its core network infrastructure. These milestones reflect meaningful progress

1. Ghana - Information and Communications Technology (2025) https://www.trade.gov/country-commercial-guides/ghana-information-and-communications-technology-ict (Accessed on 30 November 2025).
2. Briefing By The Minister For Communications And Digitalisation To Parliament On Internet Disruption In Ghana As A Result Of The Damage To Submarine Cables (2024) https://moc.gov.gh/wp-content/uploads/2023/03/Briefing-on-Submarine-Cable-Disruptions-2-1.pdf (Accessed on 30 November 2025)
3. Ghana's Information Communication Technology Sector (2019) https://www.ecexportsymposium.co.za/wp-content/uploads/2020/06/ICT-SECTOR-PROFILE-2019.pdf (Accessed on 13 November 2024)
4. Ghana - Digital Acceleration Project (2025) https://documents.worldbank.org/en/publication/documents-reports/documentdetail/938111649959522167/ghana-digital-acceleration-project
5. Government Launches Next-Gen Infraco For 5g Deployment In Ghana (2024) https://moc.gov.gh/2024/06/03/government-launches-next-gen-infraco-for-5g-deployment-in-ghana/ (Accessed on 30 November 2025)

following earlier delays in 2024.[6] Ghana appears to be doing better amongst its regional peers, having scored 66.2 out of 100 on the 2024 ICT Development Index, surpassing Nigeria and the Ivory Coast, which scored 46.9 and 65.3, respectively.[7] It also ranked fifth within Africa on the 2023 Network Readiness Index (NRI), outperforming its region in each of the four pillars of the index.[8]

The liberalisation of the ICT sector, following the constitutional changes with the enactment of the 1992 constitution, has also significantly influenced the growth of the mass media landscape. As of 2025, there were a total of 176 TV stations[9] and 768 FM radio stations[10] licensed to operate in Ghana. Before 1993, there were only one TV and one radio station in Ghana. This feat couldn't have been achieved without the combination of technological advancement and a favourable legal and policy environment. There appears to have been a symbiotic relationship between the gradual growth of Ghana's democratic ethos and the expansion of the Ghanaian media landscape, as may have been expected by the framers of the 1992 Constitution.[11] Article 12 of the Constitution guarantees press freedom and provides guidelines for responsible journalism by stipulating a right to rejoinders.[12] The Criminal Libel Law, which had restricted press freedom and criminalised free speech for over a century, has been repealed.[13] Nonetheless, Section 208 of the Criminal Offences Act (Act 29) and the Electronic Communications Act (Act 775) are two laws that still impede press freedom.

Despite the good rankings in related global indices, Ghana still faces some challenges in the ICT and mass media landscape. In the Londa 2024 report on Ghana, press freedom and online expression were reported as declining. An existing digital divide, shown by differences in service quality, access to digital technologies, and digital skills among various population groups, was also reported. Data protection, privacy, and cybersecurity concerns were noted as needing careful consideration and proactive solutions to keep up with the changing technology landscape.

Internet Access

As of 2025, Ghana had a total of 38.3 million active cellular connections, representing a mobile phone penetration rate of 120%. On average, individuals possess more than one cellular connection, reflecting the growing reliance on mobile technology in daily life. Among connected devices, smartphones accounted for 58%, feature phones for 26%, and basic phones for 16%.[14] Mobile internet penetration reached approximately 70%, with around 24.3 million internet users, predominantly in urban areas, making Ghana the ninth country with the most internet users in Africa. This represents an increase of approximately 9% from 2024. Most new internet users are mobile-first, as many have never used a desktop or laptop computer.[15]

6. Q2 Sectorial Briefing By The Honourable Minister For Communication, Digital Technology & Innovation (2025) https://moc.gov.gh/wp-content/uploads/2023/03/Q2-Briefing-MoCDTI-_2-July.pdf (Accessed on 09 December 2025)
7. Measuring digital development - The ICT Development Index (2024) https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2024-3-pdf-e.pdf (Accessed on 12 November 2024)
8. Network Readiness Index (2023) https://download.networkreadinessindex.org/reports/countries/2023/ghana.pdf (Accessed on 30 November 2025)
9. List of Authorised TV Broadcasting Stations as at Third Quarter (2025) https://nca.org.gh/television/ (Accessed on 30 November 2025)
10. Authorised VHF-FM Radio Stations as at Third Quarter (2025) https://nca.org.gh/authorised-radio/ (Accessed on 30 November 2025)
11. Changes in Ghana's media landscape over 30 years (2023) https://ifex.org/changes-in-ghanas-media-landscape-over-30-years/ (Accessed on 30 November 2025)
12. Regulatory Framework of the Media in Ghana (2017) https://philipatawura.wordpress.com/2017/05/02/regulatory-framework-of-the-media-in-ghana/ (Accessed on 14 November 2024)
13. The Ghanaian Media Landscape: How unethical practices of journalists undermine progress (2012) https://ghana.mom-gmr.org/uploads/tx_lfrogmom/documents/18-476_import.pdf (Accessed on 14 November 2024)
14. Quarterly Statistical Bulletin On Bulletin On Communications In Ghana Communications In Ghana (2025) https://nca.org.gh/wp-content/uploads/2025/07/Q1-2025-Statistical-Bulthe US$1.17letin.pdf (Accessed on 02 December 2025)
15. Internet Users in Ghana Accelerates to 26 Million — But Millions Still Rof emain Offline (2025) https://labarijournal.com/internet-users-in-ghana-accelerates-to-26-million-but-millions-still-remain-offline/ (Accessed on 03 December 2025)

There are 7.95 million social media users, representing 23% of the total population.[16] This group spends an average of three hours and 23 minutes on social media daily, making Ghana the sixth country globally with the highest social media usage and third in Africa.[17] Facebook and YouTube have the most users.[18]

There are three mobile network operators, three fixed network operators, and one broadband wireless access provider. MTN Ghana and Telecel hold the largest market shares, exceeding 70% combined.[19] Market competitiveness for internet customers and end users is very poor.[20] Ghana ranked number one on the list of countries in Africa with the most expensive internet, at $2.58 per Mbps.[21] A few providers control most of the country's fibre backbone, leading to high wholesale rates that smaller Internet Service Providers (ISPs) must pass on to consumers.[22] Nonetheless, mobile internet data is relatively cheaper. Recently, the sector Minister announced a 10% minimum increase in data volumes included in mobile internet plans, without any further increase in prices. This, he stated, is part of the government's efforts to accelerate Ghana's digital transformation by facilitating greater access to the Internet via mobile phones.[23] The introduction of 5G technology is also expected to enhance the quality and speed of data services, thereby further increasing internet penetration. To this end, MTN Ghana has announced plans to gradually phase out its 2G and 3G networks, allowing customers ample time to transition to modern technology.[24]

Smartphones are essential for driving internet penetration. Hence, the government must work to make them more affordable. As of 2025, import tax on smartphones is still in place. In 2022, according to the Alliance for Affordable Internet, the cost of a smartphone as a percentage of people's average monthly income in Sub-Saharan Africa is 39%.[25] A low-end smartphone in Ghana costs US$49.90, while higher-end phones can cost over US$325.73. As of 2025, the daily minimum wage in Ghana was US$1.28, up from US$1.17 in the previous year.[26] With the average monthly wage income estimated to be GH¢2,922,[27] approximately US$ 267, a low-end smartphone could take 27% of the average monthly wage income of the vast majority of people who earn wage income in Ghana. It would also cost them US$0.40 per gigabyte to purchase mobile internet data.[28] Ghana is the second and third cheapest country for mobile internet data in West Africa and Africa, respectively.[29] The government is dedicated to enhancing digital literacy

16. Digital 2025: Ghana (2025) https://datareportal.com/reports/digital-2025-ghana (Accessed on 02 December 2025)
17. Internet Usage in Ghana (2024) https://genderanddigital.org/internet-social-media-usage/ (Accessed on 17 November 2024)
18. YouTube and Facebook Have The Most Users in Ghana in 2025 (2025) https://techlabari.com/youtube-and-facebook-have-the-most-users-in-ghana-in-2025/ (Accessed on 03 December 2025)
19. Global Perspectives on Ghana Telecom Market Growth: 2025-2033 Insights (2025) https://www.marketreportanalytics.com/reports/ghana-telecom-market-90137#summary (Accessed on 02 December 2025)
20. Ghana report (2025) https://pulse.internetsociety.org/en/reports/GH/ (Accessed on 02 December 2025)
21. African countries with the most expensive internet in 2025 (2025) https://africa.businessinsider.com/local/lifestyle/african-countries-with-the-most-expensive-internet-in-2025/j7w09dx (Accessed on 02 December 2025)
22. Why Is Ghana's Internet Still So Expensive in 2025? (2025) https://thehighstreetjournal.com/why-is-ghanas-internet-still-so-expensive-in-2025/ (Accessed on 02 December 2025)
23. Ghana announces increased internet volumes from July 1 (2025) https://extensia.tech/ghana-announces-increased-internet-volumes-from-july-1/ (Accessed on 01 December 2025)
24. MTN Ghana outlines plan to shut down 2G and 3G services (2025) https://www.gbcghanaonline.com/technology/mtn-ghana-outlines-plan/2025/ (Accessed on 03 December 2025)
25. The cost of smartphones falls, but they remain unaffordable for billions, around the world (2022) https://a4ai.org/news/the-cost-of-smartphones-falls-but-they-remain-unaffordable-for-billions-around-the-world (Accessed on 17 November 2024)
26. Ghana's National Daily Minimum Wage increased by 10% for 2025 (2025) https://www.graphic.com.gh/business/business-news/ghanas-national-daily-minimum-wage-increased-by-10-for-2025.html (Accessed on 03 December 2025)
27. Navigating Inflation: Impacts of the Cost-of-Living Crisis on Workers in Informal Employment in Accra, Ghana (2024) https://www.wiego.org/resources/navigating-inflation-impacts-cost-living-crisis-workers-informal-employment-accra-ghana (Accessed on 17 November 2024)
28. Top 20 Countries With The Cheapest Mobile Data Prices in Africa (2025) https://talkafricana.com/african-countries-with-the-cheapest-mobile-data-prices/ (Accessed on 03 December 2025)
29. Mobile data price in Ghana third cheapest in Africa, second in West Africa (2024) https://www.modernghana.com/news/1328926/mobile-data-price-in-ghana-third-cheapest-in-afric.html (Accessed on 17 November 2024

and digital inclusion by providing affordable mobile data for all. A report by GSMA projects this could result in the expansion of mobile internet adoption to 20.6 million unique users by 2029.[30]

Internet shutdowns and outages are uncommon in Ghana. There are currently no government restrictions on internet access and no reported cases of governmental censorship and monitoring of emails or internet chat rooms without judicial oversight. This can be attributed to several factors, including available laws, political will, and efforts by civil society organisations. No internet shutdown was recorded in 2025, although the sector Minister is said to have contemplated a temporary nationwide internet shutdown to halt the circulation of disturbing videos following the August 6 helicopter crash involving key government officials.[31]

According to the 2025 Freedom on the Net Index published by Freedom House, Ghana's internet freedom is classified as "partly free," receiving a score of 64 out of 100,[32] having dropped one point from the previous year. This indicates a moderate level of digital rights and online accessibility, reflecting the positive aspects and challenges in the country's digital landscape. Quality of service is a concern for the segment of the population with access to the Internet.

As of the third quarter of 2025, MTN provided the fastest mobile internet in Ghana with an average download speed of 21,3 Mbs. The highest data upload speed was recorded with MTN at 13,5 Mbs. The lowest ping was observed with Telecel at 134 milliseconds. During the same period, the fastest broadband internet in Ghana was provided by Starlink with an average download speed of 81.2 Mbs. Ghana ranked 130th globally and 19th in Sub-Saharan Africa on the 2025 (3rd quarter) Global Network Excellence Index.[33]

MTN continues to be a significant market player among mobile network operators in Ghana, with a 75% market share. Telecel is a significant market player for fixed network operators, with a 73% market share.[34] This has raised concerns about preserving fair competition, encouraging innovation, and protecting consumer rights. Although the government introduced a technology neutrality policy as a step towards addressing the market imbalances and enhancing consumer choice in the telecommunications sector,[35] the impact of this on the market is yet to be assessed.

Schedule 2 of the National Communications (Quality of Service) Regulations, 2016 establishes the benchmark parameters that every cellular mobile service provider must meet.[36] In cases of non-compliance with the set service quality indicators, the regulator penalises the industry player in breach. There were no reported cases of penalties against any of the telecommunication companies for the under review. That notwithstanding, the government has issued a strong warning of fines and sanctions if they fail to improve service quality by the end of the year.[37] To strengthen the regulator and modernise the regulatory and institutional framework for Ghana's

30. Digital Reforms Could Add US$3.4 Billion to Ghana's Economy by 2030 (2025) https://www.newsghana.com.gh/digital-reforms-could-add-us3-4-billion-to-ghanas-economy-by-2030/ (Accessed on 08 December 2025)
31. Minister weighed temporary internet blackout to curb spread of horrific helicopter crash videos (2025) https://www.myjoyonline.com/minister-weighed-temporary-internet-blackout-to-curb-spread-of-horrific-helicopter-crash-videos/ (Accessed on 03 December 2025)
32. Freedom on the Net (2025) https://freedomhouse.org/country/ghana/freedom-net/2025 (Accessed on 03 December 2025)
33. Global Network Excellence Index - Q3 2025 update (2025) https://insights.opensignal.com/2025/10/21/global-network-excellence-index-q3-2025-update/dt (Accessed on 08 December 2025)
34. Industry Market Statistics (2023) https://nca.org.gh/wp-content/uploads/2023/04/Mobile-Data-Year-ended-2022-Jan-2023.pdf (Accessed on 20 November 2024)
35. NCA Introduces Technology Neutrality in Ghana (2023) https://nca.org.gh/2023/07/18/nca-introduces-technology-neutrality-in-ghana/ (Accessed on 20 November 2024)
36. The National Communications (Quality Of Service) Regulations, (2016) https://nca.org.gh/wp-content/uploads/2021/11/Draft-QoS-Regulations-April-2016.pdf (Accessed on 17 November 2024)
37. Improve service quality by December or face heavy fines – Sam George warns Telcos (2025) https://citinewsroom.com/2025/05/improve-service-quality-by-december-or-face-heavy-fines-sam-george-warns-telcos (Accessed on 03 December 2025)

communications sector, the government has begun the process of amending the National Communications Authority Act (Act 769, 2008).[38]

Freedom Of Expression

Ghana's Constitution guarantees freedom of speech and the freedom and independence of the media, as outlined in Chapters 5 and 12. Nonetheless, there are still laws being used to harass, arrest, and incarcerate journalists in Ghana. These are Section 208 of the amended Criminal and Offences Act (Act 29) and the Electronic Communications Act (Act 775).[39] These two laws cover the dissemination of misinformation and disinformation, respectively. They are vague and can be used to criminalise nearly any speech that may be interpreted as inducing fear or alarm.[40] Arguments have also been made about the draconian nature and outdatedness of these laws, as they violate international and national human rights laws concerning freedom of speech.[41] The Government has initiated the process of amending the Electronic Communications Act (Act 775) and promulgating new legislation to address misinformation, disinformation, hate speech, and the publication of other information in the digital space. The general public has been invited to make inputs into these laws.[42] The legislation is expected to establish a clear framework for defining freedom of speech, aimed at preventing the arbitrary arrest, harassment, and assault of journalists. Ghana currently falls into the moderate risk category for disinformation. This is based on its levels of governance, media freedom, and digital penetration. The country received a score of 57% on the 2025 Disinformation Index Report, indicating a relatively strong resilience against disinformation, with a detection rate of 96%. Although detection is high, only 31.2% take the extra step to verify content.[43] Political party propaganda, the legacy media's sacrifice of news accuracy for speed, and the Ghana government's regulatory challenges are the main drivers of the problem of misinformation and disinformation.[44]

There were three reported cases of arrest and interrogation of journalists by law enforcement agencies in 2025. This involved Oheneba Nana Asiedu, a journalist at Wontumi TV;[45] Prosper Agbenyegah, an Editor at Current Issues[46] and Samuel Amadotor, a journalist at Dklassgh.net.[47] Harassment and attacks on journalists by citizens are also prevalent. There were two reported

38. Invitation for Comments – National Communications Authority Bill (2025) https://nca.org.gh/2025/10/16/invitation-for-comments-national-communications-authority-bill/ (Accessed on 03 December 2025)
39. The two laws surviving the repealed criminal libel law in Ghana (2022) https://mfwa.org/issues-in-focus/the-two-laws-surviving-the-repealed-criminal-libel-law-in-ghana (Accessed on 19 November 2024)
40. Ghana's law on publication of false news is vague and easily abused (2022) https://blogs.lse.ac.uk/africaatlse/2022/02/25/ghana-law-publication-of-fake-news-vague-easily-abused-free-speech (Accessed on 19 November 2024)
41. Ghana's law on publication of false news is vague and easily abused – it should go (2022) https://theconversation.com/ghanas-law-on-publication-of-false-news-is-vague-and-easily-abused-it-should-go-177470 (Accessed on 19 November 2024)
42. Ghana extends time for feedback on new laws to regulate tech evolutions and emerging digital areas (2025) https://www.africa-legal.com/news/ghana-extends-time-for-feedback-on-new-laws-to-regulate-tech-evolutions-and-emerging-digital-areas/123829# (Accessed on 03 December 2025)
43. Disinformation Index Report for West Africa (2025) https://penplusbytes.org/wp-content/uploads/2025/10/1st-October-2025-PenPlusBytes-Disinformation-Index-Report-2025.pdf (Accessed on 04 December 2025)
44. Stakeholders identify three main drivers of mis/disinformation in Ghana (2023) https://mfwa.org/issues-in-focus/stakeholders-urge-tech-giants-govt-to-attend-to-mis-disinformation-situation-in-ghana/ (Accessed on 04 December 2025)
45. Ghana: Journalist detained, questioned to disclose source of information (2025) https://mfwa.org/country-highlights/ghana-journalist-detained-questioned-source-disclosure/ (Accessed on 03 December 2025)
46. Ghana's National Security Secretariat interrogates newspaper editor over "leaked" document story (2025) https://mfwa.org/country-highlights/ghana-journalist-interrogated-over-publication/ (Accessed on 03 December 2025)
47. Police under fire over arrest and continued detention of journalist (2025) https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Police-under-fire-over-arrest-and-continued-detention-of-journalist-2010381 (Accessed on 03 December 2025)

cases of citizen assault on journalists. This involved Carlos Lorlornyo Atsu Calony[48] and Latif Iddrisu,[49] both journalists at JoyNews. During this year, Daniel Owuusu Karanteng, a suspect in the murder of Ahmed Suale, was identified, arrested, and arranged before court[50] From 2019 to 2025, at least 36 Ghanaian journalists and media workers have faced arrests, assault, and threats in connection with their work. In 2025 alone, at least 18 journalists have been physically or verbally assaulted[51] As of the time of this report, no outcomes have been reported regarding the judicial prosecution of the perpetrators of these assaults against journalists. Without proper safety measures, the neutrality of news is jeopardised. Ghana's position on the Global Press Freedom Index has been steadily declining over the years, from 23rd in 2018, to 60th in 2022, 62nd in 2023, and finally 50th in 2024.[52] As of 2025, Ghana ranked 52nd on the Global Press Freedom Index.[53] On the 2025 Freedom in the World Index, it scored 80 out of 100[54] This shows that Ghana is a relatively open society where everyone is free to express their opinions and beliefs or non-beliefs.

48. Press group urges Ghana to act following assault against journalists (2025) https://www.jurist.org/news/2025/08/press-group-urges-ghana-to-act-following-assault-against-journalists/ (Accessed on 03 December 2025)
49. Ghana: Police arrest suspect involved in assault on journalist (2025) https://mfwa.org/country-highlights/ghana-police-arrest-suspect-assault-joynews-journalist/ (Accessed on 03 December 2025)
50. Ghana: Police arrest a suspect in the murder of journalist Ahmed Suale (2025) https://www.ifj.org/media-centre/news/detail/category/africa/article/ghana-police-arrest-a-suspect-in-the-murder-of-journalist-ahmed-suale (Accessed on 03 December 2025)
51. Investigative Report: 18 Ghanaian journalists attacked between January and July 2025 (2025) https://ghana.dubawa.org/investigative-report-18-ghanaian-journalists-attacked-between-january-and-july-2025/ (Accessed on 05 December 2025)
52. MFWA blames rising violations for Ghana's declining press freedom ranaccountsking (2025) https://citinewsroom.com/2025/11/mfwa-blames-rising-violations-for-ghanas-declining-press-freedom-ranking/ (Accessed on 03 December 2025)
53. Ghana: World Press Freedom Index (2025) https://rsf.org/en/country/ghana (Accessed on 03 December 2025)
54. Freedom in the World 2025 (2025) https://freedomhouse.org/country/ghana/freedom-world/2025 (Accessed on 05 December 2025)

Data Protection and Privacy

As the Internet and technology continue to become more accessible to Ghanaians, the importance of data protection and privacy cannot be overstated. The Data Protection and Privacy Act, 2012 (Act 843), provides the necessary guardrails as Ghana's primary legislation governing privacy and data protection. There are other legal instruments with privacy and data protection provisions.[55] The Constitution, the Electronic Communications Act 2008 (Act 775), and the Cybersecurity Act (2020) (Act 1038). Article 18(2) of the 1992 Constitution enshrines citizens' fundamental privacy rights. Clauses 8 (1) and 8 (2) of the Electronic Communications Act, 2008 (Act 775) preserve the data privacy of the service users. While these laws safeguard citizens' data and privacy, there are exceptions. The right to privacy may be restricted by the law when necessary for the safety and economic well-being of the country, the protection of health or morals, the prevention of disorder or crime, or the protection of the rights and freedoms of others. The judiciary ensures strict and impartial adherence to these legal instruments. In a landmark case in 2024, the court ruled that Executive Instrument (E.I) 63 was illegal and instructed the government to delete all data collected using this instrument.[56]

Data breaches are a significant issue in Ghana. As of the third quarter of 2025, the country recorded an average of 15 data breaches for every 100 Ghanaians, ranking Ghana ninety-third globally, with over 5.3 million breached accounts since 2004 to date.[57] This year, MTN

55. Data Protection Laws of the World: Ghana 2024) (https://www.dlapiperdataprotection.com/index.html?t=law&c=GH (Accessed on November 2024)
56. Ghana: MFWA welcomes high court ruling ordering government to stop collecting personal data (2021) https://mfwa.org/ghana-mfwas-welcome-high-court-ruling-ordering-government-to-stop-collecting-personal-data/ (Accessed on 22 November 2024)
57. Global data breach statistics - Ghana (2025) https://surfshark.com/research/data-breach-monitoring (Accessed on 23 November 2024)

Ghana suffered a major data breach that impacted 5,700 customers, raising concerns about whether regulators are effectively enforcing data protection regulations.[58] Following this, the Ghana Data Protection Commission launched its 'Privacy Awareness' campaign to educate data subjects and data controllers about their rights and obligations under the Data Protection Act 2012[59] There has been no public reporting of the outcome, if any, of the probe launched into the MTN data breach incident by the sector ministry and regulators.[60] It reported that data from 35 institutions in Ghana—including ministries, regulatory agencies, banks, hospitals, and universities—were found circulating on the dark web, posing risks of privacy breaches and potential national-level compromises.[61]

Recent data breaches may indicate a lack of effective cybersecurity measures. Ghana has seen a significant increase in cybercrime, resulting in approximately US$1.8 million loss in the first nine months of 2025. This represents a 17% rise compared to the same period in 2024.[62] Reported cybercrime incidents increased from 1,317 in early 2024 to 2,008 in 2025, with online fraud, cyberbullying, and blackmail accounting for the majority of cases.[63] By way of distribution, online fraud constituted 36%, while cyberbullying constituted 25%. The percentages for the remaining categories are as follows: blackmail at 14%, unauthorised access at 12%, and information disclosure at 9%.[64] Cyberbullying has become increasingly common, especially on social media platforms. The anonymity of online interactions largely contributes to this trend. By integrating the Cybersecurity Act of 2020 (Act 1038) with the Data Protection Act of 2012 (Act 843), the Cyber Security Authority is establishing a framework that includes awareness campaigns, educational programs, and guidelines for responsible online behaviour.[65]

The Cybersecurity Authority runs awareness campaigns every year to educate citizens. This year's campaign, themed "Building a Safe, Informed, and Accountable Digital Space," aims to counter misinformation and deepfake manipulation while promoting responsibility among citizens and institutions.[66] Law enforcement agencies have not been left out in the fight against cybercrimes. A Joint Cyber Security Committee, working closely with international security agencies, exists to protect Ghana's digital economy. This year, a major INTERPOL operation across 14 African countries has resulted in the arrest of 260 suspected scammers, with Ghanaian authorities arresting 68 individuals and seizing significant evidence.[67] The Cybersecurity Act is being reviewed to greatly expand the powers of the Cybersecurity Authority to effectively

58. MTN Ghana Data Breach: A Wake-Up Call for Privacy Rights and Corporate Accountability (2025) https://www.modernghana.com/news/1396072/mtn-ghana-data-breach-a-wake-up-call-for-privacy.html (Accessed on 04 December 2025)
59. The Data Protection Commission Launches Public Awareness Campaign (2025) https://dataprotection.org.gh/the-data-protection-commission-launches-public-awareness-campaign/ (Accessed on 04 December 2025)
60. Communication Ministry probes cybersecurity breach affecting 5,700 MTN users (2025) https://www.gbcghana-online.com/general-news/communication-ministry-probes-cybersecurity-breach-affecting-5700-mtn-users/2025/ (Accessed on 04 December 2025)
61. GH₵15m lost to cyberfraud in first-half 2025 (2025) https://thebftonline.com/2025/09/09/gh%E2%82%B515m-lost-to-cyberfraud-in-first-half-2025/ (Accessed on 04 December 2025)
62. Ghana faces rising cybercrime costs and incidents in 2025 (2025) https://www.africanwirelesscomms.com/news-details?itemid=9710&post=ghana-faces-rising-cybercrime-costs-and-incidents-in-2025-397234 (Accessed on 05 December 2025)
63. Cybercrime: Ghana's Growing Digital Weak Spot (2025) https://imaniafrica.org/2025/09/cyber-crime-ghanas-growing-digital-weak-spot/ (Accessed on 05 December 2025)
64. Ghana's cybercrime losses in first half of 2025 revealed (2025) https://www.ghanaweb.com/GhanaHomePage/business/Ghana-s-cybercrime-losses-in-first-half-of-2025-revealed-1999119 (Accessed on 05 December 2025)
65. Ghana: Cybersecurity Authority develops a framework to combat cyberbullying among students (2024) https://publicsectormag.net/2024/06/10/ghana-cybersecurity-authority-develops-framework-to-combat-cyberbullying-among-students/ (Accessed on 23 November 2024)
66. Minister Launches 2025 National Cyber Security Awareness Month and Calls for Safer, More Accountable Digital Space (2025) https://moc.gov.gh/2025/09/03/minister-launches-2025-national-cyber-security-awareness-month-and-calls-for-safer-more-accountable-digital-space/ (Accessed on 05 December 2025)
67. 68 scammers arrested in Ghana as INTERPOL dismantles $2.8m African cybercrime ring (2025) https://www.gbcghanaonline.com/general/ghana-interpol-scammers/2025/ (Accessed on 05 December 2025)

combat cybercrimes.

There is currently no legislation in place for data localisation. However, there are indications that the government is working on a framework to ensure local hosting of all data hosted externally.[68] Even though the Data Protection Act does not prescribe specific conditions for cross-border data transfers, data controllers that outsource processing to foreign processors are required to comply with Ghanaian laws, disclose data transfer destinations, and obtain consent from data subjects during registration.[69] As of 2025, Ghana has eight data centres, ranking eighth on the table of African countries with data centres.[70] The drive for the growth of the data centre sector is guided by the Ghana ICT for Accelerated Development Policy and the Ghana Digital Acceleration Project (GDAP), which focuses on infrastructure development. Other key policies include the Enabling Physical Infrastructure (EPI) policy for broadband and the National Information Technology Act 2008, which empowers the National Information Technology Agency (NITA) to regulate the sector. In 2024, the Agency held a public consultation to develop a regulatory framework for data centre services.[71]

Ghana uses mass surveillance technologies. The known contracts with various overseas companies for these technologies total approximately US$184 million. Most of this amount has been allocated to a “Safe City” project that includes a CCTV system powered by facial recognition AI from the Chinese company Huawei. Additionally, several new biometric identification systems require citizens to submit either facial recognition data or fingerprint biometrics.[72] The demand for these technologies has come as a result of the country’s rapid technological development and its focus on national security.[73] The total expenditure on national security for 2025 is not publicly available. Nonetheless, historical data show that the total budget allocation for the Ministry of National Security in 2024 was GH¢ 1.6 billion, approximately US$ 106 million.[74] Government spending on national security accounts for 0.71% of the total budget expenditure for last year. Ghanaians have been encouraged to utilise the Right to Information law to obtain details about the spyware acquired by the government over time.[75] Monitoring and surveillance of journalists is pervasive across West Africa.[76] Ghana is not an exception. Journalists, activists, and ordinary citizens have been tracked, arrested, and detained simply for posting critical messages on social media. Under the guise of national security, governments have exceeded their legal surveillance powers.[77] The amendment to Ghana’s Cybersecurity Act (Act 1038) has sparked considerable debate, with critics warning that it may infringe on fundamental rights by enabling extensive monitoring, which could adversely

68. Government Working To Host All Data Centres Locally (2024) https://moc.gov.gh/2024/06/26/government-working-to-host-all-data-centres-locally/ (Accessed on 04 December 2025)
69. DPA Digital Digest: Ghana (2025) https://digitalpolicyalert.org/digest/dpa-digital-digest-ghana (Accessed on 04 December 2025)
70. Top 10 African Countries by Number of Data Centres (2025) https://www.africanexponent.com/top-10-african-countries-by-number-of-data-centres-2025/ (Accessed on 04 December 2025)
71. Public Consultation on: Regulatory Framework for Data Centre Services (2024) https://www.brr.gov.gh/consultation?cd=MjM= (Accessed on 04 December 2025)
72. Ghana’s democracy at risk due to use of surveillance technology, warns new report (2023) https://www.ids.ac.uk/press-releases/ghanas-democracy-at-risk-due-to-use-of-surveillance-technology-warns-new-report/ (Accessed on 05 December 2025)
73. Surveillance devices in Ghana: Analysing the growing trend and its implications (2025) https://malawifreedom-network.com/2025/02/03/surveillance-devices-in-ghana-analyzing-the-growing-trend-and-its-implications/ (Accesed on 05 December 2025)
74. Programme Based Budget Estimates (2024) https://mofep.gov.gh/sites/default/files/pbb-estimates/2024/2024-PBB-MNS_.pdf (Accessed on 23 November 2024)
75. Ghanaians urged to use RTI law to ask government to disclose information on spyware (2025) https://www.ghanabusinessnews.com/2025/06/02/ghanaians-urged-to-use-rti-law-to-ask-government-to-disclose-information-on-spyware/ (Accessed on 05 December 2025)
76. How Digital Surveillance Threatens Press Freedom In West Africa (2023) https://humanglemedia.com/how-digital-surveillance-threatens-press-freedom-in-west-africa/ (Accessed on 22 November 2024)
77. African Governments Spend Too Much On Surveillance Tech for the Wrong Reasons (2023) https://www.africanliberty.org/2023/11/07/african-governments-spend-so-much-on-surveillance-tech-for-the-wrong-reasons/ (Accessed on 22 November 2024)

affect activists and whistleblowers.[78]

Censorship and content moderation

The media and internet users in Ghana enjoy an information space free from technical censorship. Nonetheless, individuals risk arrest for posts with national security implications, and online journalists face threats of harassment and assaults for their critical reporting. Although the Constitution guarantees free speech and an independent press under Chapter 12, it also provides the basis for derogation from these rights, which enables content moderation. Article 164 permits restrictions on free speech in the interests of public order, morality, or national security.[79] The Electronic Communications Act, 2008 (Act 775), is a key statute that governs content moderation in Ghana. It establishes the legal framework for electronic communications and online platforms. False signalling and False communication are captured respectively as offences under Sections 75 and 76 of the Law.

The rising prevalence of fake news has become a major concern for the government, especially in its efforts to maintain social cohesion among citizens. Some political actors disseminate misinformation using automated tools and paid social media commentators. False information, content manipulation, and plain lies are becoming more prevalent.[80] This issue undermines public trust and the integrity of information, which can lead to social division and the spread of misinformation. A 2024 study revealed that about 64.4% of Ghanaians "ignore" and do nothing to protest or caution others when they see fake news or false information in the media.[81] To address this the government is working to introduce the Misinformation, Disinformation and Hate Speech and Publication of Other Information Act. Currently at the draft stage, the bill, when passed, will promote responsible communication, safeguard national cohesion, and protect citizens from the dangers of disinformation.[82] However, some provisions in their current form pose significant threats to constitutional rights, particularly freedom of expression, media independence, privacy, and due process.[83] These provisions include Sections 68 (4) and 84 (3), Section 30(6) and 31(8), Sections 9, 10, 11 & 12, and Sections 69, 78, & 80 (1). These provisions introduce an unconstitutional licensing regime, broaden the definitions and criminalisation of speech, reverse the burden of proof, enable executive control over enforcement, and foster unaccountability of big tech and digital platforms.

The large number of media outlets in Ghana does not necessarily indicate a pluralistic media landscape, as most media outlets are owned by or affiliated to politicians. Approximately 70% of Ghanaian media houses are owned by politicians.[84] This significantly influences editorial decisions, with journalists working in politically affiliated media feeling pressured to align their reporting with the owner's interests.[85] Although there is no state

78. Ghanaian journalists warn proposed cybersecurity amendments could affect press freedom (2025) https://cadeproject.org/updates/ghanaian-journalists-warn-proposed-cybersecurity-amendments-could-affect-press-freedom/ (Accessed on 05 December 2025)
79. Constitution of Ghana (1992) https://www.ghanalegal.com (Accessed on 23 November 2024)
80. Election Disinformation Trends in Ghana: Tips for Combating Them (2024) https://en.hive-mind.community/blog/1013,election-disinformation-trends-in-ghana-tips-for-combating-them (Accessed on 23 November 2024)
81. About 64.4% of Ghanaians encourage spreading of fake news – Study (2024) https://www.myjoyonline.com/about-64-4-of-ghanaians-encourage-spreawithhousesding-of-fake-news-study/ (Accessed on 23 November 2024with)
82. Ghana Drafts Bill To Tackle Misinformation And Hate Speech (2025) https://wadr.org/ghana-drafts-bill-to-tackle-misinformation-and-hate-speech/ (Accessed on 05 December 2025)
83. Ghana's New Bills on Mis/Disinformation, Cybersecurity & Hate Speech: MFWA Raises Concerns (2025) https://mfwa.org/issues-in-focus/ghanas-new-bills-on-mis-disinformation-cybersecurity-hate-speech-mfwa-raises-concerns/ (Accessed on 05 December 2025)
84. 60%-70% of Ghana's media ownership are politicians – GJA President (of been,been,2025) https://citinewsroom.com/2024/05/60-70-of-ghanas-media-ownership-are-politicians-gja-president/ (Accessed on 05 December 2025)
85. Media and politics: investigating government interests, ownership influence and media independence in combating corruption in Ghana (2025) https://www.tandfonline.com/doi/full/10.1080/23311886.2025.2483391#abstract (Accessed on 05 December 2025)

censorship, there is a significant amount of self-censorship amongst journalists due to safety concerns and fear of legal repercussions. Ghana ranked 41 out of 180 countries on the legal context component of the 2025 World Press Freedom Index. It had previously ranked 38 out of 180 in 2024.[86] This highlights a major limitation on journalistic practices, which restricts journalists' ability to deliver accurate and comprehensive coverage of significant events, ultimately impacting the quality of information available to the public.

The National Communication Authority, in the exercise of its mandate, shuts down or suspends media houses that violate Regulation 54 and 56 of the Electronic Communications Regulations, 2011, L.I. 1991 and Section 2 (4) of the Electronic Communications Act, 2008 (Act 775). In 2025, 62 radio stations were suspended. These stations did not hold valid broadcasting authorisations or did not have a Certificate of Compliance to commence operations.[87] In the past, this exercise has been perceived as censorship of radio stations critical of the government through the National Communication Authority.[88] Censorship and content moderation in Ghana are nuanced. As digital platforms continue to grow, the Ghanaian government and various stakeholders face the difficult task of creating regulations that safeguard individuals from harmful content—such as hate speech, misinformation, and online harassment—while upholding the fundamental right to free speech. This delicate tension reflects broader global discussions about the government's role in regulating digital spaces, the consequences of unchecked expressions, and the need for a framework that promotes open dialogue and ensures the safety and well-being of all citizens.

86. World Press Freedom Index: Ghana (2025) https://rsf.org/en/country/ghana (Accessed on 05 December 2025)
87. NCA Orders Defaulting FM Broadcasting Stations to Suspend Operations (2025) https://nca.org.gh/2025/06/12/nca-orders-defaulting-fm-broadcasting-stations-to-suspend-operations/ (Accessed on December 2025)
88. Ghana 2024 Elections: A Risk Assessment of the Online Information Space (2024) https://www.iri.org/resources/ghana-2024-elections-a-risk-assessment-of-the-online-information-space/ (Accessed on 23 November 2024)

Access to information

Ghana has the Right to Information Act (RTI) in place to protect citizens' right to access information and facilitate an open, inclusive environment that promotes greater accountability and public debate. Citizens can request and obtain information from public and select private institutions. It is based on Article 21(1)(f) of the 1992 Constitution, which states that all persons have the right to information, subject to necessary qualifications in a democratic society. All public institutions are required to submit annual reports capturing details stipulated under Section 77(2) of the Act.

Records in 2023 showed that 1,000 requests had been made under the RTI Act. Of these requests, 838 have been granted, 47 have been rejected, and 45 have been transferred.[89] During that period, 14 public institutions have been fined GH¢1,310,000, approximately US$ 109,258 for failing to comply with the Right to Information Commission's orders to provide applicants with the requested information.[90] Report suggests that the public requests for information increased by 47% in 2024, reflecting growing citizen engagement and trust in the right to information system.[91] There is no published data yet on the number of requests made in 2025. The government has created a centralised digital platform to offer citizens a secure way for submitting RTI requests, allowing for tracking, timely responses from public institutions, and data generation for compliance monitoring.[92]

89. Over 1000 Requests Made Since Passage of RTI Law – Oppong Nkrumah (2023) https://moi.gov.gh/news-room/2023/05/over-1000-requests-made-since-passage-of-rti-law-oppong-nkrumah/ (Accessed on 28 November 2024)
90. 14 Institutions fined GH¢1.3m for non-compliance with RTI Law (2023) https://www.graphic.com.gh/news/general-news/14-institutions-fined-gh-1-3m-for-non-compliance-with-rti-law.html (Accessed on 28 November 2024)
91. Request for information through RTI surges - Commission now prioritising digital access (2025) https://www.graphic.com.gh/news/general-news/ghana-news-request-for-information-through-rti-surges-commission-now-prioritising-digital-access.html ...
92. Launch an Online Platform for Right to Information Requests (2025) https://www.opengovpartnership.org/the-open-gov-challenge/ghana-launch-an-online-platform-for-right-to-information-requests/..

Civil society organisations play a significant role in educating the public about this law. For example, the Media Foundation for West Africa implemented workshops educating citizens about the Right To Information law to enable them to request information independently.[93]

Despite the constitutional and legal guarantees and the digital measures implemented by the government and civil society actors, there are still significant barriers to access to information. These barriers include an uneven digital divide, gender inequality, infrastructural gaps, and the cost of accessing information. Substantial work is needed to enhance the proactive disclosure of information on government websites. This involves making relevant documents, datasets, and reports available and ensuring they are easily accessible and understandable to the public. Furthermore, the information should be updated regularly and organised in a user-friendly manner to promote transparency and encourage citizen engagement with government activities. A draft legislative instrument that addresses some of these issues has been submitted to the Subsidiary Legislative Committee of Parliament for review as of 2024. Although the Committee met to discuss the draft, it had yet to submit its report to the plenary for passage.[94]

AI and Emerging Technologies

The government launched the National AI strategy (2023 - 2033) in 2025 to drive innovation.[95] A Responsible AI

93. MFWA enhances capacities of more than 600 citizens on Ghana's Right to Information Law (2023) https://mfwa.org/issues-in-focus/mfwa-enhance-capacities-of-more-than-400-citizens-on-ghanas-right-to-information-law/ (Accessed on 28 November 2024)
94. 5 Years of empowering transparency: Celebrating Right to Information Commission's journey (2) (2025) https://theghanareport.com/5-years-of-empowering-transparency-celebrating-right-to-information-commissions-journey-2/ (Accessed on 07 December 2025)
95. Embracing the Future: Ghana Launches National AI Strategy to Drive Innovation (2025) https://moc.gov.gh/2025/05/02/embracing-the-future-ghana-launches-national-ai-strategy-to-drive-innovation-2/ (Accessed on 07 December 2025)

(RAI) Office is set to be established to oversee the implementation of the strategy, ensuring alignment with ethical standards and national goals, while coordinating efforts, monitoring progress, and facilitating stakeholder engagement.[96] The National Communications Authority also launched a 5-year strategic plan (2024 – 2028) that will position the Regulator to stay ahead of industry demands, creating an enabling and well-protected digital ecosystem. As advanced technology becomes more prevalent in data management, prioritising data governance is essential for the success of Ghana's digitisation efforts.[97] The government is working on a national data strategy.

At the centre of Ghana's AI discourse are the regulatory gaps, ethical concerns, infrastructural challenges, and digital literacy and skills. Some lawmakers have raised concerns about the potential misuse of AI and have called for legislation to regulate it in the country.[98] Others have also called for AI regulation to be balanced as it is essential to foster innovation and creativity.[99] To this end, a new draft law - the Emerging Technologies Bill, 2025 is being worked on. It is currently under ongoing public consultation,[100] and pending review by Parliament in 2026.[101] At its core is

96. Ghana's National Artificial Intelligence Strategy (2023–2033) (2025) https://dig.watch/resource/ghanas-national-artificial-intelligence-strategy-2023-2033 (Accessed on 07 December 2025)
97. Ghana develops its national data strategy in collaboration with Smart Africa and Team Europe (2024) https://smartafrica.org/ghana-develops-its-national-data-strategy-in-collaboration-with-smart-africa-and-team-europe/ (Accessed on 8 December 2024)
98. MPs propose legislation to regulate Artificial Intelligence (2023) https://citinewsroom.com/2023/06/mps-propose-legislation-to-regulate-artificial-intelligence/ (Accessed on 9 December 2024)
99. Balanced AI regulation essential to foster innovation and creativity (2024) https://www.ghanaweb.com/GhanaHomePage/business/Balanced-AI-regulation-essential-to-foster-innovation-and-creativity-Valentine-Obi-1930934 (Accessed on 9 December 2024)
100. Public Consultation on: Emerging Technologies Bill, 2025 (2025) https://www.brr.gov.gh/consultation?cd=NDU= (Accessed on 07 December 2025)
101. Gov't to lay Emerging Technologies Bill before Parliament in 2026 (2025) https://citinewsroom.com/2025/11/govt-to-lay-emerging-technologies-bill-before-parliament-in-2026/ (Accessed on 07 December 2025)

responsible technology governance.[102] Policy experts have questioned how this law will interact with the amended Cybersecurity and Data Protection Act when passed because there could be a potential overlapping of mandates and duplication of regulatory authority.[103]

Ghana's startup ecosystem is driving the adoption of AI and emerging technologies through product and service innovation. The country ranked 101st and 8th at global and Africa level, respectively, showing stronger innovation outputs (93rd) than inputs (108th) on the 2025 Global Innovation Index, with strengths in creative services and unicorn valuation.[104] The country is attracting the requisite private sector investment to develop infrastructure that supports AI and emerging technologies. In 2025, Google launched its AI Community Centre, backed by a US$37 million commitment to support artificial intelligence innovation across the continent.[105] Degas Limited pledged US$100 million over the next four years to make Ghana the first AI-powered agricultural hub in Africa.[106] Ghana and the United Arab Emirates (UAE) signed a US$1 billion partnership to build Africa's largest AI and Technology Hub in Ningo-Prampram.[107]

102. Ghana Is Pushing A New Law For Emerging Technologies. But Does It Create Too Much Bureaucracy? (2025) https://labarijournal.com/ghana-is-pushing-a-new-law-for-emerging-technologies-but-does-it-create-too-much-bureacracy/ (Accessed on 07 December 2025)
103. Ghana Faces Regulatory Coordination Challenges in AI Framework (2025) https://www.newsghana.com.gh/ghana-faces-regulatory-coordination-challenges-in-ai-framework/ (Accessed on 07 December 2025)
104. Global Innovation Index: Ghana (2025) https://www.wipo.int/edocs/gii-ranking/2025/gh.pdf (Accessed on 08 December 2025)
105. Google Launches AI Community Center in Ghana With $37M Investment, Deepening U.S.–Africa Tech Collaboration (2025) https://amchamghana.org/2025/07/31/google-launches-ai-community-center-in-ghana-with-37m-investment-deepening-u-s-africa-tech-collaboration/ (Accessed on 08 December 2025)
106. Ghana's $100M AI-Powered Agriculture Hub: What It Means for the Future of Farming (2025) https://sesitechnologies.com/ghanas-100m-ai-powered-agriculture-hub-what-it-means-for-the-future-of-farming/ (Accessed on 08 December 2025)
107. Ghana, UAE sign $1bn deal to build tech hub - Targets over 11,000 foreign companies (2025) https://www.graphic.com.gh/news/general-news/ghana-news-ghana-uae-sign-1bn-deal-to-build-tech-hub-targets-over-11-000-foreign-companies.html (Accessed on 08 December 2025)

Digital Inclusion

Gender gaps exist in the ownership of digital devices in Ghana. Smartphone ownership and overall mobile phone ownership are lower for women, limiting their access to internet-based services and opportunities. This phenomenon is primarily influenced by two main factors: the high costs of acquiring these devices and the lack of adequate skills to utilise these technologies effectively. These factors originate from underlying social structures that contribute to gender disparities. As a result, women often have limited access to education compared to men, affecting their earning potential. As of mid-2025, reports indicated that smartphone ownership among women in Ghana was nearly 87%, approaching parity with men.[108] While mobile device ownership is lower among women, 75% of them access the internet exclusively via mobile devices, compared to 58% of men. Access to smartphones and the internet remains beyond the reach of certain segments of the population, including the poor.[109] Even though the data on multidimensional poverty for 2025 have not been released yet, the 2024 report shows that 24% of Ghana's population are multidimensionally poor. As of 2025, approximately 25.4% of the country's total population, mostly in rural Ghana, do not have internet access.[110] In rural communities, only 19% of households have reliable internet access, compared to 63% in urban areas.[111]

The private sector is leveraging the robust digital payment ecosystem

108. African women gain financial control through mobile money (2025) https://www.africanewsanalysis.com/african-women-gain-financial-control-through-mobile-money/18/09/31/58/07/2025/ (Accessed on 08 December 2025)
109. Multidimensional Poverty Report, Ghana (2024) https://statsghana.gov.gh/gssmain/fileUpload/pressrelease/MPI%20GHANA%20REPORT.pdf (Accessed on 08 December 2024)
110. Digital 2025: Ghana (2025) https://datareportal.com/reports/digital-2025-ghana (Accessed on 08 December 2025)
111. Technology in Rural Education to Bridge the Digital Divide in Ghana (2025) https://futureseedsfoundation.com/technology-in-rural-education-to-bridge-the-digital-divide-in-ghana/ (Accessed on 08 December 2025)

and identification system, to roll out buy-now-pay-later schemes that enable low income earners to own smartphones on credit basis. Through the Ghana Investment Fund for Electronic Communications (GIFEC), the government is also implementing several projects, including the Ghana Rural Telephony and Digital Inclusion Projects to bridge the digital divide.[112] As of 2025, GIFEC has constructed 1,897 roaming sites, 269 community ICT centres, and connected 1,139 schools to the Internet. These projects were funded by a 1% regulatory fee levied on the net annual revenue of communication service providers and operators, contributions from government, and grants from development partners. At the time of writing this report, there were no comprehensive annual financial reports available online to ascertain the total funds accessible to GIFEC for projects and operations.

Online child protection and safety are crucial for digital inclusion, particularly as smartphone penetration increases. Recent data indicates that 90.5% of children aged 8 to 17 have used the Internet at some point. Of those who use the Internet, 45.7% access it via smartphones. Furthermore, 56.7% of children who access the Internet through smartphones receive little or no supervision. This lack of oversight could lead to involvement in fraudulent activities, exposure to sexual and violent content online, and other risks, such as addiction.[113] While there is no recent data for 2025, a 2020 reported by the National Center for Missing and Exploited Children revealed that over 13,000 images and videos of child sexual abuse were accessed or uploaded to the internet from Ghana.[114] The Cybersecurity Act (Act 1038) criminalises online child abuse, including the production, viewing, and distribution of child sexual abuse materials, online grooming, cyberstalking, and sextortion under Sections 62-67. The Children Act of 1998 does not adequately cover the nuances of the current technological advancements and the associated exposure of children to harm. The government seeks to bridge the gaps with the National Child Online Protection Framework.[115] Ghana has ratified several international legal frameworks, conventions, and protocols in the past that address child sexual exploitation and abuse both online and offline. Some of the frameworks include the Council of Europe Convention on Cybercrime, the African Union Convention on Cyber Security and Personal Data Protection, and the United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Pornography. There were no reported incidents of child online abuse in the under review.

112. Government Is Determined to Bridge Digital Divide (2024) https://moi.gov.gh/newsroom/2024/02/govt-is-determined-to-bridge-digital-divide-ursula-owusu/ (Accessed on 11 December 2024)
113. Internet usage, access, and supervision among Ghanaian children: a cross-sectional study (2024) https://doi.org/10.1057/s41599-024-03482-8 (Accessed on 27 March 2025)
114. President of FIDA-Ghana leads child online protection in Ghana (2022) https://www.csa.gov.gh/president_of_fida_leads_cop.php (Accessed on 27 March 2025)
115. Cyber Security Authority https://www.csa.gov.gh/resources/National%20COP%20Framework.pdf (Accessed 20 March 2025)

Conclusion

Liberalising the Information and Communications Technology (ICT) sector has been instrumental in enhancing infrastructure and elevating Ghana's competitiveness within the regional landscape. The implementation of a comprehensive and coherent set of laws, policies, and targeted projects—each aimed at addressing specific objectives—has significantly contributed to this advancement. Ghana boasts relatively favourable rankings in various global indices related to ICT development; however, the nation continues to grapple with several critical challenges. One of the most pressing issues is the ongoing decline in press freedom and the curtailment of online expression. This trend raises concerns about the implications for democratic engagement and the flow of information.

Additionally, the digital divide poses significant hurdles, evidenced by stark disparities in service quality, access to digital technologies, and levels of digital literacy among diverse demographic groups. Vulnerable populations, particularly those in rural areas, face pronounced barriers that hinder their ability to participate in the digital economy. There are rising concerns surrounding data protection, individual privacy, and cybersecurity. As the technology landscape evolves, it is essential to devise proactive solutions that address these issues while ensuring the safety and security of online users. To effectively tackle these challenges, developing robust regulatory frameworks is crucial, as is fostering meaningful collaboration between government entities and the private sector. Such partnerships can lead to innovative strategies that not only address existing gaps but also anticipate future needs.

A more equitable and secure digital future for all citizens can be achieved when the government implements targeted policies that focus on safeguarding investments in the digital sector, encouraging innovation, and expanding access to technology, especially for underserved communities. By prioritising existing initiatives, Ghana can create a more inclusive digital ecosystem that truly benefits everyone.

Recommendations

Recommendations to improve internet access, freedom of expression, access to information, digital inclusion, data protection and privacy and protect digital rights are based on an analysis of reported events and the country's overall score on TheScore Index. These recommendations are presented in relation to the interactions among stakeholders in the digital space.

The Government should:

- Elevate the National Media Commission to an Authority status to enhance its power in overseeing and regulating media content with the confines of the Misinformation, Disinformation, Hate Speech and Publication of Other Information (MDHI) Bill, 2025. This would establish ethical reporting and responsible behaviour guidelines, fostering a more transparent and trustworthy media environment for journalists and the public.
- Establish a specialised court to swiftly address assaults on journalists, ensuring timely justice and enhancing press freedom protections. By prioritising these cases, the country can deter violence against media professionals and safeguard their rights. Additionally, resources and support for journalists affected by such attacks during legal proceedings should be provided.
- Expand GIFEC's resources to support AI and emerging technologies by increasing funding, enhancing infrastructure, and fostering collaborations with tech innovators. This will drive economic growth and improve nationwide services. The current 1% being levied on telecom networks should be reviewed and increased. Big tech companies and social media platforms must also be levied to fund internet expansion initiatives.

- Implement comprehensive policies to ensure fair competition among all participants in the digital ecosystem. These policies should remove barriers that disadvantage certain market players, promote transparency in pricing, encourage innovation, and protect consumer interests. By focusing on fair practices, the country can create an environment where large and small entities can thrive. This, in turn, will benefit the overall economy and foster a diverse and vibrant digital landscape.
- Implement regulatory framework, guidelines, and standards for mobile network operators, internet service providers and big tech social media companies to protect children online. This should include measures for safeguarding personal information, implementing age verification protocols, promoting digital literacy, and enhancing reporting mechanisms for online threats.
- Consider reviewing the unique policy of a single and shared wholesale 4G/5G network infrastructure through Next Gen InfraCo (NGIC) to allow participation of other providers. This approach will create market efficiency and accelerate the deployment of 5G networks.

Civil Society Organisations should:

- Work with agencies under the sector ministry to launch a public engagement campaign to educate citizens about their rights and responsibilities regarding freedom of expression, data protection, and data privacy. The campaign should provide clear information on these rights, emphasising expression and the importance of recognising boundaries to prevent harm and misinformation.
- Work with government stakeholders to develop research-based and data-driven policies that promote digital inclusion for underrepresented communities while protecting citizens' rights.
- Develop a legal aid initiative to support journalists facing trials and legal challenges due to their reporting. This initiative should provide legal representation, financial support for legal fees, and resources to navigate the legal system. It should also include education on journalists' rights and foster partnerships with legal professionals dedicated to press freedom, ensuring journalists can perform their duties without fear of legal repercussions.
- Continue the advocacy and gatekeeping role to ensure accountability from the political class. By actively interrogating government policies and tracking government initiatives, civic society organisations can hold the government to stringent ethical standards.

The Private Sector should:

- Comply with regulatory industry guidelines, including conducting regular audits and assessments to evaluate compliance status.
- Provide training and resources to enhance understanding of regulations and promote a culture of accountability and continuous improvement.
- Work with civic society organisations to create and implement initiatives to educate citizens about their responsibilities when using digital solutions and consuming information.

The Score Index

Ghana, 2025

Totally non-compliant, Mildly compliant - which is a mild attempt at compliance with critical gaps , Moderately compliant - where there are areas of improvement, Considerably compliant - Minimal areas of reform, Fully Compliant - No concerns

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	5	5	There have been no reported cases of Internet Shutdowns. The government works with stakeholders to keep the Internet on.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	4	4	The government has several policies and initiatives to achieve the desired outcome on this indicator. The majority of the initiatives are spearheaded by GIFEC. This law will be replaced with the Digital Economy and Innovation Development Fund Bill, 2025. The NCA has also amended Quality of Service (QoS) Indicators to ensure good service to consumers.
False News Criminalisation	P22(2)	1	1	A law prohibiting the publication of false news exists. The Criminal Code and the Electronic Communication Act (Act 775) are the applicable laws at present. A new law - Misinformation, Disinformation, Hate Speech and Publication of Other Information (MDHI) Bill, 2025, is currently being worked on.
Sedition Legislation	P22(2)	3	3	Sedition is no longer a crime after the repeal of the criminal libel and seditious laws in 2001. Concerns persist regarding Section 208 of the Criminal Offences Act, which targets false news intended to incite fear, as well as aspects of the Electronic Communications Act, 2008 (Act 775).
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	2	2	Existing laws are being misapplied to arrest and harass journalists, and the government does not appear to be protecting them. The Criminal Code and the Electronic Communications Act are the applicable laws. The Electronic Communication Act is undergoing amendment. A Revised Broadcasting Bill is also being worked on.
Data Protection Legislation.	P42	5	5	A law exists to safeguard citizens' personal information and data and ensure privacy. The Data Protection Act, Cyber Security Act, Electronic Communication Act, and the Constitution are applicable laws. The Data Protection Act, Cybersecurity Act, and the Electronic Communications Act are undergoing amendments. There's no public data on enforcement

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	4	4	There is a provision in the Electronic Communication Act that is rarely utilised. This legislation is undergoing an amendment.
Invasion of Privacy of Communications	P41	5	5	There are laws protecting privacy, but there are also provisions within these laws that allow for exceptions to this protection. The applicable laws include the Constitution, Data Protection, Electronic Communication Act and Cyber Security Act. The Data Protection, Electronic Communication Act, and Cyber Security Act are undergoing amendment.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	3	3	The right to information is protected by The Right to Information Act. Implementation however is fraught with challenges. The law is being amended.
AI and Emerging Technologies national strategies	P39(6)	3	4	There is a national strategy, tools for ethical use, and policies to build the required infrastructure. The Emerging Technologies Bill is being worked on to set the framework for AI, blockchain, and other advanced technologies.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P39(6)	3	3	There is existing policy and legislation to protect children online, but gaps remain, particularly in regulations for mobile operators and telecom companies. The Cyber Security Act applies, while the Children Act of 1998 is outdated regarding current technology and its risks to children. The Cyber Security Act is undergoing amendments to expand the powers of the Cyber Security Authority,
Digital Inclusion	P37(3)	4	4	Institutions, policies, initiatives, and strategies exist to ensure inclusive access to digital technology. The majority of initiatives are driven by GIFEC. This law will be replaced with Digital Economy and Innovation Development Fund Bill, 2025.

Total (out of 60):	2024: **42**	2025 **43**	The overall country performance rating indicates that Ghana is moderately compliant.

Kenya

By Miriam Beatrice Wanjiru

Executive Summary

Kenya's LONDA 2025 report offers a comprehensive overview of the country's digital landscape, examining the state of digital rights and digital inclusion. The report is founded on the African Commission on Human and Peoples' Rights (ACHPR) Declaration of Principles on Freedom of Expression and Access to Information in Africa and is informed by a mixed-methods approach, drawing on desk-based legal and policy analysis, secondary data review, Key informant interviews conducted with regulators and sector stakeholders and media monitoring to assess trends, developments and emerging challenges. Thematic areas covered include internet access and disruptions, digital inclusion, freedom of expression, data protection and privacy, as well as developments in ICT and technologies. It further delves into the gaps and failures in the digital space, which leave a large part of the population disadvantaged due to poverty, regional marginalisation, or infrastructural limitations. Throughout the report, several key breaches are highlighted, primarily involving the state and its various organs. Finally, the report provides recommendations to the state, media, and civil society on potential best practices for achieving a just society. The government is encouraged to ensure all digital policies and actions respect rights and prioritise inclusion and accountability. The media ought to investigate and clearly explain digital rights issues while amplifying the voices of those most affected by exclusion and repression. Civil society must continuously document digital rights abuses, support affected communities, and use evidence to advocate for legal and policy reforms.



Introduction

Kenya is a youthful country of 57.5 million people with a median age of 21.1 years.[1] The expectation of the Kenyan polity, as defined by its Constitution, promulgated in 2010, is a state that values human rights, equality, freedom, democracy, social justice, and the rule of law.[2] Kenya leads in regional technology development, with the ICT sector posting strong growth and sector output estimated at KES 608 billion (approximately US$4,704,061,897).[3] As of early 2025, there were 27.4 million internet users, representing 48% penetration, and 15.1 million social media users, which is about 26.5% of the population.[4] Despite being ranked among Africa's top performers in e-government and inclusive internet readiness, high data and broadband costs continue to exclude many lower-income Kenyans from fully participating in the digital economy.[5] Kenya's media landscape is among the most vibrant on the continent, though journalists face harassment and intimidation, and press-freedom-restricting laws remain on the books.[6]

Internet Access and Disruptions

Similar to 2024, the Internet was throttled during youth-led protests on 25th June 2025.[7] Netblocks, a global internet observatory that monitors cybersecurity and digital rights, reported a sharp drop in access to platforms such as Telegram[8] on various Kenyan telecommunications companies and Internet Service Providers, including Safaricom PLC, Jamii Telecommunication Ltd, and Liquid Intelligent Technologies.[9] Additionally, on 25 February 2025, the Nairobi County Government destroyed critical ICT infrastructure during a standoff with the national Kenya Power Company over unpaid bills, which resulted in widespread downtime for businesses, households, and mission-critical sectors such as healthcare, finance, and public services.[10]

Such instances mark a departure from Kenya's history of relatively open internet access. Internet disruptions, whether partial, intermittent, or complete shutdowns, are infringements on digital rights and threaten civic spaces. Further, disconnecting the already connected due to intentional interference prevents people from disseminating information, responding to crises, conducting business, and enjoying internet freedoms, as provided for in Articles 33, 34, and 35 of the Kenyan Constitution (2010).

Online Freedom of Expression and Access to Information

Despite Articles 33, 34, and 35 of the Kenyan Constitution (2010), which provide for the rights to free expression, freedom of the media, and access to information, select events in 2025 highlighted a conflict between state authority and free speech. The Computer Misuse and Cybercrimes Amendment Act 2024, enacted in October 2025has overly broad and vague provisions with potential to curtail rights and freedoms, especially for activists, human

1. PopulationPyramids.org, "Kenya Population Pyramid 2025" (2025) https://www.populationpyramids.org/kenya? (accessed on 25th November, 2025)
2. Constitution of Kenya (2010)
3. KNBS, "Economic Survey 2025" (2025) https://www.knbs.or.ke/publications/ (accessed on 25th November, 2025).
4. Datareportal, "Digital 2025: Kenya" (2025) https://datareportal.com/reports/digital-2025-kenya (accessed on 25th November, 2025)
5. University World News, "Digital divide, brain drain threaten vibrant digital economy" (2025) https://www.universityworldnews.com/post.php?story=20250921183835849#:~:text=%E2%80%9CUsage%20rates%20vary%20from%2064.7,entry%20into%20the%20digital%20economy. (accessed on 25th November 2025).
6. Freedom House, "Kenya Press Freedom" (2025) https://freedomhouse.org/country/kenya/freedom-net (accessed on 25th November, 2025).
7. Business Daily 'Bloggers decry digital rights purge by State' (2025) https://www.businessdailyafrica.com/bd/economy/bloggers-decry-digital-rights-purge-by-state-5147032 (accessed on 27 November 2025).
8. Netblocks (2025) https://x.com/netblocks/status/1937850265597534670 (accessed on 27 November 2025).
9. KICTANET 'URGENT: Internet Access Blocked in Kenya — KICTANet Condemns Digital Rights Violations' (2025) https://www.kictanet.or.ke/urgent-internet-access-blocked-in-kenya-kictanet-condemns-digital-rights-violations/ (accessed on 27 November 2025).
10. Citizen TV Kenya 'Standoff disrupts internet services in Nairobi' (2025) https://www.youtube.com/watch?v=W-kOMbn9xAFo (accessed on 27 November 2025).

rights defenders, journalists and political opponents. Citizens such as Rose Njeri, a software developer, have already become victims of the law. Rose, who created and launched an email automation tool that allows citizens to submit directly to Parliament, was charged with violating Section 16 of the cyber law. Her arrest misrepresents a legitimate act of civic engagement as a cybercrime.

Closely linked to that, Mr Jackson Kuria, a prison officer turned activist, was charged on 20 January 2025 with publishing false information in terms of Section 23 of the Computer Misuse and Cybercrimes Act No.5 of 2018.[11],[12] The arrest of Mr Kuria is one of many examples of the narrowing space available for whistleblowers and online activists. Mr Titus Sifuna was arraigned at a Magistrate's Court in Nairobi to face charges of publishing false information while pretending to be President Ruto.[13] The 22-year-old was accused of impersonating President Ruto on social media and falsely claiming that the Head of State was succumbing to public pressure and planning to step down.

Even more concerning is the posthumous case of Albert Ojwang, who was arrested on 7 June 2025 after Kenya's Deputy Police Chief Eliud Lagat filed a complaint, accusing the blogger of defaming him on social media.[14] Following the death of Mr Albert Ojwang on 8 June 2025 in police custody, the officers tampered with the CCTV footage of the cells, denying investigators the necessary evidence for the judicial process.[15] This is despite the

11. The Guardian ''This is lawfare': Kenya weaponising the law' to silence critics and protesters' (2025) https://www.theguardian.com/global-development/2025/aug/08/kenya-weaponises-law-mass-arrests-crackdown-critics-protesters (accessed on 27 November 2025),.
12. NTV Kenya 'Cop Shakur charged with publishing false information about President Ruto' (2025) https://ntvkenya.co.ke/news/cop-shakur-charged-with-publishing-false-information-about-president-ruto/ (accessed on 27 November 2025)
13. Daily Nation 'How social media users face threats of jail and heavy fines for their posts' (2025) https://nation.africa/kenya/news/how-social-media-users-face-threats-of-jail-for-their-posts-5018434 (accessed on 27 November 2025).
14. BBC 'Police officers charged with murder of Kenyan blogger' (2025) https://www.bbc.com/news/articles/cz09l4k4184o (accessed on 27 November 2025).
15. Reuters 'Senior Kenyan policeman arrested over death of blogger in custody' (2025) https://www.reuters.com/world/africa/senior-kenyan-policeman-afive-yearrrested-over-death-blogger-custody-2025-06-13/ (accessed on 29 November 2025).

fact the right to access information is enshrined under Article 35 of the Constitution and the Access to Information Act of 2016.[16] In 2025, in what seems like systemic suppression of freedom of expression the national government increasingly used anti-terrorism courts to prosecute protesters, charging over 70 individuals, mostly youth and digital activists, with terrorism-related offences.[17]

On a separate note, but in relation to free speech and freedom of the media, the Communication Authority of Kenya (CA) ordered an immediate halt to live television and radio broadcasts of the June 2025 protests, failure to which would result in regulatory sanctions.[18] Using regulatory power to deter broadcasters against live coverage curtails media freedoms and access to information.

On a positive note, a High Court in Kenya ruled that Meta, Facebook's parent company, can be sued in country for its alleged role in facilitating the spread of content that incited ethnic violence.[19] The landmark decision rejected Meta's argument that Kenyan courts lack jurisdiction since the company is not registered in Kenya.

Privacy and Surveillance

The right to privacy is protected by the Kenyan Constitution (2010) under Article 31 and is given effect by the Data Protection Act, 2019 (DPA). In 2025, a five-year strategic plan was launched by the Office of the Data Protection Commissioner (ODPC) with key goals including continuous review of the Data Protection Act and regulations, institutional capacity-building for compliance enforcement, and

16. Kenya Law 'Access to Information Act' (2025) https://new.kenyalaw.org/akn/ke/act/2016/31/eng@2022-12-31 (accessed on 29 November 2025).
17. Amnesty Kenya 'The Dangerous Expansion of Kenya's Anti-Terrorfive-year Laws' (2025) https://www.amnestykenya.org/the-dangerous-expansion-of-kenyas-anti-terror-laws/#:~:text=July%2023%2C%202025-,THE%20DANGEROUS%20EXPANSION%20OF%20KENYA'S%20ANTI%2DTERROR%20LAWS,through%20the%20lens%20of%20counterterrorism? (accessed on 27 November 2025).
18. Citizen Digital 'Communications Authority orders stop to live broadcasts of June 25 protests' (2025) https://www.citizen.digital/article/communications-authority-orders-stop-to-live-broadcasts-of-june-25-protests-n365216 (accessed on 29 November 2025).
19. 19 KICTANET 'High Court Rules Meta Can Be Sued in Kenya' (2025) https://posts.kictanet.or.ke/high-court-rules-meta-can-be-sued-in-kenya/ (accessed on 27 November 2025).

increased monitoring, surveillance, and public trust in Kenya's data governance ecosystem.[20] Subsequently, the Kenya Revenue Authority (KRA) issued regulations for the new Significant Economic Presence Tax (SEPT), expanding taxation on all locally consumed digital services, regardless of provider location. SEPT targets online platforms (non-resident entities) that provide internet or electronic services to local users. Although the regulation serves a valid purpose in taxing digital services consumed in Kenya, potential non-compliance with the Data Protection Act may lead to the tax authority's enhanced surveillance of Kenyan users.

Despite having strong laws and regulations on data protection, the national government suffered a significant data breach at the Business Registration Service (BRS) that exposed sensitive information about millions of Kenyan companies.[21] As the sole custodian of Kenya's company registry, BRS holds critical data on all registered businesses, including company names, directors' and shareholders' details.[22] The cyberattack highlighted serious vulnerabilities in the cybersecurity of state systems, which can lead to data and identity theft.

Another significant incident involved the Directorate of Criminal Investigations (DCI), which suffered a cyber-attack on its official digital platforms, including X (formerly Twitter) and Facebook. Attackers took control of the accounts and used the platforms to promote cryptocurrency scams, reportedly making illicit profits of approximately 64.7 Solana (SOL) tokens, approximately $4,000 and $13,000, in earnings before authorities regained control.[23] The attack exposed cybersecurity vulnerabilities of the government's digital systems.

Similar to 2024, debt shaming by digital lenders is becoming increasingly prominent nationwide. Some digital credit providers, in the course of debt collection, access clients' contact lists sometimes without their knowledge or consent.[24] As such, the ODPC sought license revocation of Kenyan digital lenders over persistent breaches of data protection laws.[25] The Central Bank of Kenya is yet to revoke a digital lender's license as was recommended by the ODPC albeit errant firms like Chapeo Capital Limited, Mulla Pride, and Azura Credit are known debt shaming players with regulatory warnings and fines. Apart from predatory data use in digital lending, consent is also undermined in formal financial markets. Standard Investment Bank collected a complainant's email address without explicit permission before sending them promotional content.[26] This constituted a breach of Section 26(a) of the DPA, which mandates that data subjects be informed about the collection and use of their personal data at or before the point of collection.[27]

Beyond corporate environments, state security agencies have also been implicated in intrusive data practices. According to a forensic analysis done by Citizen Lab, a Canadian internet watchdog based at the University of Toronto, spyware (FlexiSPY) was installed on Mr Bryan Adagala's Phone in May 2025.[28] Mr Adagala was among the makers of the documentary, "Blood Parliament", and was, as a result, arrested by Kenya's Directorate of Criminal Investigation. FlexiSPY, a surveillance

20. Citizen Digital 'Kenya strengthens data governance with new ODPC strategic plan and Nyeri regional office' (2025) https://www.citizen.digital/article/kenya-strengthens-data-governance-with-new-odpc-strategic-plan-and-nyeri-regional-office-n365814 (accessed on 27 November 2025).
21. Capital News 'Govt Confirms Data Breach on main registry exposing millions of companies' (2025) https://www.capitalfm.co.ke/news/2025/02/govt-confirms-data-breach-on-main-registry-exposing-millions-of-companies/ (accessed on 27 November 2025).
22. Business Daily 'Cybercriminals steal business owners' IDs, phone, house details' (2025) https://www.businessdailyafrica.com/bd/corporate/technology/cybercriminals-steal-business-owners-ids-phone-house-details-4910734 (accessed on 27 November 2025).
23. Citizen Digital 'DCI says regained control after Facebook, X accounts hacked' (2025) https://www.citizen.digital/article/dci-says-regained-control-after-facebook-x-accounts-hacked-n357347 (accessed on 28 November 2025).
24. Business Daily 'Data Protection Office asks CBK to revoke permits for two digital lenders' (2025) https://www.businessdailyafrica.com/bd/economy/dpo-asks-cbk-to-revoke-permits-for-two-digital-lenders-5162924 (accessed on 28 November 2025).
25. Business Daily 'Cash-thirsty Kenyans tap 5.5m loans from digital lenders' (2025) https://www.businessdailyafrica.com/bd/economy/cash-thirsty-kenyans-tap-5-5m-loans-from-digital-lenders-5184404 (acccessed on 28 November 2025).
26. CR Advocates LLP 'Two Rulings That Reshape Legal Compliance and Judicial Review in Kenya' (2025) https://www.linkedin.com/pulse/two-rulings-reshape-legal-compliance-judicial-review-o8egf/ (accessed on 28 November 2025).
27. ODPC 'Andrew Endovo v. Standard Investment Bank (Complaint No. 0697 of 2025)' (2025) https://www.odpc.go.ke/wp-content/uploads/2025/10/STANDARD-INVESTMENT-BANK.pdf (accessed on 28 November 2025).
28. Citizen Digital 'Filmmaker behind 'Blood Parliament' claims state surveillance via hacked phone' (2025) https://www.citizen.digital/article/filmmaker-behind-blood-parliament-claims-state-surveillance-via-hacked-

tool, can record phone calls, intercept messages, capture audio, track locations and delete or modify data.[29]

In 2025, telecommunications entities also failed in their data protection duties. Two former managers at Safaricom accessed and shared subscribers' data for sale to a top sports betting firm[30] which is a violation of Section 49 of the DPA.[31] Potential implications of the leaked data include SIM swap fraud, financial scams, profiling, and blackmail.

Elsewhere, the Kenya Information and Communications (Amendment) Bill 2025 mandates Internet Service Providers (ISPs) to collect and submit detailed personal data, including ID numbers and usage patterns, to the Communications Authority of Kenya (CA).[32] This poses a direct threat to the right to privacy, which is constitutionally protected under Article 31 and further enshrined in the DPA.

In a significant judicial fete, the High Court of Kenya presided by Justice Chacha Mwita sitting in Nairobi on 18 July 2025, in Katiba Institute v Communications Authority of Kenya & Others quashed the Communications Authority (CA) and the Kenya Revenue Authority (KRA) public notices mandating disclosure of mobile phone IMEI numbers, declaring them unconstitutional, unlawful, and null and void. The Court held that compulsory IMEI collection violated Article 31 (right to privacy) and failed the proportionality test under Article 24 of the Constitution. The court issued orders of prohibition, thereby halting plans for a centralised device database tied to tax-compliance verification.

Developments in ICT and Emerging Technologies

Kenya's new Artificial Intelligence Strategy 2025–2030 aims to establish strong AI governance, drive adoption in priority sectors (agriculture, security, health, education, public services), grow a local AI ecosystem, and position Kenya as a regional hub for AI research, model development, and scalable innovation.[33] The Strategy aligns the development of AI with other digital economy strategies, such as the Digital Economy Blueprint (2019) and the National Digital Master Plan (2022-2032), which emphasise digital government, digital businesses, infrastructure, innovation, and digital skills.

Kenya also pioneered and launched AI and digital courses for public servants, a progressive capacity-building step towards onboarding the country on the AI strategy and influencing adoption in various public sectors.[34] This program will provide civil servants with critical governance skills that advance digital transformation with integrity, transparency, and accountability, thus securing a future for Kenya that is prosperous, inclusive, ethical, and built on trust.[35]

However, the country lacks a comprehensive and specific regulatory framework for AI. While existing legal frameworks, such as the Data Protection, Computer Misuse and Cybercrime, Intellectual Property, and Consumer Acts[36] provide some guidance, they are insufficient to address the regulatory complexities that come with AI. Such structural gaps create fertile ground for AI-driven cyberattacks, which rose by 28% between July and September 2025, compared to a similar period in 2024.[37]

phone-n369412 (accessed on 28 November 2025).

29. Daily Nation 'How the DCI spies on your phone' (2025) https://nation.africa/kenya/news/how-the-dci-spies-on-your-phone--5189894 (accessed on 28 November 2025).
30. Business Daily 'Deal on stolen data of 11.5m Safaricom subscribers flops' (2025) https://www.businessdailyafrica.com/bd/corporate/technology/deal-on-stolen-data-of-11-5m-safaricom-subscribers-flops-5238396 (accessed on 28 November 2025).
31. ODPC 'Guidance Note on Processing Biometric Data' (2025) https://www.odpc.go.ke/wp-content/uploads/2025/05/Draft-1-Guidance-Processing-of-Biometric-Data.pdf (accessed on 28 November 2025).
32. ICJ Kenya 'Human Rights Analysis of the Kenya Information and Communications (Amendment) Bill, 2025' (2025) https://icj-kenya.org/news/human-rights-analysis-of-the-kenya-information-and-communications-amendment-bill-2025/ (accessed on 28 November 2025).
33. Ministry of ICT 'Kenya Artificial Intelligence Strategy 2025-2030' (2025) https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf (accessed on 28 November 2025).
34. UNESCO 'Kenya Launches UNESCO–Oxford free online course on AI and Digital Transformation' https://www.unesco.org/en/articles/kenya-launches-unesco-oxford-free-online-course-ai-and-digital-transformation (accessed on 19 February 2026).
35. Joint SDG Fund 'Kenya launches pioneering AI and digital courses for public servants' https://www.jointsdgfund.org/article/kenya-launches-pioneering-ai-and-digital-courses-public-servants (accessed on 19 February 2026).
36. CMS Legal 'Data protection and cybersecurity laws in Kenya' (2025) https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/kenya (accessed on 28 November 2025).
37. Daily Nation 'Kenya cyber threats up 28pc as criminals deploy AI tools' (2025) https://nation.africa/kenya/busi-

Digital Inclusion

While 53.7% of Kenyans aged three years and above own a mobile phone, ownership remains heavily skewed toward urban areas, where 64.6% of residents have access to a device compared to only 48.6% in rural regions.[38] This persistent divide underscores structural challenges that continue to isolate rural populations from digital participation. Regarding Kenya's readiness for a digital future, the Competency-Based Curriculum (CBC) was designed to prepare learners for a technologically integrated world. However, as of 2025, only 22% of teachers in the country had undergone formal ICT training.[39] This skills gap within the teaching workforce significantly hampers the development of a digitally literate generation, stifles national innovation capacity, and undermines Kenya's competitiveness in an increasingly digital global economy. According to the Communications Authority of Kenya, plans are underway to establish 1,450 digital hubs across the country.[40] When paired with Universal Service Fund investments, the initiative could lower access costs, increase skills and job opportunities, and improve rural inclusion.

There are concerns regarding the implementation of digital government service platforms. For many individuals living in poverty, the financial burden of acquiring smartphones, computers, or maintaining reliable connectivity remains prohibitive.[41] Furthermore, this exclusion was compounded on 1 August 2025 when data revealed a significant rise in the number of Kenyans relying on feature phones, reaching 32,573,748 users, up from 30,579,714 in the first quarter.[42] While feature phones offer basic communication, they do not support access to the government's digital platforms, nor do they provide immediate access to online information, digital payments, or entertainment services.

Moreover, further evidence emerged of structural exclusion within Kenya's digital policy landscape. Innovators and developers frequently overlook the requirements of persons living with disabilities, resulting in digital platforms and products that are non-inclusive by design. This systemic neglect was echoed when stakeholders in Vihiga County reported that more than 29,000 registered persons living with disabilities continue to lack access to essential digital tools.[43] Many specialised education centers in the region lack computers, limiting learners' ability to develop digital skills and restricting their opportunities in education, employment, and civic participation.47 Together, these regressions reveal deep-seated accessibility gaps that undermine the digital inclusion of people living with disabilities in the country.

Child Online Safety

The digital safety of children in Kenya focused primarily on enforceable compliance expectations as opposed to awareness programs. In 2025, the Communications Authority of Kenya issued the industry guidelines for child online protection and safety in Kenya. These guidelines require ICT providers to institute child online protection policies, as well as, supporting digital literacy for children to enable them to participate fully in the digital ecosystem.[44] In the same vein, the ODPC issued guidance notes for

ness/kenya-cyber-threats-up-28pc-as-criminals-deploy-ai-tools--5233336 (accessed on 28 November 2025).

38. Communication Authority of Kenya 'Urban-Rural Digital Divide Hinders ICT Uptake, Joint CA and KNBS Survey Shows' (2025) https://www.ca.go.ke/urban-rural-digital-divide-hinders-ict-uptake-joint-ca-and-knbs-survey-shows (accessed on 30 November 2025).
39. Citizen Digital 'Bridging the Digital Divide in Education: Why Teachers Need Urgent Upskilling' (accessed on 30 November)
40. Ministry of ICT '47 ICT Centres and 1,450 Hubs Nationwide to Bridge Digital Divide and Spur Innovation' (2025) https://www.ict.go.ke/47-ict-centres-and-1450-hubs-nationwide-bridge-digital-divide-and-spur-innovation (accessed on 28 November 2025).
41. 41 World Economic Forum 'Trade and Labour: Pathways for Decent Work in Kenya's Digital Economy' (2025) https://reports.weforum.org/docs/WEF_Trade_and_Labour_Pathways_for_Decent_Work_in_Kenya's_Digital_Economy_2025.pdf (accessed on 30 November 2025).
42. Capital Fm 'Bridging Kenya's Capital Divide: Why Smartphones Matter for Economic Growth' (2025)https://www.capitalfm.co.ke/news/2025/08/bridging-kenyas-digital-divide-why-smartphones-matter-for-economic-growth/ (accessed on 30 November 2025).
43. The Standard 'Stakeholders Push for Digital Inclusion for Persons Living With Disabilities in Vihiga'(2025) https://www.standardmedia.co.ke/western/article/2001531509/stakeholders-push-for-digital-inclusion-for-persons-with-disabilities-in-vihiga (accessed on 30 November)
44. Communications Authority of Kenya 'Industry Guidelines For Child Online Protection and Safety In Kenya April 2025' https://www.ca.go.ke/sites/default/files/2025-04/%20Industry%20Guidelines%20for%20Child%20Online%20Protection%20%28COP%29%20and%20Safety%20in%20Kenya_Apr2025.pdf (accessed on 19 February 2026).

processing children's data. These notes emphasise verifiable parental consent, age-verification mechanisms, and high-risk processing data protection impact assessment.[45] Importantly, the Kenya Children Policy (2025) flags barriers to digital inclusion for children, such as digital literacy gaps and urban-rural disparities and reinforces the need for equitable access, infrastructure, and training.[46] Undoubtedly, these policy frameworks are pivotal in enabling children to safely learn, access, create, and participate online.

Universal Service Fund

According to a Key Informant Interview conducted in December 2025 with an official from the Communications Authority of Kenya, the Universal Service Fund (USF) continued to expand ICT access in unserved and underserved areas through infrastructure deployment and targeted subsidies. As at July 2025, the Voice Infrastructure Project (Phases 1–4) had a cumulative allocation of approximately KES 6.43 billion (approximately US$49,748,549), with Phase 1 completed (76 sub-locations), Phase 2 ongoing (69 of 101 sub-locations covered, expected completion in FY 2025/26), Phase 3 underway (10 of 68 sub-locations connected), and Phase 4 at contract preparation stage. Under the Fibre Infrastructure and Services Project (Digital Superhighway Project – DSHP), 2,193 km of fibre had been deployed, and 541 out of 608 targeted government institutions connected under Phase I, with completion expected by December 2025. Phase II, targeting 3,868 government offices across all 47 counties, had completed site surveys and network designs and was scheduled for implementation through June 2026. In addition, Digital Terrestrial Television (DTT) broadcast infrastructure for Mandera, Marsabit and Turkana counties had been tendered in June 2025.

Beyond infrastructure expansion, the USF supported sector-specific digital inclusion initiatives in 2025. These included the enhancement of access to educational content for learners with print disabilities (30% complete, targeting 1,000 learners), the fully operational Kenya Education Cloud Open Educational Resources Portal, the Judiciary Automation Project covering 42 court stations across 27 counties, and the Kenya Agricultural Content Digitisation project (approximately 85 per cent complete, targeting 9,400 farmers). The interview further indicated that USF projects undergo annual audits conducted by the Office of the Auditor General. While these developments reflect continued state investment in bridging the digital divide, several projects will extend into FY 2026/27 and 2027/28, underscoring the importance of sustained oversight, timely delivery, and long-term impact assessment.

45. ODPC 'Guidance Notes for Processing Children's Data' https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-%E2%80%93-Guidance-Note-for-Processing-Childrens-Data.pdf (accessed on 19 February 2026).
46. National Council for Children Services 'Kenya Children Policy' https://www.nccs.go.ke/sites/default/files/resources/Draft%20Kenya%20Children%20Policy.pdf (accessed on 19 February 2026).Egypt: artificial intelligence readiness assessment report https://unesdoc.unesco.org/ark:/48223/pf0000395173?posInSet=1&queryId=39fff3b8-75bb-433c-a655-aef57bffb73d

Conclusion

Kenya's 2025 digital rights landscape is defined simultaneously by progress and state overreach. Ambitious investments in connectivity, e-government, data protection, and emerging technologies have expanded digital opportunities and reinforced Kenya's status as a regional tech leader. These gains, however, coexist with internet disruptions, intrusive surveillance, pervasive data abuses, criminalisation of online expression, and persistent impunity by security agencies. High costs, poor infrastructure, and inaccessible design continue to exclude rural, low-income communities and persons with disabilities from meaningful digital participation. Without stronger safeguards, accountability, and inclusive policy implementation, technological progress will deepen inequality and erode constitutional guarantees, rather than advancing rights and social justice.

Recommendations

The Government should:

- Establish harmonised rules on cross-border data transfers, data localisation, and cloud contracts to ensure that Kenyan public data and sensitive information are protected under Kenyan law.
- Expand affordable connectivity by prioritising infrastructure in rural, informal, and marginalised communities,
- The Communications Authority of Kenya should put in place an effective and transparent tracker for the Universal Service Fund where the public and different stakeholders can monitor use of funds and progress of projects.
- Amend provisions in the Computer Misuse and Cybercrimes Act and regulations regarding "publishing false information," "impersonation," "vague cyber crimes," and broad categories of electronic communications that impinge on the tenets under Articles 33 and 35 of the Kenyan Constitution (2010), ensuring they relate to clearly identified and deliberate harm rather than critical commentary or satire, and that most offences related to online publishing are handled in civil lawsuits.

The media should:

- Use human-interest storytelling and data-driven journalism to demonstrate how restrictive ICT policies and digital disruptions result in the disenfranchisement of deprived and marginalised com
- munities from basic services, and highlight ways to foster successful inclusion.
- Investigate government partnerships with private developers in the deployment of surveillance and propaganda technology, and engage the public in evidence-driven discussions about the impact of such technology on democracy.
- Leverage the Media Council of Kenya and the Kenya Editors Guild to systematically challenge broadcast bans and gag orders in court, to obtain declarative relief and sustain judicial jurisprudence on protecting media freedoms and access to information.

The private sector should:

- Implement child online safety compliance by applying the ODPC child-data guidance and the CA child online protection expectations.
- Align organisational AI deployments with Kenya's AI strategic goals, including model development, data governance, and scalable innovation.
- Lending firms should uphold fair collection standards and lawful independent escalation channels during debt recovery.

The Score Index

Kenya, 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	2	There were restrictions on access to the social media platform Telegram during national exams. There was also recorded internet throttling during the June 2025 protest
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	3	3	There are various laws and policies, including the Universal Service Fund, aimed at promoting affordable internet access across the country
False News Criminalisation	P22(2)	1	2	Computer Misuse and Cybercrimes (Amendment) Act 2025 criminalises the spreading of false news; however, there are concerns that have required judicial intervention
Sedition Legislation	P22(2)	2	3	Despite concerted efforts by the state to criminalise sedition the judiciary has been steadfast in upholding the constitutional spirit of freedom of expression
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	2	There were numerous arbitrary arrests and harassments of activists during protests and after
Data Protection Legislation.	P42	5	5	Data Protection Act (2019) safeguards Kenyans' personal data, regulates its use by state and private actors, and establishes an independent data protection commission for oversight. The office was particularly active in 2025 and went after top lending apps and companies
Online Content Removal Without Process	P38 and P39(4)	4	2	The Computer Misuse and Cybercrimes (Amendment) Act 2025 grants the state powers to remove online content they deem "unacceptable" on social media
Invasion of Privacy of Communications	P41	1	2	The government, through its security agencies, have been accused by reputable international watchdog Citizen Lab of installing spyware on some of the makers of the "Blood Parliament" documentary that led to the death of finance bill protesters
Failure by the government to proactively disclose and disseminate information on digital technologies.	P29(3)	3	3	The Access to Information Act (2016), together with Article 35 of the Kenyan constitution, guarantees citizens access to information of national importance held by the state.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
AI and Emerging Technologies national strategies	P39(6)	3	5	Kenya launched the national Artificial Intelligence Strategy 2025–2030, focused on establishing strong AI governance and growing the local AI ecosystem in the country
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	3	5	Kenya utilises a patchwork of legal frameworks, such as the Computer Misuse and Cybercrimes (Amendment) Act 2025, the Children Act, 2022, the Industry Guidelines for Child Online Protection and Safety in Kenya (CA, April 2025), ODPC Draft Guidance Note for Processing Children's Data (2025), to foster children's online digital safety and privacy. There are also established state departments set aside to handle children safety matters.
Digital Inclusion	P37(3)	2	3	Kenya has expanded connectivity through the Universal Service Fund and national fibre rollout; however, there is need to have a publicly available USF tracker. There are still affordability and accessibility gaps for persons with disabilities as well as poor and rural communities
Total (out of 60):	2024: **34**		2025 **35**	



Lesotho

Sibongile Mokapane

Executive Summary

This report analyses Lesotho's digital rights landscape through a combination of research methods. A desk-based study was used to explore existing qualitative data and in-person interviews were used to collect primary data. A tailored index, TheScore, developed by Paradigm Initiative, is used to score Lesotho's compliance with the Declaration of Principles on Freedom of Expression and Access to Information, 2019.

The research discusses the state of internet access and network coverage, legal and institutional frameworks on data protection, cybersecurity, access to information, censorship and content moderation, and the compliance of Lesotho with its obligations to respect and promote the right to freedom of expression.

The Londa Lesotho 2024 report analysed legislative and policy developments, their

critical gaps, and the overall progress of digital development and made recommendations . This report assessed the same progress and highlights that affordability of connectivity, and existence of pre and post independence laws post a threat to free media. Further that, the lack of laws on content moderation, access to public information, and the operationalisation of the Data Protection Commission, and availability of information regarding the projects and expenditure of the Universal Service Fund (USF) are of concern. The Cybersecurity and Computer Crimes Bill, 2024 (CCCB) and Receipt and Access to Information Bill, 2021 have still not been passed into law. The reports further highlight progress on several digital policies and strategies adopted for Lesotho's digital transformation. The report highlights that there has been minimal progress within Lesotho's digital landscape and has earned a score of 36 on the Score Index.



Introduction

Since the 2024 Londa report, the digital rights landscape has not seen much progress. Internet access and network coverage seem to be the only thematic areas where there has been progress. The cost of broadband access is still a concern. The absence of a Data Protection Commission has contributed to the stagnation of updated data protection standards. Additionally, there is a regression in respect to media freedom by security agencies. The lack of a legislative framework to access public information has been. This represents slight compliance with the African Commission on Human and Peoples' Rights' (ACHPR) Declaration of Principles on Freedom of Expression and Access to Information in Africa (the Declaration), 2019. During the year under review, Lesotho adopted its National Digital Transformation Strategy, 2024-2030 and the National AI Policy, 2025. However, the State keeps regressing because of its interference with individuals' right to freedom of expression online

Internet Access

As of November 2025, Lesotho's internet penetration rate is between 47% and 50.25%, with most coverage in urban areas.[1] With approximately 69% of the population living in rural areas, there is a significant gap in digital access geographically, especially in remote and mountainous regions. The telecommunications company, Starlink, promises to extend reliable, high-speed internet and sees itself as a catalyst for digital inclusion and innovation in Lesotho.[2]

Despite the presence of local Internet Service Providers (ISPs) such as Leo and Jenny, Vodacom Lesotho and Econet Telecom Lesotho are still the two leading telecommunications companies that offer internet services.. All these corporations are regulated by the Lesotho Communications Authority (LCA), an

1. Statistica, 2025. "Digital & Connectivity Indicators – Lesotho" https://www.statista.com/outlook/co/digital-connectivity-indicators/lesotho. [Accessed on 16/11/2025]
2. https://newsdayonline.co.ls/t-connects-vision-for-transforming-connectivity-in-lesotho

independent authority that grants licences to all telecommunication companies and develops principles of governance for the industry, including ISPs.[3]

The Lesotho Communication Authority (LCA) in 2024 adopted the Lesotho Communications Authority Quality of Service Rule, 2023. The objective of the rules was to set minimum standards for the quality of services provided by telecommunications entities, such as the standards for network coverage and web browsing parameters. It prescribes that establishing an Internet Protocol (IP) connection to a web server should be less than eight seconds, while the average data transfer for downloading to be a minimum of 5Mb per second and 25 Mb per second for 3G and 4G connections, respectively. The Rules further made provisions for monitoring compliance from licensees and have the power to impose sanctions of at most LSL two million (approximately USD 119, 560)[4]. To date the regulations remain in force and have not been amended.

In 2025, broadband in Lesotho showed moderate performance but mixed affordability for the general public. Average internet speeds of around 14 Mbps indicate a basic but not highly competitive level of connectivity, although some providers offer faster mobile speeds in specific cases.[5] While fixed broadband contracts are generally more cost-effective than prepaid data, many people still rely on prepaid options, which can become expensive relative to income despite small entry packages. [6]Even though there are somewhat affordable bundles and uncapped plans available, overall internet access remains only moderately affordable, suggesting that cost can still be a barrier for widespread, consistent use across the population.

3. Established by section 3 of the Communications Act, 2012.
4. Rule 7 and of the Lesotho Communications Authority Quality of Service Rules, 2023
5. The average broadband connection speed is 14 thousand kilobits (or 14 megabits) per second (Mbps) from both Econet Telecom Lesotho and Vodacom Lesotho. https://www.vodacom.co.ls/business/fixed-solutions/, https://www.etl.co.ls/personal-data-packages/?package=ADSL&plan=Unlimited, [Accessed on 16/11/2025].
6. Vodacom Lesotho offers entry prepaid data at 35MB for LSL 3 (approximately USD 0.060) and 10GB for LSL 99 (approximately USD 6), and uncapped data of a 10 Mbps package for LSL 350 (approximately USD 21) per month. Econet Telecom Lesotho offers data bundles from LSL 6 (approximately USD 0.36) for 500MB and the ADSL/Fixed Internet package for LSL 99 for 10GB https://www.vodacom.co.ls/business/fixed-solutions/, https://www.etl.co.ls/personal-data-packages/?package=ADSL&plan=Unlimited, [Accessed on 16/11/2025].

Online Freedom of Expression and Access to Information

Principle 10 of the Declaration on Freedom of Expression and Access to Information, 2019 provides that freedom of expression includes seeking, receiving and disseminating information through various media and platforms.[7] The right facilitates the tenets of media freedoms such as the protection of journalists and publishing houses, their diversity, independence, and balanced governance by the state or independent authority.[8] Recognition of the right itself entails a nuanced understanding of how different target groups enjoy it and how its violation disproportionately affects each group. This entails exploring themes such as gendered disinformation and its interrelatedness with other issues such as Technology Facilitated Gender Based Violence(TFGBV).

Section 14(2) of the Constitution, 1993 limits the right on the grounds of public health, order, safety, morality, and reputation of others, and restricts public officers[9]. The Sedition Proclamation No.44, 1938 has not been repealed and makes seditious intent and possession of a seditious publication an offence under Section 4. It criminalises all conduct that incites hatred or discontent about government leadership and the administration of justice. This may encourage censoring both the public and media in holding the government accountable for its policies and decisions, or requesting transparency.

Section 10(1) of the Printing and Publications Act, 1967 makes it an offence to produce and disseminate information that has the potential to disturb public order or safety. The Internal Security Act, 1984 makes subversion an offence regardless of whether such statements were communicated within or outside of Lesotho's borders[10]. Section 8 therefore makes abetting

7. Part II Principle 10 (n1).
8. Part II Principle 11 to 16 (n1)
9. Section 14(2) of the Constitution of Lesotho 1993. https://www.constituteproject.org/constitution/Lesotho_2018 [Accessed on 14/11/2024].

subversion through monetary and/or property contribution an offence, and Section 34 also makes it an offence to utter or publish statements that could incite public violence.

The Computer Crime and Cyber Security Bill, 2024, a proposed legislative framework designed to address rising digital threats, has still not been passed into law. As stated in previous editions of the Londa report, the Bill continues to raise similar concerns over its provisions, including one that could criminalise publishing "false information" and Part IV of the Bill, which are broad and vague. This could be used to limit free speech, force self-censorship among journalists, and restrict citizen's access to verified information. Its enactment will be a major regression in Lesotho's democracy. The Bill is commended for penalising xenophobia, racism, image-based abuse, online fraud, and hacking; however, other prescribed offences threaten democratic dispensation, limiting free media and access to information.

Lesotho currently has no laws on online content moderation and censorship. In the previous years, the National Security Service (NSS) was accused of monitoring citizens and journalists online. The Constitutional Court declared a section of the NSS Act, which allowed the authority to seize and search mobile phones without a court order, as unconstitutional.[11]

Platforms like Facebook and the X app have become significant forums for political debate and criticism of the government. One notable case of limited freedom of expression is the June 2025 detention of Tšolo Thakeli (also known as Tjeka-Tjeka), a youth activist who was detained for posting a video on Facebook, where he criticised the government's failure to deliver on its promises of job creation for youth. He was later charged with sedition and inciting public violence. Another arrest was that of Mohalenyane Phakela, the editor of Lesotho Times and Sunday Express, a local newspaper and online news provider, in August 2025 by the Directorate on Corruption and Economic Offences (DCEO) in

10. Section 7 of the Internal Security Act, 1984. https://www.vertic.org/media/National%20Legislation/Lesotho/LS_Internal_Security_General_Act.pdf [Accessed on 10/10/2024].
11. Authorities in Lesotho attempt to block social media. https://monitor.civicus.org/explore/lesotho/?utm [Accessed on 14/11/2025]

connection with a story published in the newspaper.[12] This case highlighted the potential for arrests around sensitive content, with authorities issuing warnings against subversive posts online. These cases have raised significant concerns among human rights activists and media freedom organisations.

Access to Information

The Declaration affirms that access to information is a right to seek information from both public and parastatal entities in a timeous and affordable manner, especially where such information is vital in protecting other rights.[13] It prescribes that any enacted law on access to information should take preference over other Acts that seek to prohibit such access and any attempt to limit the right should be based on exhaustive exemptions.[14] Additionally, state entities should create, manage and provide comprehensive information that is of public interest.

In practice, there are no existing laws to facilitate access to public information in Lesotho. There are, however, laws that are restrictive, such as the Official Secrets Act, 1967 and the Public Service Act, 2005. Provisions in these laws restrict and make it an offence for public servants to grant access to "confidential" state information without authorisation. As a result, requests for information from government entities have been challenging for individuals and professionals, as there are no set guidelines for such requests or for justifying denials.[15]

However, this can be proven to occur not only in government entities but also in privately owned entities. During the collection of data for this report, several unjustifiable restrictions from non-state actor entities were imposed, citing management prohibiting employees from commenting on anything company or organisation-related or even from giving

12. https://groundup.org.za/article/lesotho-times-editor-wrongfully-arrested-admits-anti-corruption-agency/ [Accessed on 20/11/2025]
13. Principle 26 (1) (a) and (b) of the Declaration of Principles on Freedom of Expression and Access to Information, 2019.
14. Principles 27 and 28 of the Declaration of Principles on Freedom of Expression and Access to Information, 2019
15. MISA, "Access to Information" (2024) https://lesotho.misa.org/issues-we-address/access-to-information/ [Accessed on 16/11/2025].

data collectors access to archives of information which would normally fall under the public domain.

The Receipt and Access to Information Bill, 2021 has not yet been passed into law despite its enactment enabling access to information from the government, its agencies, and departments that is of public interest. It was applauded for its intention to appoint information officers and their contact publicised to expedite information requests[16]. Section 20 of the Bill prescribes 30 days for an information officer to make a decision on a request and to notify the requester. Failure to make such notification is deemed to be a denial of a request and entitles the requester to an appeal.[17] Interestingly, the legal officer has discretion to deny a request if they consider the information frivolous or vexatious. These wide discretionary powers threaten timeous access and subject the requester to stringent processes of appealing the denial. Other grounds for denial include for privacy of individuals, if the requestor is a minor, to protect third-party trade secrets, confidential state information, public safety and/or national security[18].

The lack of existing frameworks or systems to access information from government bodies is still a challenge that requires immediate intervention.

Gendered Disinformation and Technology Facilitated Gender Based Violence (TFGBV)

The 'Digital Rights in Lesotho' 2023 report by University of Pretoria's Centre for Human rights recognised the existence and disproportionate impact of online violence against women and its ramifications to impede their political participation, especially engaging in polarised discourse or running for elections, and made policy and legislative recommendations to address these concerns[19] such as ensuring capacitation of women to navigate the digital sphere and the amendment of some domestic legislation. The Counter Domestic Violence Act, 2020 is the only law that explicitly criminalises TFGBV under Section 3(k). However, the provision is overly broad and conflates various forms of misconduct into a single criminal act without distinguishing among them. This poses a threat to certain crimes carrying disproportional penalties and therefore unbalanced when it comes to the rights and interests at play.

Data Protection and Cybersecurity

The Data Protection Act, 2011 protects personal information and includes provisions for civil claims. The Act is the primary legislation governing data privacy in Lesotho, broadly defining personal information to include anything that can identify an individual, such as their image. It generally requires that personal information be collected directly from the data subject and with their explicit consent. It specifically entrenches a civil claim for damages for individuals whose rights are breached.[20] However, a current challenge in Lesotho is the lack of a functioning Data Protection Commission, which means that individuals have no effective recourse for data breaches or misuse, except through the courts.

A significant recent notable case, which could set a precedent for image rights, is that of Adv. Lemohang Nzuzi vs. Lesotho Mounted Police Service (LMPS), where an attorney filed a constitutional case challenging the police's practice of posting suspects' photographs and personal details on social media before trial, arguing it violates constitutional rights to dignity and privacy.[21] This case highlighted the misuse of images by a state actor. The case has not been finalised.

16. Section 4 and 7 of the Receipt and Access to Information Bill, 2021 https://www.osall.org.za/docs/2011/03/Lesotho-Access-and-Receipt-of-Information-Bill-2000.pdf [Accessed on 16/11/2025]
17. Section 23 of the Receipt and Access of Information Bill, 2000 (n32).
18. Section 34,35(a), 36,37 and 38 of the Receipt and Access to Information Bill, 2021 (n32)
19. M.R Kulehile, 2023." Digital Rights in Lesotho: A Situational Analysis. ' Centre for Human Rights. PULP https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Digital_Rights_in_Lesotho_Report.pdf?utm_source=chatgpt.comhttps://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Digital_Rights_in_Lesotho_Report.pdf?utm_source=chatgpt.com at page 55. [Accessed on 10/11/2026]
20. African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) Freedom House.
21. https://lestimes.com/lmps-sued-m1-5m-over-facebook-post/ [Accessed on 14/12/2025]

Copyrights over personal images in the context of privacy are a concern, especially when the Data Protection Act exempts the use of such images in journalistic or literary use to fall beyond its scope.[22] Certain provisions of the Act need to be updated to comply with international data protection and privacy standards. This includes Section 23, which provides that a breach should be reported within a reasonable time and not within a specific timeframe, such as 24 hours.[23] While the Data Protection Commission is not yet operational, the Act is in enforcement and businesses are expected to comply. Due to the absence of a Data Protection Authority, there is no recourse or complaints mechanism for reporting breaches. Therefore, there is no record of breaches that may have occurred.

Privacy and Surveillance

There are cybercrime laws in Lesotho, and the lack of implementation of the Malabo Convention affects marginalised groups due to several systemic and institutional issues. Marginalised communities often have limited access to information and awareness about their digital rights and available legal remedies. This makes it difficult for them to understand when and how their data has been used or misused or to seek redress. There are some concerns around the processing and use of biometric data, especially for surveillance.[24]

The CCCB, 2024 raises further concerns about surveillance. Section 23 on illegal interception criminalises unauthorised interception and dishonest transmission of private data and imposes a penalty of LSL10,000 (approximately US$ 625) or 15 years' imprisonment. Although not expressly stated, this implicitly recognises that authorised interception exists. Section 64 grants law enforcement surveillance powers through obtaining court orders requiring disclosure of traffic data. Section 66 grants power to install remote forensic tools on suspects' computer systems, to collect evidence including "keystroke logging or transmission of an internet protocol address", as well as monitoring and data collection from suspect devices. This type of regulation already poses a threat to individuals' right to privacy as there are no safeguards

Open-source reporting on the procurement of commercial surveillance tools is nonexistent. However, regulatory measures such as mandatory SIM registrations raise concerns regarding privacy and potential surveillance of their movements. Registration of each SIM requires biodata, including a photograph of the user and a copy of their identity document. Therefore, movement can be traced via mobile towers that the user's mobile device connects to. This takes away an individual's freedom and option for anonymity, or control over how such data is captured and processed. The absence of procurement transparency and independent review, acquisition of monitoring/disinformation-tracking systems further creates more discomfort as citizens are not informed about the existence and/or deployment of surveillance technology within the country.[25]

Lesotho collects biometric data in national identity and civil-registration programmes, including fingerprints and facial images. This biometric national-ID architecture is explicit in official project documents. Recently, the country has been rolling out SIM re-registration drives that also require national ID/biometric verification , which links telecom identifiers to state identity records and raises risks of aggregation and linkage of mobility and communication metadata to biometric identity.

Developments in ICT and Emerging Technologies

The Draft National Digital Policy, 2024, the National AI Policy and the National Digital Transformation Strategy 2024-2030 are Lesotho's current AI frameworks. The National Digital Policy marked the first attempt to articulate priorities for digital transformation. The policy recognises the potential of AI, Blockchain, Biotechnology and Internet of Things (IoT),[26] with the aim

22. Section 4 (d) of the Data Protection Act,2011
23. Section 4 (d) of the Data Protection Act,2011
24. https://www.lena.gov.ls/ai-surveillance-changes-how-journalists-work/ [Accessed on 14/12/2025]
25. Kulehile, M.R, 2024, Digital Rights in Lesotho: A Situational Analysis. Centre for Human Rights, PULP.

to strengthen legal and institutional frameworks for emerging technologies and envisions new digital-governance institutions such as the Chief Digital Officer, the National Digital Council and the National Digital Agency, setting its implementation horizon to 2035.

While the policy is commendable, it does not yet provide ethical guidelines for AI development and deployment, human rights safeguards, standards for accountability, transparency and fairness. It also does not cater for the data governance models needed for AI systems, oversight mechanisms, or regulatory enforcement capacity. However, it mentions critical entities to be established by the CCCB, 2024, such as the National Cybersecurity Advisory Council and the National Cybersecurity Incident Response Team (CSIRT), which will be responsible for coordinating cybersecurity measures and safeguarding any digital infrastructure and improving their resilience.

As a complement to the draft policy, Lesotho has also launched the National Digital Transformation Strategy 2024-2030 and the National AI Policy alongside the Ministerial Strategy.[27] These two roadmaps are designed to guide Lesotho into a more connected, innovative, and digitally empowered future over the next five years. During the review of the second draft of the National AI Policy, the Centre for AI and Digital Policy recommended that the policy adopt the UNESCO Readiness Assessment Methodology (RAM) and Ethical Impact Assessment (EIA).

Digital Inclusion

Digital inclusion, trust and safety are foundational requirements for equitable participation in the digital society. Achieving inclusion involves meaningful access, safety and trust of digital platforms for everyone, including children, by adopting and enforcing child online safety laws, strengthening digital literacy and removing barriers that prevent vulnerable groups from fully exercising their digital rights.

LCA's Child Online Protection Guidelines, 2024 which were launched in February 2025,[28] have been designed to create a safer digital environment for children, covering their online rights, protecting them from online abuse and capacitating responsible internet use. The guidelines adopted a multistakeholder and multifaceted approach to child protection online. It recognises the rights and responsibilities of children as internet users. It additionally sets obligations for parents and guardians, mobile and internet service providers, as well as content service providers. The Guidelines are, however, lacking with regard to the enforcement of these measures through collaboration with security sectors. There is also a need to strengthen the Guidelines through legislative measures that would criminalise and/or penalise conduct that violates children's rights and safety. The Cybersecurity and Computer Crime Bill, 2024, under Part IV, is the only proposed legislation that may criminalise child sexual abuse content in image or video format. Section 29 of the Data Protection Act, 2011 makes provision to the effect that a child's personal information shall only be subject to processing with parental consent

Universal Service Fund (USF)

The Universal Service Fund is administered by the LCA and partners with local corporations on connectivity initiatives. With a financial contribution from Vodacom Telecom Lesotho, the State Library in Lesotho has opened a new Insight Centre for visually impaired persons.[29] The centre has a braille translator and printer, and assistive reading devices. However, the LCA has not been willing to disclose USF funding or project activities and does not have any public reports of the same. The 2025 USF funding is therefore unknown. In previous reports, the LCA declined to disclose the financial records of the Fund, and this lack of disclosure and transparency contradicts the core principles of the ACHPR Declaration.

All telecommunications companies are required to contribute up to 2% of the net operating income to the Fund, part of which is used to expand network access to underserved and rural areas.

26. Priority 8 and 11 of the National Digital Policy, 2024 Draft [unpublished].
27. https://www.gov.ls/government/national-digital-transformation-is-launched/ [Accessed on 17/12/2025]
28. Lesotho Communications Authority, 2025. Child Online Protection Guidelines https://lca.org.ls/legislation/ [Accessed on 18/03/2026]
29. Vodacom Lesotho Impact Booklet. (October 2024) https://www.vodacom.co.ls/assets/uploads/docs/Vodacom_Lesotho_Impact_Booklet_Oct_2024.pdf

Conclusion

The digital rights landscape in Lesotho has the potential to guarantee meaningful and safe participation online through various frameworks and strategies. Implementation is still a great challenge and therefore brings to light why there is a stark difference between paper and reality on the ground. Accessibility and internet connection are one of the categories that the country has made significant strides in, with about 65% coverage across the country. With the USF, digital inclusion is another low-hanging fruit that both the public and private sectors could leverage to ensure no one is left behind, both in ICT development and discourse as stakeholders. The government has taken strides to prepare for emerging technologies by developing a National AI Policy and the National Digital Transformation Strategy, 2030, which will be Lesotho's roadmap for governance of such innovations.

However, the insufficiency of existing legal and institutional mechanisms to promote and protect digital rights is of great concern, particularly in protecting personal data and privacy. The lack of a data protection authority to regulate, as well as potential threats to surveillance. Another concern is the respect of the right to freedom of expression of citizens, activists and journalists. They are often subjected to harassment and intimidation by security institutions. Their right is also unjustifiably limited by existing laws, and faces potential threats from the draft Computer Crimes and Cybersecurity Bill, 2025. Lack of progress on draft bills, such as the Receipt and Access of Information bill, is another issue that requires urgent attention. The insufficiency of policy and legislative frameworks that address children's online safety and privacy is another issue that needs to be addressed with urgency. Lesotho's overall score is 34 as its compliance is mild and has critical gaps to be addressed in terms of its systems, institutions and legal measures.

Recommendations

The Government should:

- Pass the Receipt and Access of Information Bill 2021;
- Amend the wording of the offences in Part IV and their penalties of the CCCB, 2024 to address the potential threat of free media access to information in the interest of the public, and the right to freedom of expression as a whole.
- Ensure the operationalisation of the Data Protection Commission by allocating a budget to fund the Data Protection Secretariat.
- Repeal the Sedition Proclamation No. 44,1938 entirely; section 10(1) of the Printing and Publications Act, 1967.
- Adopt the National Digital Policy.
- Develop laws and policies on content moderation, children's online safety and meaningful connectivity for education.

Civil Society Organisations should:

- Provide financial and technical support to initiatives, programs and projects that advance digital rights and inclusion in Lesotho.

Regulators (Lesotho Communications Authority and Data Protection Commission) should:

- Develop regulatory principles and guidelines on an equitable approach to broadband affordability and ensure intermediaries, MNOs and data processors' policies and standards align with international human rights standards.

Private Sector should:

- Partner with other relevant stakeholders and contribute technical skills, fiscal contribution and/or a platform for discourse on emerging tech development.
- Develop internal policies/codes of conduct that align with international human rights standards and report on content moderation and user data requests.

Academia should:

- Conduct relevant research to inform government policies and strategies on AI and emerging technologies, their governance and their potential social impact.

The Media should:

- Raise awareness of emerging issues in technological development and governance, and facilitate public discourse platforms.

The Score Index

Lesotho, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	4	4	Although there have been no reported internet shutdowns in Lesotho, the absence of legal frameworks that align with human rights standards on the right to freedom of expression online raises concerns about potential future shutdowns.
Inexistent laws, policies and other measures to	P37	4	4	The National Digital Policy intends to promote internet access. However, broadband affordability is a current hurdle to meaningful connectivity in Lesotho.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
promote universal, equitable, affordable and meaningful access to the internet				
False News Criminalisation	P22(2)	3	3	Although there is no specific legislation criminalising false news. The proposed penalty for disinformation by the Cybersecurity and Computer Crimes Bill, 2024 is not proportional to the threat or harm caused by such misconduct.
Sedition Legislation	P22(2)	1	1	There is a Sedition law in existence which has not been repealed. Although it has not been applied for some time, its existence is still a threat and limits the right to freedom of expression.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	The June and August 2025 incidents where a youth activist was arrested and the journalist falsely arrested are great concerns for threats against the right to freedom of expression. There have only been two recorded incidents in 2025.
Data Protection Legislation.	P42	4	4	There has been a law in place since 2011 but no Data Protection Commission to enforce it. There is also a need to revise a few provisions to align with current international standards on data Protection and Privacy.
States interfere and require the removal of online content by internet intermediaries	P22(2)	3	4	There has been only one request on Meta and none from Tiktok for content takedown by the government
Invasion of Privacy of Communications	P41	3	3	There is no law governing surveillance, particularly of private communication. MNOs have adopted internal policies to only issue out information requested if ordered by a court of law as of 2023.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	2	2	Several government departments maintain websites and social media accounts. However, the greatest challenge is the lack of up-to-date, relevant public-interest information on these platforms.
AI and Emerging Technologies national strategies	P39(6)	2	3	The National AI Policy and the National Digital Transformation Strategy, 2024-2030 are the two frameworks on ICT development, in particular emerging technologies such as AI and comply with the UNESCO RAM and EIA.
Adoption of specific child laws, policies	P37(5)	1	3	In 2025, the LCA developed guidelines on Children's online safety.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
and measures promoting children's digital safety and privacy online				
Digital Inclusion	P37(3)	1	3	The USF within the LCA has played a vital role in improving network coverage in Lesotho through collaboration with the private sector to establish a centre for PWD to access assistive technologies.
Total (out of 60):	2024: **31**		**2025 35**	



Malawi

By Charles Kajoloweka

Executive Summary

This report examines the state of digital rights in Malawi, focusing on key achievements and concerning regressions observed in 2025. It provides actionable recommendations for both government and non-state actors, grounded in empirical evidence and desk research. The analysis evaluates quantitative and qualitative aspects of digital rights and governance, offering a comprehensive view of the country's digital landscape. Specifically, the report dissects seven key digital spheres: Internet access, Freedom of expression, Data Protection and Privacy, Censorship and content moderation, Access to information, AI and Emerging Technologies, and the Universal Service Fund. It presents a contextual analysis of these thematic areas and provides actionable recommendations for both state and non-state actors.

While in the reporting period, Malawi made some notable gains in expanding

and safeguarding digital space, including the historic repeal of criminal defamation law by the Constitutional Court, its overall performance on The Score Index developed by Paradigm Initiative (PIN) improved from 35 to 36 out of 60 and is rated “moderately compliant”.[1] The improvement is attributed to a better legal protection environment for digital rights, including the repeal of criminal defamation, the UNESCO AI assessment, and the promulgation of the Data Protection Act Guidelines.



1. Londa Score Index is a digital rights index developed by Paradigm Initiative that evaluates compliance of the country with regard to key human rights elements and is inspired by the African Commission on Human and Peoples’ Rights Declaration of Principles on Freedom of Expression and Access to Information

Introduction

The period under review witnessed an improvement in internet freedom, with fewer internet users criminally charged for their online expression than the previous year. Additionally, the Constitutional Court repealed Section 200 of the country’s Penal Code, which criminalised defamation, a significant step in upholding the constitutional guarantee of freedom of expression and media freedoms. Malawi also commenced a participatory review of the Communications Act, 2026, to align the regulatory framework with rapid technological advancements, market developments, and stakeholder needs. Malawi also made significant strides in expanding access to information, particularly in the context of the September 16 2025 elections. Additionally, initiatives rolled out under the Universal Service Fund (USF) represented significant progress toward expanding digital access for the offline majority.

Despite these gains, several challenges persisted. While there were reduced cases of online crackdowns in the year as compared to previous years, authorities continued to arrest online users for their online expression. The official criminalisation of speech remained a significant concern. There were also strong suspicions of government surveillance ahead of the September 2025 general elections. The Government’s increase of Value Added Tax (VAT) from 16.5 to 17.5% on all mobile products and services significantly undermined digital inclusion efforts. Other structural challenges, such as high connectivity costs, unreliable electricity, limited rural infrastructure, and low digital literacy, continued to exclude significant portions of the population from full participation in digital systems. The absence of an artificial intelligence legal and policy framework also remained a major gap.

Looking forward, the Malawian government is called upon to review the prohibitive tax policy on ICT services and products, strengthen operational capacity and accountability mechanisms for the National ID system, particularly for replacement and renewal services, and develop regulatory and ethical use standards of artificial Intelligence with proper governance structures and strengthen digital rights principles—access, equality, remedy, and accountability—into all digital public infrastructure by design. While the

Court's decision to outlaw Section 200 of the penal code is welcome, Malawi needs to review other repressive laws that undermine free expression, including Section 60 of the Penal Code, as well as the Electronic Transactions and Cyber Security Act, 2016.

Internet Access And Disruptions

Section 157 of the Communications Act of 2016 provides for Universal Services and Access to Telecommunication. Malawi Telecommunications Regulatory Authority (MACRA), as a regulator, is mandated

> "to ensure that the provision of universal services is made on affordable tariffs that are accessible to all".[2]

Moreover, in 2021 the government rolled out a five-year Digital Economy Strategy (2021-2026), which sets new targets, including expanding internet access from 14.6% to 80% of the population and broadband coverage to 95% by 2026.[3]

In 2025, the official internet penetration rate was at 27.7%.[4] However, the 2025 DataReportal report shows that only 18% of the total population used the Internet by October 2025.[5] Kepios's analysis shows that the number of internet users in Malawi increased by 2.6 per cent% between October 2024 and October 2025. Thus, there were 4.02 million internet users in Malawi at the end of 2025. About 82% of the total population of 24.4 million people remained offline in the year.

Further, Malawi was home to 2.4 million social media user identities in October 2025, representing 10.7%t of the total population.[6] According to Kepios, social media users in Malawi increased by 50% between late 2024 and the end of 2025.[7] Notably, 38% of Malawi's social media users were women, an increase from 35.8% in 2024, while 62% were men.

According to Meta, Facebook penetration in Malawi was at 10.7% (an increase from 6.1% in 2024), with 37.8% of users being women, while 61.7% were men.[8] Meanwhile, Instagram's reach was only 178,000 people, an increase from 130,400 in 2024, equating to 20% penetration growth, with 38.7% of Instagram's users being female, while 60.7 per cent were male. There were only 420,000 LinkedIn users in Malawi, an increase from 290,000 in 2024, with 34.5 per cent female members and 65.5 per cent male members. It is worth noting that women's inclusion across most social media platforms was significantly lower than that of men. This disparity highlights the need for targeted interventions to address the unique challenges faced by women. Similarly, there is also a geographic gulf in internet access between rural and urban areas. In 2025, with a population of 22.4 million people, 19% of Malawi's population lived in urban centres, while 81% lived in rural areas. Telecommunication companies are unwilling to invest in Malawi's remote regions due to the high cost of infrastructure development.[9] According to a 2023 National Statistical Office (NSO) report, 40.7% of people in urban areas had access to the Internet, as opposed to 13.5% of those in rural areas.[10] It is also worth noting that Malawi's electric grid is urban-biased, standing at 62% of urban households, compared with a mere 5% of rural households.[11]

In addition, by October 2025, Malawi registered a total of 14.1 million cellular mobile connections, equivalent to 63%of the total population. Thus, the number of mobile connections increased by 8.6% between the end of 2024 and the end of 2025.[12] According to GSMA Intelligence,

2. Communications Act of the Republic of Malawi, 2016
3. Malawi Digital Economy Strategy, 2021 https://dig.watch/resource/the-malawi-digital-economy-strategy-2021-2026 (accessed 28 December 2025)
4. Ministry of Information and Digitalisation, 2025 "Malawi Digital Readiness Assessment"
5. S Kemp "Digital 2026:Malawi", November 8, 2025, https://datareportal.com/reports/digital-2026-malawi (accessed 28 December 2025)
6. Kemp
7. Kemp
8. Kemp
9. Freedom House "Freedom on the Net 2024 " Malawi: Freedom on the Net 2024 Country Report | Freedom House (accessed 31 December 2025).
10. National Statistical Office, "National Survey on Access and use of Information and Communication Technologies by Households and Individuals in Malawi 2023" "http://www.nsomalawi.mw/images/stories/data_on_line/economics/ICT/Natio.... accessed 22 December 2024
11. The Economist Group, 2022 "The Inclusive Internet Index 2022,"https://impact.economist.com/projects/inclusive-internet-index/2022. (accessed 31 December 2025)

92.5% of mobile connections in Malawi are now considered “broadband”, which means that they connect via 3G, 4G, or 5G mobile networks.[13] A low ICT literacy rate of 62 % also remains a major hurdle to digital transformation.[14]

Despite a persistent digital exclusion landscape, in the reporting year, the government increased its tax policy on all ICT products and services, which in turn increases the cost of internet access. Through its revised national budget, the government introduced the new Value Added Tax(VAT) rate of 17.5% and a new e-money transfer levy.[15]

In Malawi, the telecommunications regulator, Malawi Communications Regulatory Authority (MACRA), requires internet service providers (ISPs) to pay a 3.5% tax on annual sales and turnover, annual license and spectrum fees and a 0.5% tax on all ICT equipment entering the country[16]. Worse still, in the reporting period, the government maintained the prohibitive taxes on ICT services, including 17.5% value-added tax (VAT) on mobile phones, 16.5% on internet services and 10% excise duty on messages and internet data transfers. As a result, mobile service providers raised prices across various products, including internet data. For example, in November, Telecom Network Malawi (TNM), adjusted prices for a 20 GB weekly internet bunder from K9,000 (US$5) to K 9,500 (US$5.4); while the Airtel Malawi’s ‘Morefire Chezani’ weekly bundle, previously priced at K8,000 (US$4.6) and offering 20GB of data, increased to K9,500 (US$5.4) providing 22 GB of data.

Despite the government’s commitment in the Digital Economy Strategy to review these taxes, which are significant drivers of high costs of internet and mobile services, there was no action in the reporting period. These taxes continue to make the costs of ICT prohibitive, impacting the country’s poorest the most, as they are effectively shut off from essential digital communication platforms and important services, such as mobile banking and money services, education, and commercial markets, which could help lift them out of poverty. During the coverage period, there were no internet restrictions, blocking or filtering of protected content imposed by authorities. Social media platforms are widely available, including those critical of authorities.

Freedom Of Expression And Access To Information

Fewer internet users were criminally charged for their online expression, as compared to previous years. It is no coincidence that Freedom House’s ‘Freedom on the Net’ 2025 reports that

> “Internet freedom in Malawi improved during the coverage period”.[17]

On July 16 2025, Malawi celebrated a landmark victory for freedom of expression after the High Court of Malawi, sitting as a Constitutional Court, declared Section 200 of the Malawi Penal Code, which criminalised defamation, unconstitutional.[18] In a unanimous decision, three Constitutional Court justices ruled that the defamation law was a “disproportionate and unjustifiable limitation on constitutional freedom,” especially when civil remedies are already available to address reputational harm.[19]

The court’s decision stemmed from the case of Joshua Chisa Mbele, a social media influencer who challenged the constitutionality of the criminal defamation law following criminal defamation charges for his remarks about a senior military official regarding allegations of corruption.

12. Kemp
13. Kemp
14. The Economist Group, 2022 “The Inclusive Internet Index 2022” https://theinclusiveinternet.eiu.com/explore/countries/performance/read.... (accessed 28 December 2025)
15. Capital FM, October 3, 2025 https://web.facebook.com/CapitalFMMalawi/posts/telecommunications-company-tnm-plc-has-announced-that-it-will-adjust-its-tariffs/1198373518977247/?_rdc=1&_rdr# (Accessed 30 December 2025)
16. M Malakata, “Business, Tech Lobbies Malawi’s Govt to Relax Tax,” ITWeb, January 13, 2022, https://itweb.africa/content/o1Jr5Mx9n8VqKdWL. (accessed 23 December 2024)
17. Freedom House, “Freedom on the Net 2025”. https://freedomhouse.org/country/malawi/freedom-net/2025 (Accessed 30 November 2025 how)
18. Nation Publications Limited ‘Court outlaws criminal defamation provision’, 16 July 2025 https://mwnation.com/court-outlaws-criminal-defamation-provision/ (Accessed 30 November 2025)
19. See Judgement Summary https://cpj.org/wp-content/uploads/2025/07/Ruling-summary-Criminal-Defamation-and-Freedom-of-Expression-ConCourt-Referral.-July-2025-Summary-.pdf (Accessed 29 December 2025)

Welcoming the ruling, a group of civil society organisations stated in a joint statement,

> "This ruling sends a powerful message: in a democratic society, the remedy for offensive or false speech is not imprisonment, but more speech. It is through open dialogue—not the blunt instrument of criminal law—that truth, justice, and accountability are served".[20]

The decision also places Malawi in line with regional and international human rights standards, including guidance from the African Commission on Human and Peoples' Rights and the UN Human Rights Committee, both of which have long urged states to decriminalise defamation. In particular, Principle 22(2) of the African Commission on Human and Peoples' Rights (ACHPR) on Freedom of Expression and Access to Information in Africa (ACHPR Declaration) calls on states to 'repeal laws that criminalise sedition, insult and publication of false news'.

Despite this significant gain, Malawi still has restrictive laws on freedom of expression. Section 60 of Malawi's penal code criminalises publishing false news, with penalties of fines or up to two years in jail, and the 2016 Electronic Transactions and Cyber Security Act makes unauthorised transmission of data or information punishable by a fine of MWK2,000,000 (US$1,153) and a five-year imprisonment. Thus, the Malawi government needs to reform these remaining laws that restrict free expression.

Additionally, while there were reduced incidences of online-user crackdown in 2025 as compared to previous years, Malawi authorities continued to arrest social media users, particularly those critical of authorities.[21] Previous incidents have involved actual court convictions of internet users, detentions, seizure of laptops and phones of journalists, and many arrests. For example, in 2024 alone, the Londa report recorded the arrests of 17 internet users, including journalists.

In March 2025, police arrested social media influencer Julius Mithi over a social media post in which he alleged that over one million Malawian eligible voters' names were deleted in the National Registration Bureau (NRB) and Malawi Electoral Commission (MEC) systems. According to police, the arrest followed complaints from the National Registration Bureau and the Malawi Electoral Commission (MEC). He was charged with publication of false news likely to cause fear and alarm to the public, which is an offence under Section 60 of the Penal Code.[22]

Similarly, in December 2025, police arrested two senior officials of the opposition Malawi Congress Party (MCP), Vitumbiko Mumba and Jessie Kabwira, for allegedly spreading false news and causing public alarm, an offence under Section 60 of the Penal Code.[23]

In 2025, the Media Institute of Southern Africa (MISA) Malawi documented over ten cases of attacks on journalists, including intimidation, disruption of live coverage, and online bullying during the election period. On October 10 2025, a group of men suspected to be the ruling Democratic Progressive Party (DPP) cadres stormed the Malawi Broadcasting Corporation (MBC) Kwacha premises in Blantyre, forced MBC Director General George Kasakula to a live on-air apology to President Peter Mutharika and the DPP before forcing him out of the premises.[24]

Censorship And Content Moderation

In 2025, there were no incidents of the state blocking or filtering, or compelling service providers to block or filter internet content. However, due to the crackdown on social media online users by authorities, including arrests of journalists and ordinary users, self-censorship could not be ruled out.[25]

20. CSOs Joint Statement (hard copy)
21. Paradigm Initiative Press Release, https://paradigmhq.org/press-release-civil-society-groups-call-for-digital-rights-protection-in-malawis-upcoming-general-election/ (Accessed 29 December 2025)
22. A Banda, 28 March 2025 https://web.facebook.com/zbsnews/posts/zbsnewslilongwe-principal-resident-magistrate-benjamin-chulu-has-granted-bail-to/1089719569854079/?_rdc=1&_rdr# (Accessed 29 December 2025)
23. P Malimba 'Mumba, Kabwira Granted Bail', 16 December 2025, https://times.mw/mumba-kabwila-granted-bail/ (Accessed 29 December 2025)
24. MISA Malawi, "2025: The year impunity for crimes against freedom of expression reigned in Malawi" , 31 December 2025, https://malawi.misa.org/2025/12/31/2025-the-year-impunity-for-crimes-against-freedom-of-expression-reigned-in-malawi/#:~:text=In%20the%20year%202025%2C%20journalists,the%20cases%20include%20the%20following: (Accessed 29 December 2025)

Access to Information

The right to information is guaranteed under Section 37 of the Constitution, as well as the Access to Information Act (ATI Act) of 2016. To operationalise the ATI Act, regulations were developed in 2021, and the ATI Unit was established under the Malawi Human Rights Commission (MHRC) to oversee the overall operationalisation of the Act.

In September 2025, Malawi held tripartite general elections to elect the President, Members of Parliament and local government councillors. Thus, access to information was critical for the management of a fair and credible election. According to the Malawi Human Rights Commission,

> "Proactive disclosure of electoral information and adequate voter education were essential for a transparent and credible election, and to reduce misinformation".[26]

According to MHRC[27], Malawi made some notable strides in the reporting period, including training 34 public institutions on the access to information legal framework. Out of these institutions, 70% developed information manuals, and 36,000 information requests were received and processed by various institutions. 96% of the requests were addressed by information holders. The MHRC also recognised and awarded ten best compliant institutions with the ATI Act and conducted monitoring of mainstreaming access to information and electoral civic education across the country, which uncovered gaps and challenges in the electoral civic education, such as not being disability friendly and poor participation of accredited CSOs in civic education due to a lack of funding.

Despite notable progress in expanding access to information, there were critical gaps that need redress. These include non-compliance by information holders and resource constraints facing the MHRC's ability to carry out extensive awareness campaigns, particularly for

25. Freedom House, "Freedom on the Net 2025". https://freedomhouse.org/country/malawi/freedom-net/2025 (Accessed 30 November 2025)
26. Chance Kalolokeska, Key informant, Malawi Human Rights Commission (27 December 2025)
27. Chance Kalolokeska, Key informant, Malawi Human Rights Commission (27 December 2025)

rural communities. The government has not allocated a separate budget for implementing the ATI Act. The MHRC also noted that the "demand for capacity building by information holders declined in 2025, though the level of compliance was not satisfactory across the institutions", noting that enforcement of the Act, where there are no administrative penalties or sanctions, has proved to be problematic.[28]

Data Protection And Cybersecurity

Malawi's Data Protection Act (2024) and National Cybersecurity Strategy (2019–2024) provide a strong legal foundation for safeguarding personal data, promoting privacy and ensuring secure digital transactions. The Electronic Transactions and Cybersecurity Act (2016), which sets standards for data governance and transparency, further supports these efforts.

In the reporting period, the Malawi government was registering voters for the general elections slated for September 2025. While the use of National IDs in the voter registration process was a significant step forward, the integration of National IDs with voter registration systems raised concerns about data integrity. Inaccuracies, such as mismatched data between the ID and voter rolls, were reported. Moreover, there were concerns about the security of voter data, with stakeholders questioning how well the system could protect sensitive information.[29] These concerns raise critical concerns about whether the National ID should be the sole form of identification for voter registration, as it may disenfranchise citizens' right to participate in elections. Other forms of identification beyond the National ID would be necessary to guarantee universal suffrage.

There were no cases related to data breaches enforcement by MACRA or before the courts. Additionally, throughout 2025, government institutions began the early stages of operationalising the Data Protection Act, particularly in relation to digital public services, national databases and emerging uses of data-intensive technologies. In the year, MACRA,

28. Chance Kalolokeska, Key informant, Malawi Human Rights Commission (27 December 2025)
29. Vinicent Kumwenda, Key Informant Interview (31 December 2025)

through the Data Protection Office, published the Data Protection Guidelines and conducted awareness campaigns on the requirements of the Data Protection Act. However, the Data Protection Act's implementation capacity remains limited. Enforcement institutions lack adequate staffing, technical expertise and public-facing complaint mechanisms. Moreover, the law does not yet address automated decision-making, algorithmic profiling or AI-specific risks, leaving gaps as more and more institutions increasingly adopt data-driven and AI-enabled systems.[30]

However, the challenges concerning the Data Protection Act persisted as no legal reforms were undertaken to address the flaws. A 2025 Malawi Digital Readiness Assessment (DRA) by the United Nations Development Programme (UNDP) highlights significant gaps in the enforcement of data protection laws, including a lack of public awareness of various laws. "These findings suggest that even where privacy laws exist, enforcement remains inconsistent or ineffective, leaving individuals vulnerable to data breaches, cyber threats and misuse of personal information."[31]

For example, Section 4 designates MACRA as the Data Protection Authority (DPA), potentially compromising the financial, decision-making, and institutional independence of the DPA.[32]

Additionally, Section 8 (b)(vi)(vii) allows the lawful processing of personal data for "public interest" or "legitimate interests," terms that are vague and undefined. This could grant excessive discretion to data controllers and processors in determining the lawful processing of individuals' personal data.

Further, Section 42 grants MACRA the authority to suspend or cancel the registration of a data controller or processor "of significant importance" based on vague and broad grounds including for not complying "with any provision" of the Act or any term or condition imposed on the registration; or if "there is any other reasonable ground to suspend or cancel the registration".[33] These broad provisions would potentially lead to undue restrictions.[34]

While the Act is a shift in the right direction, significant attention should be given to the gaps in the law to prevent authorities from abusing concerning provisions. To ensure the law is applied effectively, it is also essential to invest in training and public awareness interventions for stakeholders, data controllers, researchers and processors.

Surveillance and Cyber-Security

Malawi's National Cybersecurity Strategy provides key interventions to address cybercrime, protect critical infrastructure, and enhance digital security. The government has also established the Computer Emergency Response Team (CERT), a department within MACRA that acts as a focal point for the coordination of cybersecurity-related issues at the national and international levels. Established under Section 6 of the Electronic Transaction and Cyber Security Act, 2016, CERT takes charge of critical information infrastructure protection actions and serves as a base for national coordination to respond to cybersecurity threats.

In December 2025, the Government of Malawi developed the draft Cybersecurity Policy and the National Cybersecurity Strategy, and conducted validation consultations with stakeholders.[35] This is a critical step to address gaps in existing legislation and enhance the protection of Malawi's digital space.

However, enforcement remains a gap, undermining the effectiveness of legislative efforts. A UNDP Stakeholder's Survey (2024) shows mixed perceptions re-

30. Vinicent Kumwenda, Key Informant Interview (31 December 2025)
31. UNDP Malawi, Malawi Launches First-Ever Digital Readiness Assessment to Guide Inclusive Digital Transformation. 15 May 2025. https://www.undp.org/malawi/press-releases/malawi-launches-first-ever-digital-readiness-assessment-guide-inclusive-digital-transformation (Accessed 30 December 2025)
32. CIPESA 'Analysis of the Malawi Draft Data Protection Bill, 2021' (May 2021) file:///C:/Users/User/Downloads/Analysis-ofthe-Malawi-Draft-Data-Protection-Bill-2021.pdf (accessed 30 December, 2025)
33. Section 42(1) of the Data Protection Act of 2023
34. See the '2024 Londa report - Malawi' for more analysis on Malawi Data Protection Act https://paradigmhq.org/wp-content/uploads/2025/09/Londa-24-Malawi.pdf (Accessed 30 December 2025)
35. C Mulekano, 'Government moves to strengthen cybersecurity framework through policy review', 5 December 2025, https://web.facebook.com/malawinewsagency/posts/mananewsgovernment-moves-to-strengthen-cybersecurity-framework-through-policy-re/1368123351992844/?_rdc=1&_rdr# (Accessed on 28 January 2026.

garding the existence and enforcement of cybercrime laws in Malawi.[36] While 30% of respondents indicated that cybercrime laws exist and are fully enforced, an equal 30% said that they exist but are only sometimes enforced, suggesting inconsistencies in law application and regulatory gaps. In addition, 20% of respondents believe that cybercrime laws exist but are seldom enforced, and 10% report that such laws exist but are never enforced, indicating weak implementation and possible lack of institutional capacity to effectively combat cyber threats. Additionally, 10% of respondents stated that no cybercrime laws exist, exposing gaps in awareness.

In 2025, there were strong suspicions of government surveillance of ICT activities by various stakeholders, including civil society groups[37] due to new reports that authorities had acquired a surveillance system. The Malawi Human Rights Commission (MHRC) launched an investigation into the potential human rights impact of the surveillance system that the Malawi Communications Regulatory Authority (MACRA) procured from Hashcom Ghana Limited to track misinformation and disinformation ahead of the country's general elections.[38] At the time of writing this report, the MHRC had not released its investigation report.

In 2023, there were credible reports about Malawi's procurement of the Cellebrite Universal Forensic Extraction Device (UFED) system, and concerns that police used extraction tools to search journalists' devices.[39] Investigative reports in 2024 revealed that in 2019, MACRA procured the UFED system, a powerful technology designed to access and extract information from electronic devices such as phones and laptops sold by the Israel-based company Cellebrite.[40] MwCERT, MACRA's cybersecurity unit, confirmed that it had access to the tool as of January 2023. MACRA also confirmed that it provides services to the police, military, and intelligence services during cybercrime investigations, though the regulator stated that it follows a search warrant and approval process that requires a court order. However, some sources reported that Cellebrite has since ceased issuing license renewals to several countries, including Malawi.[41]

Ai And Emerging Technologies

In June 2025, Malawi became the 28th African country to successfully complete the UNESCO Readiness Assessment Methodology (RAM) for AI ethics and governance. The assessment supported Malawi to evaluate its capacity to adopt responsible AI technologies, and is part of Malawi's efforts to develop an AI Ethics strategy.[42] The assessment shows that AI governance remains underdeveloped, with no statutory requirements for transparency, explainability, human oversight, or algorithmic impact assessments.[43]

Despite growing policy interest, Malawi did not enact AI-specific legislation or binding ethical standards. This regulatory gap has implications for digital rights, particularly where automated or semi-automated systems are used in public service delivery, revenue administration, agriculture, and civic technologies. Citizens currently lack clear legal protections against algorithmic bias, opaque automated decisions, or misuse of data in AI systems, despite that Resolution 473 of the African Commission on Human and Peoples' Rights calls on State Parties to develop a comprehensive legal and ethical governance framework for AI technologies so as to ensure compliance with human rights standards.

36. Ministry of Information and Digitalisation, 2025 "Malawi Digital Readiness Assessment" https://www.undp.org/sites/g/files/zskgke326/files/2025-05/dra_malawi_report_2025_a4_print.pdf (accessed 28 December 2025)
37. Paradigm Initiative, "Press release: Civil society groups call for digital rights protection in Malawi's upcoming General Election" April 3, 2025, https://paradigmhq.org/press-release-civil-society-groups-call-for-digi.... (Accessed 30 November 2025)
38. E Banda, "MHRC investigates human rights concerns over Macra's K2.6bn surveillance system," Malawi 24, January 23, 2025, https://malawi24.com/2025/01/23/mhrc-investigates-human-rights-concerns... (Accesssed 30 November 2025)
39. Freedom House, "Freedom on the Net 2025". https://freedomhouse.org/country/malawi/freedom-net/2025
40. Freedom House, "Freedom on the Net 2024". Malawi: Freedom on the Net 2024 Country Report | Freedom House
41. E Chimoyo "Unveiling MACRA's sophisticated phone, PC data extracting tool: balancing privacy and security," Platform for Investigative Journalism, January 26, 2024, https://www.investigativeplatform-mw.org/show-story/unveiling-macras-so.... (accessed 30 November 2025)
42. A Chauwa 'Malawi: Kabwila - Malawi Must Lead, Not Lag, in Global Ai Revolution', 27 June 2025 https://allafrica.com/stories/202506270502.html#:~:text=Revolution%20%2D%20allAfrica.com-,Malawi:%20Kabwila%20%2D%20Malawi%20Must%20Lead%2C%20Not%20Lag%2C%20in,ethics%20and%20governance%20of%20AI. (Accessed 29 January 2026)
43. Ministry of Information and Digitalisation, 2025 "Malawi Digital Readiness Assessment" https://www.undp.org/sites/g/files/zskgke326/files/2025-05/dra_malawi_report_2025_a4_print.pdf (accessed 28 December 2025)

Digital Inclusion

In 2025, Malawi continued expanding its digital public infrastructure (DPI), including digital identity systems, digitised registries, Data Centres and online public services. The National ID system, in particular, became increasingly central to governance, service access and civic participation.

A defining digital rights issue in 2025 was the decision to use the National ID card as the sole proof of identity for voter registration. This marked one of the most consequential uses of digital identity infrastructure in Malawi's democratic process to date.

The policy aimed to strengthen electoral integrity by eliminating duplicate registrations and ensuring a unified, verifiable voters' roll. In principle, this represented a positive step toward credible elections and alignment between civil registration and electoral systems.

However, the implementation revealed serious challenges. Persistent issues included limited availability of physical ID cards, particularly for first-time registrants, delays in replacement and renewal of lost, damaged, or expired cards and uneven service quality and access, especially in rural and hard-to-reach areas.[44] Although the government had extended the validity period of National ID cards to mitigate these constraints, operational bottlenecks remained. As a result, some eligible citizens faced barriers to voter registration not because of legal ineligibility but because of administrative and infrastructural shortcomings. These challenges triggered court cases and public disputes[45], with concerns raised about potential disenfranchisement and the proportionality of relying on a single digital credential in a context of uneven service delivery. Civil society actors and political party players argued that weaknesses in the ID system translated directly into unequal access to political rights.
From a digital rights perspective, DPI expansion offers clear benefits such as improved service targeting, reduced fraud and increased administrative efficiency. At the same time, it concentrates sensitive personal data within state systems, increasing the importance of strong privacy protections, cybersecurity, transparency and accountability.

In May 2025, the Government of Malawi, in partnership with the United Nations Development Programme (UNDP), unveiled Malawi's first-ever Digital Readiness Assessment (DRA). The DRA comprehensively evaluates Malawi's current status and prospects in digital transformation. It assesses progress across six key pillars: Digital Public Infrastructure (DPI), Connectivity, Government, Regulation, Economy, and People. The assessment provides evidence-based recommendations to guide national strategy, investments, and policy reforms.[46]

According to the report, Malawi achieved a Digital Readiness Score of 1.96 out of 4.0, positioning the country within the "Opportunistic" stage of digital readiness. Key recommendations from the assessment include strengthening regulatory enforcement and developing future-facing policies, including a National AI and Data Strategy, improving public sector coordination, interoperability and user experience in e-services; promoting digital trust and citizenship through inclusive and accessible platforms; and investing in rural broadband infrastructure and reducing the cost of internet access. The report also emphasises the need to develop a National Digital Skills Framework focused on inclusion and workforce alignment, and establishing the Department of e-Government as an Independent Authority with a stronger implementation mandate.

The report offers an opportunity for Malawi to renew its digital transformation agenda by acting on the insights of the assessment.

Further, in August 2025, MACRA commenced public consultations to review the Communications Act of 2016 to align the regulatory framework with technological advancements, market developments and stakeholder needs. Led by a Digital Laws Taskforce,[47] input was sought through submissions on various issues, including the Universal Service Fund (USF) to improve digital inclusion and ac-

44. Vinicent Kumwenda, Key Informant Interview (31 December 2025)
45. Nation Publications Limited, 11 October 2924, https://web.facebook.com/NationOnlineMw/posts/newsa-move-by-democratic-progressive-party-dpp-to-commence-a-case-against-malawi/925019012991222/?_rdc=1&_rdr# (Accessed 29 January 2026)
46. UNDP Malawi, Malawi Launches First-Ever Digital Readiness Assessment to Guide Inclusive Digital Transformation. 15 May 2025. https://www.undp.org/malawi/press-releases/malawi-launches-first-ever-digital-readiness-assessment-guide-inclusive-digital-transformation (Accessed 30 December 2025)
47. MACRA, 19 August 2025 https://web.facebook.com/MACRA1998/posts/macra-is-reviewing-the-communications-act-cap-6801-to-ensure-it-responds-to-new-/1103242165234383/?_rdc=1&_rdr# (accessed 31 December 2025)

cessibility. Malawi also faces a significant gender digital divide. The latest (2023) Global Gender Gap Index ranks Malawi in position 110 out of 146 countries, an improvement from 132 in 2022.

There are gaps in access to ICT services by persons with disabilities. In 2024, the Government, through the Universal Service Fund (USF), rolled out two interventions, the "Disability Project for Digital Inclusion" and "Sign Language," aimed at advancing digital inclusion in institutions with people with disabilities.[48] The Disability Project for Digital Inclusion is promoting ICT access and use by people with disabilities (PWDs) living in different areas of the country.[49]

The Universal Service Fund (USF)

While USF models vary across countries, their common objective is to deploy communication infrastructure and promote the adoption of ICT services in rural and underserved areas, even when not economically viable. This reflects a commitment to connecting everyone, regardless of the associated costs. Principle 37(2) of the African Commission on Human and Peoples Rights Declaration on Freedom of Expression and Access to Information (African Commission Declaration) emphasises the necessity of universal, equitable, affordable, and meaningful internet access for the realisation of various human rights. It is by no coincidence that the 32nd Session of the Human Rights Council (2016) affirmed that rights enjoyed offline should also be protected online, necessitating the availability, affordability, and accessibility of telecommunication services.[50]

In Malawi, the USF is established under Section 157 of the Communications Act of 2016, with the aim of promoting universal access and services in underserved areas.[51]

The USF budget for the 2025 fiscal year was valued at US$7.5 million (MWK13.1 billion), a 27% increase from US$5.9 million registered in the 2024 Budget.[52] In 2025, the USF continued to roll out various projects estimated at a total of US$6.8 million.[53] For example, the Connect a School (CAS) initiative targets rural and peri-urban schools by constructing ICT Labs and providing internet and ICT Equipment to facilitate access to modern ICTs and the Internet for learners and communities. In 2025, the USF Committee indicated its plans for 2026-2027 to expand the CAS ICT labs to 229 from the initial 75, covering all parliamentary constituencies across the country.[54] The CAS model, which is built on partnering with community actors, has also

Other USF-funded initiatives include Community Networks (Yathu Yathu Data),[56] expected to diversify the mobile operator market and provide a lower-cost alternative to Airtel and TNM for mobile data, particularly in rural areas. [57] In addition, the Radio Access Network (Rural Telephony),[58] Connect Teachers Training College[59]; Grants for Local Digital Content Production; Sign Language Project; E-Health Project; and E-commerce project were some of the projects in the year. USF projects also included Connect a Post Office;[60] National Addressing System Project[61]; Persons with Disability Project for Digital Inclusion; Last Mile; Virtual Postal App; Curriculum Review; SMEs Digital Skills Training; and Digital Ambassadors[62].

While USF has begun to register notable strides through projects, after inordinate inactivity, it still faces significant operational and institutional challenges, undermining its full potential. According to

48. USF Key Informant Interview (28 December 2025)
49. USF Key Informant Interview (28 December 2025)
50. UN Human Rights Council 'Report of the Human Rights Council on its thirty second session' https://documents-ddsny.un.org/doc/UNDOC/GEN/G20/008/73/PDF/G2000873.pdf?OpenElement (accessed on 25 December 2024).
51. Section 157 of the Communications Act
52. USF Key Informant Interview
53. USF Key Informant Interview
54. USF Key Informant Interview (20 December 2025)
55. USF Key Informant Interview (20 December 2025)
56. USF is piloting the Community Broadband Network Project in 8 district councils including the identification of cooperatives that will run broadband network deployments in rural areas. USF has also trained the Cooperatives and facilitated their licensing.
57. "MACRA to roll out Yathu Yathu data network," Nthanda Times, https://nthandatimes.com/macra-to-roll-out-yathu-yathu-data-network/. (accessed 24 December 2024)
58. USF is procuring 26 mobile network towers to connect 22 mobile network infrastructures unserved/underserved areas to ensure adequate broadband coverage.
59. USF Key Informant Interview (20 December 2025)
60. USF Key Informant Interview (20 December 2025)
61. USF-funded digitization of land parcels in all districts
62. USF Key Informant Interview (20 December 2025)

the USF Management, USF-funded projects were significantly affected by a precarious macro-economic environment, including high levels of inflation, pushing up the costs of the projects. The researcher also noted unrealistic ambitions in USF projects. For example, there were over 16 projects running concurrently, but with limited budgets and lean USF management staff, risking underperformance of the projects. Inordinate delays and long procedures in public procurement also affected the timely completion of some projects.[63] The limited funding for USF is another area of concern. Section 160 outlines diverse funding sources for the USF, including operators' levies, parliamentary appropriations, grants, subsidies, auctions, public access projects and funds from MACRA[64]. This assessment, however, established Parliament's failure to appropriate funds to the USF despite Section 160(b) of the Communications Act, 2016 placing an obligation on Parliament to appropriate funds to the USF. This has increased the financial burden on USF.

There are also transparency and accountability concerns arising from MACRA's failure to comply with Section 194(c) of the Communications Act, 2016, regarding the publication of fund details and reporting to Parliament on USF. Since the establishment and operationalisation of USF, MACRA has not published USF reports. There is a need for proactive disclosure of information on the USF in line with Principle 29 of the African Commission on Human and Peoples' Rights' Declaration on Freedom of Expression and Access to Information in Africa.[65]

63. Ibid
64. USF Strategic Plan
65. African Commission on Human and People's Rights (ACHPR) Declaration on Freedom of Expression and Access to Information (the Declaration) https://www.achpr.org/legalinstruments/detail?id=69 (accessed on December 20, 2024).

Conclusion

In 2025, Malawi's overall performance on the TheScore Index improved from 35 to 36 out of 60 and is rated "moderately compliant". Increased reports of surveillance, a prohibitive tax regime on ICT products and services introduced through the 2025 national budget, and criminalisation of online expression, remained major areas of concern among others.

Major gains in the year included the Constitutional Court's repeal of Section 200 of the Penal Code outlawing criminal defamation,a significant step in upholding the constitutional guarantee for freedom of expression and media freedoms. Malawi also commenced a participatory review of the Communications Act, 2026, to align the regulatory framework with rapid technological advancements, market developments, and stakeholder needs. Initiatives rolled out under the Universal Service Fund (USF) were a step in the right direction in transforming digital inclusion in the country.

Pursuant to the existing gaps, opportunities and recent developments in the digital space in Malawi, the following recommendations are made:

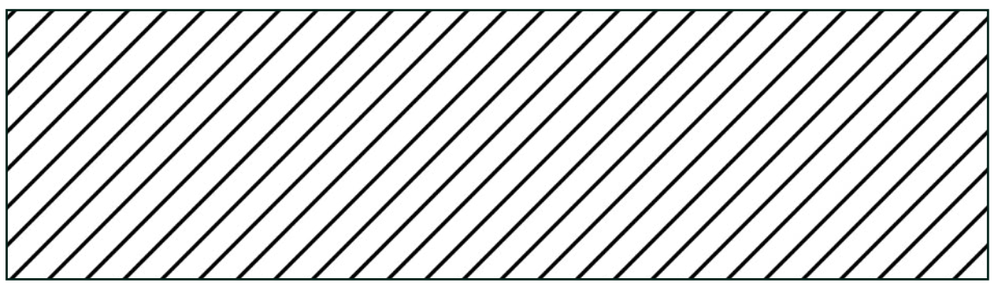
Recommendations

The Government should:

- Review the prohibitive taxation regime on ICT products and services.
- Review the Electronic Transac-

tions and Cybersecurity Act of 2016 to remove broad and vague provisions and offences, including sections 24(1) (e) and (f) and repealing any sedition laws in the Penal Code, to align with the Constitutional Court's ruling outlawing criminal defamation.

- Repeal Section 60 of the Penal Code that criminalises false or fake news to guarantee freedom of expression and media freedoms.
- Address strong suspicions of government surveillance equipment procured by MACRA to monitor social media platforms and ICT activities using the UFED system, designed to access and extract information from electronic devices such as phones and laptops sold by the Israel-based company, Cellebrite
- Guarantee Freedom of Expression and Media Freedoms by, among others, desisting from arbitrary arrests and censorship
- Intensify implementation of the Malawi Digital Economy Strategy to ensure accelerated universal access to the Internet and mobile services.
- Raise public and stakeholder awareness on the Data Protection Act
- Strengthen operational capacity and accountability mechanisms for the National ID system, particularly for replacement and renewal services.
- The Malawi Parliament should allocate funds to the Universal Service Fund (USF) in compliance with section 160(b) of the Communications Act.
- Develop regulatory and ethical use standards of Artificial Intelligence with proper governance structures.



Civil Society Organisations should:

- Advocate for the review of the government's tax regime on ICT products and services
- Advocate for the review of the Electronic Transactions and Cybersecurity Act of 2016; and repealing false news and sedition laws in the Penal Code through engagement with authorities, public awareness, and litigation
- Train law enforcement agencies, the judiciary, and regulatory institutions in digital rights
- Demand accountability on the procurement and deployment of MACRA's social media surveillance machine and UFED system for surveillance.
- Strengthen digital rights coalitions and networks to bolster civil society agencies in digital rights advocacy.
- Advocate for Malawi's ratification of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)

The Media should:

- Monitor, investigate, and expose digital rights violations
- Track government accountability on the implementation of the Malawi Digital Economy Strategy to ensure accelerated universal access to the Internet and mobile services.
- Raising public and stakeholder awareness on various digital rights-related laws, including the Data Protection Act
- Monitor the operations of the USF to ensure proactive disclosure of USF information every year, transparency, accountability, and effectiveness, while also advocating for the appropriation of funding by Parliament

Mobile Network Operators should:

- Collaborate with non-state actors in advocating for a conducive policy and legislative environment for digital rights and ICT actors.
- Proactively partner with the government in bridging the digital divide, including joint investment in ICT infrastructure targeting rural communities and provision of affordable data tariffs and mobile services.

Academia should:

- Provide intellectual leadership and guidance on issues of digital rights and inclusion.
- Conduct research on issues of digital rights and inclusion and emerging technologies such as Artificial Intelligence.

66. An improved Index score from 3 in 2024to 4 attributed to repeal of criminal defamation
67. https://malawi.misa.org/2022/11/22/members-of-parliament-in-malawi-remove-sedition-as-criminal-offence/%23:~:text%3DOn%2520November%252021%252C%25202022%252C%2520Members%2520of%252-0Parliament,Constitution%2520*%2520Open%2520up%2520the%2520civic%2520space&sa=D&source=docs&ust=1774356819281102&usg=AOvVaw3g8zpHfORNE9U-QGEEvw-T
68. https://macra.mw/download/25/rulesregulations/252806/data-protection-act-2024.pdf&sa=D&source=docs&ust=1773680549141611&usg=AOvVaw1LomaO0ATgPllyDoeiLgBM
69. The Index Score dropped from 3 to 2 due to increased prohibitive tax regimes, increasing prices of internet services and ICT products

The Score Index

Malawi, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	5	5	No incident of internet shutdown
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	4	4	Policies and laws are there but limited compliance. For example, Malawi has Communications Act, Digital Economy Strategy, Universal Service Fund, ICT Policy – but implementation is insufficient
False News Criminalisation	P22(2)	1	1	Arrests of social- media users; Section 60 of Penal Code, 87, 91, Electronic Transactions and Cyber Security Act, and Penal Code. Repeal of defamation law in 2022 (Secs 50, 51,52 and 53 of the Penal Code of Malawi)
Sedition Legislation	P22(2)	3	4[66]	No sedition law[67] in Malawi although repressive provisions exist in Section 87 of the Electronic Transactions and Cyber

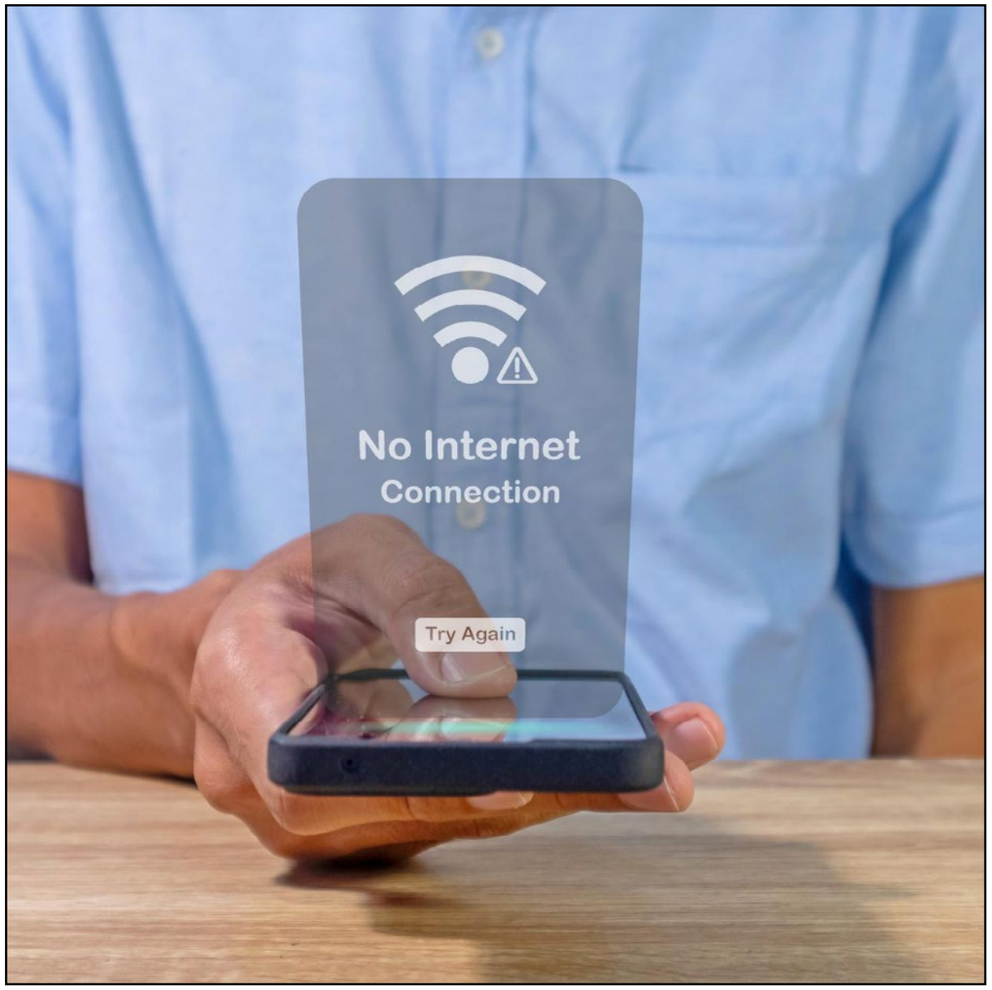
Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
				Security Act, containing aspects of criminalisation of "offensive communication".
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	2	2	Arrests of social media users
Data Protection Legislation.	P42	3	3	• Data Protection Act is in place; • Office of Data Protection Officer established to handle complaints; • Regulations for Data Protection Act promulgated in 2025; • MACRA is designated as Data Protection Authority, not a best practice • Advisory Committees[68] established under sec.7 of the Data Protection Act, to provide advice to the Authority, not yet in place
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	4	5	No incident recorded
Invasion of Privacy of Communications	P41	2	1	
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	4	3	Most government agencies have an online presence, including websites and social media platforms. However, proactive disclosure of information is limited
AI and Emerging Technologies national strategies	P39(6)	1	2	• Underwent UNESCO RAM in 2025; • No AI Policy and regulatory framework
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P29(3)	3	3	Adoption of the National Child Online Protection Strategy in 2024
Digital Inclusion	P29(3)	3	3	• Increased VAT on ICT products and services from 16.5% to 17.5% in 2025; • Introduction of 0.5% levy on e-money transfer; • Increased cost of internet data by mobile companies • Active USF projects
Total (out of 60):		2024: **35**	**2025** **36**	

Mozambique

Dércio Tsandzana, PhD

Executive Summary

This report examines the evolving state of freedoms and access to information in Mozambique. It is based on a qualitative methodology, primarily involving a desk review and similar reports related to the topic under research. An index is used in this research to evaluate Mozambique's digital rights situation. It is a qualitative assessment intended to highlight the various difficulties the nation faces, both offline and online. This report highlights the precarious state of digital rights, with an index score of 24 points that reflects both the severe gaps in the protection of basic freedoms online and the progress in expanding connectivity. The score emphasises areas such as freedom of expression, media independence, transparency, and legal protections against arbitrary digital restrictions, even though initiatives such as public access points, digital inclusion in schools, and rural connectivity projects have improved access to information and communications. The index also highlights the asymmetric nature of Mozambique's digital ecosystem, where technological and infrastructural advancements are not yet matched by institutional capacity, regulatory clarity, or civic oversight. In this context, the score serves as a benchmark for targeted interventions, signalling the urgent need for coordinated action by government, civil society, academia, and the private sector to strengthen digital rights, ensure accountability, and build a resilient, inclusive, and rights-respecting digital environment.



Introduction

Mozambique had a relatively stable political and digital landscape in 2025 following a turbulent era punctuated by internet outages, albeit this peace was nonetheless brittle and uneven. Gradually, connectivity was restored in February 2025, and online public discourse slowly reappeared, with digital platforms once more becoming forums for political commentary, information exchange, and civic engagement. Nonetheless, the recollection of recent disruptions continued to influence user behaviour, with journalists, activists, and other citizens engaging in online activities while increasing self-censorship and risk-avoidance.

State-run media outlets dominate the Mozambican media industry, often producing favourable coverage of the government. However, some smaller independent publications provide valuable coverage. Journalists routinely face government pressure, harassment, and intimidation, which often leads to self-censorship. The government has been known to retaliate against critical journalists, including cancelling public advertising contracts.[1] In recent years, journalists and political pundits who appear on television programs have been attacked and kidnapped. Police regularly harass, assault, and detain journalists.[2]

According to Reporters Without Borders, the election of Daniel Chapo in October 2024, followed by violent clashes that resulted in over 300 deaths, has further exacerbated the alarming decline of press freedom in Mozambique. Media ownership and advertising are two other ways that the State exercises control over the press. Large state-owned businesses that inherited the hyper-centralised economy of the communist era place the majority of the advertisements. This makes it easier for both State and privately held media outlets to heavily influence editorial choices, giving them little freedom to criticise the president.

1. Reporters Without Borders – Mozambique https://rsf.org/en/country/mozambique, accessed on 22 November 2025.
2. Freedom House – Freedom in Mozambique https://freedomhouse.org/country/mozambique/freedom-world/2025, accessed on 22 November 2025.

Internet Access

In early 2025, a total of 17.7 million cellular mobile connections were active in Mozambique, equivalent to 50.4% of the total population. However, note that some of these connections may include only services such as voice and SMS, and some may not include internet access. There were 6.96 million internet users in Mozambique at the start of 2025, with online penetration at 19.8%. Mozambique had 3.70 million social media user identities in January 2025, equating to 10.5% of the total population.

According to the same source[3], data shows that Mozambique's population increased by 1.0 million (+2.9 per cent) between early 2024 and the start of 2025. Meanwhile, in early 2025, 39.6% of Mozambique's population lived in urban centres, whereas 60.4% lived in rural areas. At that time, 51.5% of Mozambique's population was female, while 48.5% of the population was male. Data from GSMA Intelligence shows that there were 17.7 million cellular mobile connections in Mozambique at the beginning of 2025. For perspective, many people use more than one mobile connection, so it's not unusual for mobile connection figures to significantly exceed those for the total population. However, this practice hasn't yet pushed mobile connectivity rates in Mozambique beyond 100%, and GSMA Intelligence's figures indicate that mobile connections in Mozambique accounted for 50.4% of the total population in January 2025.

On December 16 2025, the Mozambican Council of Ministers enacted Decree No. 48/2025, which establishes new, strict regulations for telecommunications traffic control and authorizes the suspension or blocking of internet services during "imminent risks" to public security[4]. This decree aims to combat cyberattacks and fraudulent traffic but has raised concerns about state-sanctioned digital censorship. In January 2025, CDD warned that legalising

3. DataReportal, Digital in Mozambique https://datareportal.com/reports/digital-2025-angola, accessed on 4 January 2026.
4. Club of Mozambique, Mozambique introduces new regulation to tighten telecom traffic control and security https://clubofmozambique.com/news/mozambique-introduces-new-regulation-to-tighten-telecom-traffic-control-and-security/, accessed on 4 January 2026.

the blocking of communications constitutes a social control strategy incompatible with the Democratic Rule of Law.[5] In the petition submitted to the Ombudsman, CDD argues that these provisions constitute serious and unconstitutional restrictions.

Freedom of expression

The Constitution of the Republic[6] and access to information legislation guarantees freedom of expression, especially for the media. The Press Act 1991 governs the mass media, which covers print, broadcasting, and cinema. According to this law, before starting activities, the mass media must register with the Information Office, or GABINFO. Registration is not optional, as it can only be denied when an applicant fails to comply with the legal requirements and conditions established by law. With regard to print media, the Press Act further requires periodicals to disclose, in each printed edition, essential information such as the publication's circulation and the identities of its owners, editors, directors, and printer.

Article 48 of the Constitution of the Republic guarantees freedom of expression only to citizens, not to all persons, which is unique amongst SADC states.[7] A more positive attribute of the provision is that it discusses explicitly freedom of the press, with an unusual degree of detail about what freedom of the press entails, including "freedom of journalistic expression and creativity, access to sources of information, protection of independence and professional secrecy, and the right to establish newspapers, publications and other means of dissemination".

According to Article 43, the Constitutional principles in respect of fundamental rights – which include the right to freedom of expression – "shall be interpreted and integrated in harmony with the Universal Declaration of Human Rights and with the African Charter of Human and Peoples Rights".[8] However, despite all these innovations, International Press Institute (IPI) recently concluded that independent journalism in Mozambique was facing considerable legal, political, and economic pressures as the country's hard-fought democratic gains of the past three decades come under increasing strain.[9]

In June 2025, MISA Mozambique reported that the Judicial Court of Niassa Province convicted a Nigerian citizen following an assault on TV Sucesso journalists Herculano Ernesto and Mixaque Lucas.[10] The incident occurred in January 2025 during journalists' coverage of a fire at the Central Market in Lichinga. At the time of the incident, the journalists were filming a commercial establishment that was on fire when the owner of the affected premises, Edwin Onyemmeka Nwachuka, a Nigerian national, prevented them from carrying out their professional duties. The assailant demanded that the journalists stop their work and, after they refused, physically attacked reporter Mixaque Lucas, causing injuries and damaging the reporting equipment used during the coverage.

The accused was convicted and sentenced to six months' imprisonment, commuted to a fine, for the crime of simple voluntary bodily harm. He was also ordered to pay compensation to the victims. MISA Mozambique, which provided legal assistance to the case from its initial stages, welcomed the court's decision, considering it an important milestone in the fight against impunity in cases of violence against journalists. The organisation views the ruling as a positive step towards safeguarding press freedom and freedom of expression, as well as a sign of the strengthening of the rule of law in Mozambique. However, MISA Mozambique notes[11] that the penalties imposed remain lenient given the nature of the crime and argues that firmer

5. CDD https://cddmoz.org/wp-content/uploads/2026/01/Legalizing-the-blocking-of-telecommunications-networks-is-a-democratic-setback-and-an-affront-to-human-rights-.pdf, accessed on 4 January 2026.
6. Constitution of the Republic of Mozambique (English) https://cdn.accf-francophonie.org/2019/03/mozambique_const-en.pdf, accessed on 17 December 2025
7. Internews 'Chapter 12 – Mozambique' https://internews.org/wp-content/uploads/2023/11/ARISA-IEA-CHAPTER-12-Mozambique.pdf, accessed on 17 December 2025
8. Mozambique's 2004 Constitution (revised 2007), Article 43.
9. IPI – Press Freedom in Mozambique https://ipi.media/wp-content/uploads/2022/12/IPI-PRESS-FREEDOM-MISSION-MOZAMBIQUE-1.pdf, accessed on 15 November 2025.
10. MZ News, Repórteres da TV Sucesso agredidos por cidadão Nigeriano em Niassa https://mznews.co.mz/en/reporteres-da-tv-sucesso-agredidos-por-cidadao-nigeriano-em-niassa/, accessed on 5 February 2026.
11. MZ News, Repórteres da TV Sucesso agredidos por cidadão Nigeriano em Niassa https://mznews.co.mz/en/reporteres-da-tv-sucesso-agredidos-por-cidadao-nigeriano-em-niassa/, accessed on 5 February 2026

judicial decisions are necessary to deter future attacks against journalists in the exercise of their professional duties.

Data Protection and Privacy

In Mozambique, there is no specific legislation on data protection or privacy.[12] However, other sources of law impose some privacy obligations, including:

- The Civil Code (Decree-Law no. 47344, of November 25 1966, in force in Mozambique through Edict no. 22869, dated September 4, 1967)
- The Penal Code (Law no. 24/2019, of December 24, as amended by Law no. 17/2020 of 23 December)
- The Labour Law (Law no. 23/2007, of August 1) and the new Labour Law (Law no. 13/2023, of August 25)
- The Electronic Transactions Law (Law no. 3/2017, of January 9)
- The Regulations on Registration and Licensing of Intermediary Electronic Service Providers and Operators of Digital Platforms (Decree no. 59/2023, of 27 October), and Resolution no. 5/2019, of June 20, ratified the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention).

In addition, the Constitution of the Republic of Mozambique provides that all citizens are entitled to the protection of their private life and have the right to honour, a good name, reputation, protection of their public image and privacy.[13] Further, Article 71 of the Constitution identifies the need to legislate on the access, generation, security, and use of computerised personal data (by public or private entities); however, implementing legislation has not yet been approved.

12. DLA Piper – Data protection laws of the world Mozambique https://www.dlapiperdataprotection.com/index.html?t=law&c=MZ, accessed on 10 December 2025
13. ALT Advisory – Factsheet Mozambique https://dataprotection.africa/wp-content/uploads/2019/10/Mozambique-Factsheet.pdf, accessed on 11 December 2025

The Electronic Transactions Law[14] defines personal data as any information in relation to a natural person which can be directly or indirectly identified by reference to an identification number or one or more factors. The Malabo Convention identifies these factors: physical, physiological, mental, economic, cultural, or social identity. Decree 59/2023 requires the registration of Intermediate Electronic Services Providers and Operators of Digital Platforms. The Electronic Transactions Law defines the intermediate service provider as any person who, in representation of another, sends, receives, and stores data messages, and who provides network access services or provides services through a network.[15]

Any entity that performs such acts will qualify as an intermediate service provider and must be registered and licensed with National Institute of Information and Communications Technology (INTIC). The registration requirement applies to Intermediate Electronic Services Providers and Operators of Digital Platforms that offer services to receivers based in or located in Mozambique, regardless of where the providers are based. The Electronic Transactions Law requires the data processor to appoint a person responsible for compliance with the provisions on electronic personal data protection. The law does not generally restrict cross-border transfers of personal information. The Constitution of the Republic of Mozambique imposes restrictions on the disclosure of personal information to third parties, requiring prior consent from the data subject.

Although the AU Convention prohibits the transfer of personal data to a non-member state, this prohibition does not apply if the state ensures an adequate level of protection for the privacy freedoms and fundamental rights of the data subject. The AU Convention also requires that consent be sought from the national protection authority before the data controller may transfer the data

14. Electronic Transactions Law https://www.cga.co.mz/en/moz/publication/electronic-transactions-in-the-mozambican-legal-system, accessed on 11 December 2025
15. CIPESA – Digital Rights in Mozambique https://cipesa.org/wp-content/files/Submission-to-the-38the-session-of-the-Universal-Periodic-Review-Mozambique.pdf, accessed on 9 December 2025

to a third country. Currently, INTIC does not have such powers, so the principle of consent of the data subject and the transfer of data to a country with an adequate data protection framework would apply. Notwithstanding, parties may approach INTIC for further guidance on this matter.

Censorship and content moderation

There were no publicly reported requests for content takedowns during the period under review, nor is there evidence of transparency reports systematically documenting or disclosing such practices in Mozambique, according to publicly available Meta sources. However, records indicate that content removal requests were made in 2022 and again in 2025.[16] Following the internet shutdowns of 2024, 2025 did not register any officially acknowledged large-scale content blocking or nationwide restrictions. However, the absence of reported takedown requests or transparency mechanisms does not necessarily indicate censorship, but rather points to a continued lack of institutional openness and clear reporting frameworks for content moderation and State–platform interactions.

Access to information

Mozambique introduced the Right to Information Law (LEDI) in 2014 (Act No. 34/2014)[17] – a sign of government commitment to the opening of organisations holding information of public interest. It goes without saying that making information available is an important indicator of the consolidation of democracy and good governance. The commitment of public authorities to implementing LEDI therefore requires strengthening democratic principles.

16. Meta - Government Requests https://transparency.meta.com/reports/government-data-requests/country/MZ/, accessed on 15 January 2026.
17. Article 19 – Mozambique: Draft Right to Information Law https://www.article19.org/resources/mozambique-draft-right-information-law/, accessed on 5 December 2025

The law is intended to make it easier for citizens to access information held by public bodies. However, the law has some limitations, including exemptions for state secrets and the private affairs of citizens. The right to freedom of information is part of the right to freedom of expression in the Mozambican Constitution. The right to information includes the right to access public-interest information from a variety of sources, the right to information grants whistleblowers the right to disclose information critical to the public interest. The Constitution restricts the recording and handling of information that is individually identifiable, such as political, philosophical, or religious beliefs.

Public entities have been repeatedly accused by civil society organisations of denying or restricting access to information. For instance, CDD Mozambique, a civil society organization based in Maputo, has consistently reported[18] cases in which State institutions fail to respond to information requests, delay disclosure beyond legally established deadlines, or provide incomplete information, despite the existence of a legal framework guaranteeing the public's right to access information.

AI and Emerging Technologies

Mozambique is currently drafting its National Artificial Intelligence Strategy as part of a broader effort to establish a comprehensive digital governance framework for the country. The process has involved coordination between the National Institute of Information and Communication Technologies (INTIC) and UNESCO, with technical workshops and stakeholder consultations held to ensure the strategy aligns with international best practices and is adapted to national priorities. These efforts build on the successful completion of Mozambique's UNESCO Readiness Assessment Methodology (RAM) on AI in 2024, which provided key insights into the country's preparedness for AI

18. SAVANA, CDD preocupado com o silêncio do MP no concurso polémico entre IAOM e FTM https://savana.co.mz/?p=9044, accessed on 5 February 2026.

adoption and governance.

In multiple public statements, Américo Muchanga, Minister of Communications and Digital Transformation, has reiterated[19] the government's commitment to digital innovation and the responsible deployment of AI technologies. He has emphasised that the strategy aims not only to harness the potential of AI for economic growth and public service delivery, but also to ensure that ethical, legal, and human rights considerations are integrated into national policy frameworks. In his view, the digital transformation of Mozambique is irreversible, and principles of inclusion, transparency, and security must guide the adoption of advanced technologies such as AI.

Minister Muchanga has also highlighted complementary initiatives underway, including the drafting of a Data Protection Law and a Cybersecurity Law, as well as broader digital infrastructure investments, which together will provide a supportive environment for AI adoption and governance. These strategic policy instruments are being developed in consultation with international partners, including the European Union and UN agencies, to ensure that Mozambique's AI ecosystem grows in a regulated, ethical, and socially beneficial manner. When speaking at the UN General Assembly in September 2025, President Daniel Chapo emphasised[20] that justice, peace, and legality are crucial for development and also called for the responsible use of artificial intelligence, linking it to the need for critical, creative, and ethical citizens.

Digital Inclusion

In April 2025, the pilot project for rural connectivity was officially launched, marking a joint initiative between the Government of Mozambique, through the National Communications Regulatory Authority (INCM), and the private sector, involving BDQ Mobile, Movitel, VANU, and Spacecom. The initiative forms part

19. INTIC, Ministro Américo Muchanga Defende Inclusão Digital e Inteligência Artificial como Motores do Desenvolvimento Nacional https://intic.gov.mz/ministro-americo-muchanga-defende-inclusao-digital-e-inteligencia-artificial-como-motores-do-desenvolvimento-nacional/, accessed on 5 February 2026
20. Integrity, Presidente Chapo apela à unidade global https://integritymagazine.co.mz/arquivos/49372, accessed on 5 February 2026

of the Internet for All by 2030 Project and was formally launched on April 28 2025 in Xinavane, Maputo Province.[21] The project aims to facilitate the expansion of mobile telecommunications network infrastructure at relatively low cost, to promote digital inclusion and ensure access to communications for communities in rural areas where market conditions are traditionally unfavourable to private investment. By addressing structural and economic barriers to connectivity, the initiative seeks to extend basic communication services to underserved and remote populations.
The new antenna model, based on a satellite-enabled solution, can benefit approximately 15,000 people and cover a radius of up to 50 kilometres. Speaking at the launch ceremony, the Minister of Communications and Digital Transformation, Américo Muchanga, commended the private sector's active involvement and commitment in establishing partnerships that enabled the development and deployment of telecommunications base stations and innovative technologies. He emphasised that these solutions significantly reduce investment costs associated with network expansion while simultaneously strengthening digital inclusion and guaranteeing the right to communicate for rural communities across the country.
In December 2025, data presented during the 19th Review and Planning Meeting (2025–2026) of the National Communications Regulatory Authority (INCM), held in Inhambane Province from 3 to 5 December 2025 under the theme "Promoting Communications for an Inclusive and Sustainable Digital Ecosystem", highlight significant progress achieved throughout 2025 in key strategic areas for the development of Mozambique's communications sector. In the areas of network expansion and digital inclusion, INCM implemented several high-impact initiatives to reduce connectivity gaps and strengthen access to digital services. Notably, the Internet in Schools Project was expanded, resulting in the connection of more than 200 additional schools to the internet. [22] At the same time, 12 Digital Squares were reconnected using upgraded technologies to improve service quality and user experience.

21. MCTD, Xinavane Torna-se Pioneira no Projecto de Internet Rural em Moçambique https://digital.gov.mz/?p=1249, accessed on 5 February 2026.
22. INCM, INCM reúne-se para balanço e planificação https://www.incm.gov.mz/index.php/sala-de-imprensa/noticias/698-incm-balanco-e-planificacao-2025, accessed on 5 February 2026.

Further progress was recorded through the award of a public tender for the installation of 60 telecommunications antennas in previously unserved localities, representing a critical step towards extending communications infrastructure to remote and underserved areas. In parallel, INCM launched a public tender for a new Digital Squares model, including its operational management framework, to ensure sustainability and greater local impact. The year was also marked by the inauguration of the ThinkLab Technology Incubator, designed to stimulate innovation and support the digital entrepreneurship ecosystem, as well as the inauguration and handover of a cybersecurity laboratory in Nampula Province, strengthening national capacity in cybersecurity skills development and digital resilience. Overall, these developments demonstrate tangible advances towards building a more inclusive, resilient, and sustainable digital ecosystem in Mozambique.[23]

In a pioneering data-driven investigation[24], the Mozambican Disabled Persons' Organisation Forum (FAMOD) has teamed up with UK-based non-profit Data4Change to run automated accessibility testing on 90 of the most important and functional websites in Mozambique. The result is a publicly available dataset of 722,053 instances of accessibility 'violations'. Each violation represents a barrier preventing someone with a visual, hearing, physical or cognitive impairment from fully engaging with the web page. The investigation revealed that just five types of accessibility violations accounted for nearly 90% of all violations. These top five violations were low colour contrast (37%), lack of landmarks to identify regions of a page (33%), links that aren't made apparent (11%), no descriptive text for interactive elements (3%) and no 'alt text' for images (2%). The violations were defined in accordance with international standards for web accessibility, as described in the Web Content Accessibility Guidelines 2.0 and 2.1.

There is no explicit law in Mozambique that protects children in the online environment. However, the Penal Code[25] has a number of provisions that can be used for offenses involving minors, such as sexual exploitation, abuse, and the creation or broadcast of illegal information. These provisions establish a basic legal framework for dealing with specific types of harm that may occur in digital areas, particularly those relating to child pornography and online grooming.

Nonetheless, the lack of a complete legal framework explicitly designed for online child safety leaves considerable regulatory gaps, particularly in the face of rising hazards such as cyberbullying, online harassment, and the abuse of children's personal data on digital platforms.that a child's personal information shall only be subject to processing with parental consent

Conclusion

Overall, the developments observed throughout 2025 reflect an asymmetric trajectory in Mozambique's digital transformation, characterised by notable investments in connectivity, infrastructure expansion, and digital service delivery, alongside persistent vulnerabilities in the protection of digital rights. Initiatives led by INCM and its public–private partnerships helped narrow access gaps, particularly in rural and underserved areas, reinforcing the right to access information and communications. However, these infrastructure gains unfolded in a context still shaped by the legacy of internet shutdowns, weak accountability for digital rights violations, and limited legal and institutional safeguards to protect freedom of expression, media freedom, and the right to privacy online.

The completion of the UNESCO Readiness Assessment Methodology and the creation of the National Artificial Intelligence Strategy are examples of

23. INCM, INCM passa a contar com incubadora Tecnológica https://www.incm.gov.mz/index.php/sala-de-imprensa/noticias/672-incubadora-thinklab, accessed on 5 February 2026.
24. CIPESA – Investigation Finds More than 700,000 Barriers Limiting Website Accessibility in Mozambique https://cipesa.org/2021/03/investigation-finds-more-than-700000-barriers-limiting-website-accessibility-in-mozambique/, accessed on 5 December 2025

25. Mozambique Penal Code, https://reformar.co.mz/documentos-diversos/lei-24-2019-lei-de-revisao-do-codigo-penal.pdf, accessed on 10 March 2026.

policy procedures that demonstrate an increasing understanding of the necessity of responsible and rights-based digital governance. However, these procedures are still primarily normative and aspirational at this point, and their true significance will depend on future legislative clarity, enforcement strategies, and impartial oversight. Therefore, 2025 should be viewed less as a year of digital rights consolidation and more as a contentious and transitional period in which the development of digital infrastructure continues to outpace the creation of robust user rights protections.

Recommendations

The Government should:

- Create and implement explicit legal protections against arbitrary internet shutdowns and digital restrictions, ensuring that any restrictions on connectivity comply with international human rights standards, constitutional guarantees, and the principles of necessity, proportionality, and legality.
- Adopt and implement data protection, cybersecurity, and AI governance frameworks more quickly. These frameworks should have robust oversight mechanisms, independent accountability organisations, and significant public input, especially engaging young people, journalists, and marginalised populations.
- Ensure that rights-based governance, openness in public-private partnerships, and channels for citizens to denounce and seek remedies for abuses of their digital rights accompany digital inclusion policies, such as those related to public access and rural connectivity.

Academia should:

- Conduct independent, fact-based research on internet governance, digital rights, surveillance, and the use of AI in Mozambique, producing locally grounded information to guide public discourse and policy decisions.
- Develop national capacity on ethical and rights-based digital transformation by strengthening interdisciplinary teaching and training programs that connect technology, law, media studies, and human rights.
- Participate more actively in policy discussions and advisory processes, translating scholarly research into clear policy briefs and supporting national initiatives, such as frameworks for digital governance and artificial intelligence.

The Media should:

- Increase the time spent tracking, documenting, and publicly reporting digital rights violations, such as internet shutdowns, online harassment, surveillance tactics, and attacks on journalists in digital spaces.
- Promote training sessions to increase resilience against online aggression, misinformation, and digital repression, expand digital rights literacy and safety programs, especially for women, youth, activists, and journalists.
- Encourage accountability, smart litigation, and ongoing engagement with legislators on digital rights legislation, forge stronger national and regional coalitions and advocacy platforms.

Private Sector should:

- Adhere to human rights-based strategies for technology deployment and connection, such as openness in collaboration with state authorities and opposition to illegal or unreasonable requests that violate users' rights.
- Incorporate ethical AI principles, data protection, and privacy-by-design into goods and services, especially for public and rural infrastructure projects.
- Participate actively in multi-stakeholder digital governance procedures, encouraging candid communication, impartial audits, and capacity-building programs that ensure an inclusive and reliable digital ecosystem.

The Score Index

Mozambique, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	1	1	The Internet was recently (2024) shut down in Mozambique.This was the first time the government officially acknowledged the act. In December 2025, the Mozambican government approved a revision of the Telecommunications Traffic Control Regulation to grant the national telecommunications regulator the authority to block or suspend telecommunications networks in situations deemed to pose an "imminent risk" to public security or social order.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	3	3	Mozambique has an access to information law that is primarily applied to offline access. The Constitution of the Republic also includes provisions, but with less emphasis on internet access.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
False News Criminalisation	P22(2)	2	2	In 2023, the Government passed an unclear law criminalising false information about terrorism. This law is generally applied to prevent the spread of fake news related to the conflict, but media outlets fear it could be used to restrict access to information about the conflict entirely.t
Sedition Legislation	P22(2)	2	2	The Penal Code includes provisions that criminalize individuals who use traditional or digital means to insult authorities, including the President of the Republic. There are no recorded cases in 2025, but during COVID-19, the penal code was used to arrest internet users.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	During the 2024 elections, there were several cases of citizens being detained for protesting or organising mobilisations virtually.
Data Protection Legislation	P42(1)	1	2	Mozambique does not have any data protection law. The first draft was ready in December 2025, but there is no clear timeline for its final approval.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	4	4	There are no reported cases related to such incidents.
Invasion of Privacy of Communications	P41	1	1	The government of Mozambique delegated the regulatory authority to supervise all communications. During the 2024 elections, some journalists were asked by politicians to provide their materials or delete images related to the elections.
Failure by the government to proactively disclose and disseminate information through digital technologies	P29(3)	2	2	The government of Mozambique passed an Access to Information law in 2014. However, the law is not clearly applied to the digital space, failing to address how information can be easily accessed through digital technologies.
AI and Emerging Technologies national strategies	P39(6)	1	1	Mozambique is still at a very early stage in terms of discussions or initiatives in this area.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P39(6)	1	1	The general law applies only to child pornography, but there are no specific provisions related to children's digital safety.
Digital Inclusion	P37(3)	2	2	Little has been done in this area, except for some civil society initiatives
Total (out of 60):		2024: **23**	2025 **24**	

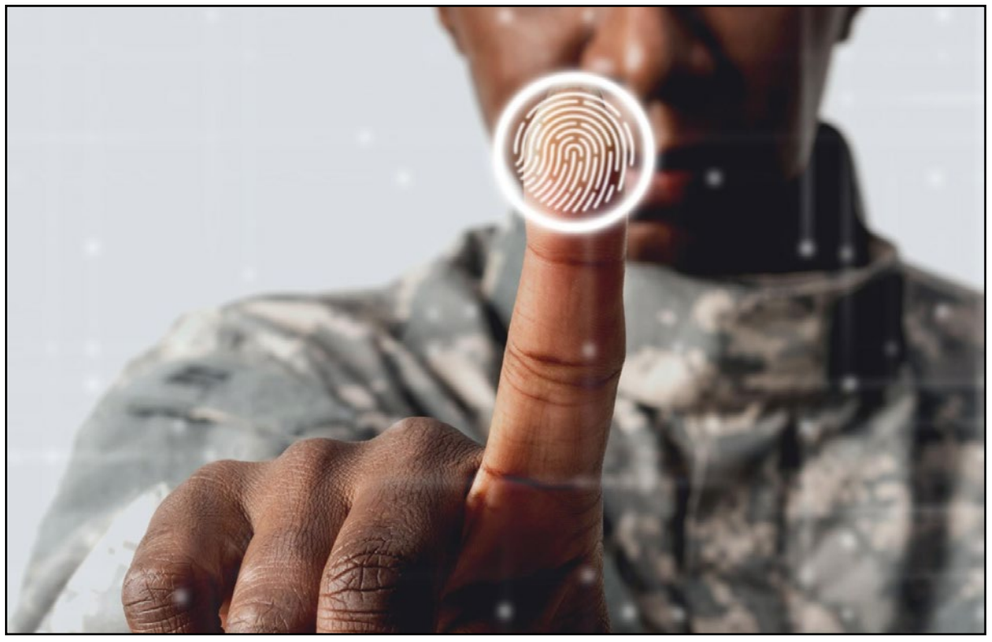
Namibia

By Emsie Erastus

Executive Summary

This report presents an overview of digital rights and digital inclusion in Namibia for 2025. It provides an overview by reviewing developments in the country as well as publicly available information and data. The report analyses academic research, news coverage, parliamentary engagement and political pronouncements on matters of interest. This study further assesses compliance with the African Charter on Human and Peoples' Rights and notes any decline or progress in 2025 when compared with findings in the Londa 2024 Report. The report demonstrates the level of State compliance with key international standards. It assesses the state of digital rights and inclusion, and scores Namibia based on 12 key indicators listed in The Score Index by Paradigm Initiative. The report examines internet access in the country and addresses accessibility as a matter of public interest. It further reviews cases of media freedom in the nation's digital landscape and considers how gendered disinformation and criminalisation of false news were addressed during the review period.

Furthermore, the report examines the state of data protection and privacy, and presents cases on cybercrimes and how they are dealt with in Namibia. The report looks at surveillance and smart city developments in Windhoek in particular and discusses how this is linked to privacy amongst citizens. Other thematic areas include censorship and content moderation by global platforms. The report also considers whether the transparency mechanisms engaged by platforms are extended to Namibia. The report reviews the work done since the passing of the 2022 Access to Information law, while also engaging with how artificial intelligence (AI) and emerging technologies are dealt with in the Namibian context, particularly in the absence of an AI-specific policy pronouncement. The report assesses the extent of digital inclusion, Digital Identification (ID) systems, costs of data, and the status of the Universal Service Fund (USF). Finally, the report makes recommendations towards improving all matters related to digital rights and inclusion in Namibia.



Introduction

Namibia is among the world's least densely populated countries[1], and in 2023, the Southern African nation's population reached a milestone of 3 million people. Its capital city, Windhoek, had 486,186 residents as per the 2023 Population and Housing Census, and this population continues to grow due to migration from other regions in Namibia.[2] The nation is ranked high in press freedom, however, internet access, digital infrastructure and cybersecurity remain a high concern.[3] The year 2025 saw landmark developments including the launch of the Universal Service Fund (USF) in March 2025 to bridge rural digital connectivity gaps,[4] establishment of the Namibia Cyber Security Incident Response Team (NAM-CSIRT) with N$20 million (US$ 1.25 million) funding in April 2025,[5] passage of the Civil Registration and Identification Act in December 2024 enabling biometric digital identity,[6] and launch of the country's AI Readiness Assessment Report in August 2025.[7] Paratus Group launched Namibia's first private mobile network with N$600 million (US$ 37.7 million) investment in September 2025, breaking the state monopoly in the mobile service provider sector.[8] In August 2025, MTC rolled out 5G services in Windhoek and other major cities, promising users much faster speeds and reduced latency.[9] In 2024, Namibians went to the polls to elect a new President and made history by electing a woman President, Vice President, and National Assembly Speaker, a key moment for gender inclusion and in the country's political landscape.[10]

Namibia further launched its National Digital Strategy (NDS), which sets forth a comprehensive blueprint for the country's holistic digital development for the period of 2025-2028.[11] The country's National Digital Strategy is aligned with the country's strategies for expanding public broadband, enhancing cybersecurity measures, and developing human capacity.

1. The Ten Least Densely Populated Countries in the World. Global Citizen Solutions. https://www.globalcitizensolutions.com/countries-with-lowest-population-density/ (Accessed 15 February 2026)
2. 2023 Population and Housing Census main report. Government of Namibia. https://nsa.org.na/document/2023-population-and-housing-census-main-report/ (Accessed 04 November 2025)
3. https://www.wesgro.co.za/uploads/files/Research/Wesgro-IQ_Namibia_2021.05.pdf
4. Communications regulator launches Universal Service Fund to boost ICT access https://economist.com.na/96240/technology/communications-regulator-launches-universal-service-fund-to-boost-ict-access/ (Accessed: 15 November 2025)
5. Namibia Launches NAM-CSIRT to Strengthen Cybersecurity Amid Rising Threats https://www.wearetech.africa/en/fils-uk/news/tech/namibia-launches-nam-csirt-to-strengthen-cybersecurity-amid-rising-threats (Accessed: 4 November 2025)
6. Civil Registration and Identification Act, 2024 https://namiblii.org/akn/na/act/2024/13/eng@2024-12-30 (Accessed: 15 November 2025)
7. Namibia Launches Artificial Intelligence Readiness Assessment Report https://www.unesco.org/en/articles/namibia-launches-artificial-intelligence-readiness-assessment-report (Accessed: 15 November 2025)
8. Namibia: Paratus Launches N$600m Nationwide Mobile Network Covering 50 Towns https://allafrica.com/stories/202509030174.html (Accessed: 4 November 2025)

Internet Access And Disruptions

International Telecommunication Union (ITU) data[12] indicates that 64.4% of individuals use the Internet. In aiming to mitigate digital inclusion challenges faced in the country's major urban area, the city of Windhoek has reportedly installed 10 km of fibre[13] in a country that has an 18,790-kilometre network. This adds to the broader expansion of terrestrial fibre networks seen to enable widespread access to cyberspace.

As reported in the Londa 2024 Report,[14] the rollout of Google's Equiano subsea cable[15] had the potential to connect

9. MTC announced 5G availability in the country. https://www.mtc.com.na/pressreleases/article/mtc-announced-5g-availability-in-the-country (Accessed: 15 November 2025)
10. The Forum on Internet Freedom in Africa 2025 (FIFAfrica25) Heads to Namibia! https://internetfreedom.africa/the-forum-on-internet-freedom-in-africa-2025-fifafrica25-heads-to-namibia/ (Accessed: 22 November 2025)
11. National Digital Strategy Namibia 2025 - 2028 https://mict.gov.na/documents/869282/6500577/NDS4+040825.pdf/aeb1c2a6-63a9-f04e-7f78-3e15549eefcf?t=1754320341496 (Accessed: 22 November 2025)
12. Figures from the previous Londa report compared to the 2024 index score https://paradigmhq.org/londa-24/ (Accessed: 27 January 2026)
13. Scramble for city's fibre market, Namibian Sun, July 2024, available at https://www.namibiansun.com/infrastructure/scramble-for-citys-fibre-market2024-07-05#:~:text=Research%20from%20We%20Are%20Social,for%20growth%20in%20internet%20services. (Accessed: 22 November 2025)
14. Londa Report, Namibia 2023 Paradigm Initiative, available at https://paradigmhq.org/wp-content/uploads/2024/06/Namibia-Country-Report.pdf (Accessed: 19 December 2024)
15. Google's Equiano subsea cable: Namibia economic impact assessment, Africa Practice, 2022, available at https://africapractice.com/equiano-namibia-eia/ (Accessed: 19 December 2024)

South Africa and Europe, adding to the impetus of heightened digital connectivity between Namibia, the rest of Southern Africa, and the rest of the world. The Google Equiano cable was activated in July 2024,[16] signifying a "quantum leap forward in Namibia's digital transformation journey, paving the way for an era of unprecedented connectivity and boundless opportunities," according to Telecom Namibia, the implementing partner. Expectations for a higher bandwidth capacity, better latency, and faster speeds at a much lower cost, are in place as a result of this activation and Namibia is expected to be on course for more rapid digitisation and an inclusive digital economy. The most transformative development for internet availability in 2025 was the official launch of the Universal Service Fund (USF) on March 19 2025 in Windhoek.[17] Dr Tulimevava Mufeti, Chairperson of the Communications Regulatory Authority of Namibia (CRAN) Board of Directors, emphasised that "connectivity is no longer a luxury; it is a necessity. It is fundamental for education, healthcare, entrepreneurship, and overall socio-economic development."[18] The government allocated N$145 million (US$ 7.25 million) over three years (2025-2028) specifically to enhance digital connectivity in rural areas and underserved communities. The Ministry of ICT's 2025-2029 Strategic Plan set an ambitious goal to achieve 100% network coverage by 2030,[19] requiring substantial infrastructure investment in geographically challenging and economically marginal areas. A landmark development reshaping Namibia's telecommunications landscape was Paratus Group's launch of the country's first privately-owned mobile network in September 2025.[20] Backed by a N$600 million (US$ 37,7 million) investment and built entirely on 4G LTE technology with 5G readiness, the network covered 50 major towns and 80 communities, focusing on the east-west and Windhoek-Oshakati routes.[21] This challenged the longstanding duopoly of state-owned Mobile Telecommunications Company (MTC) and Telecom Namibia, introducing new competitive dynamics potentially beneficial for coverage expansion and service quality. Infrastructure modernisation accelerated with Telecom Namibia announcing in June 2025 that all newly deployed mobile base stations were fully 5G-enabled,[22] implementing the International Mobile Telecommunications (IMT)-2020 (5G) Strategy for Namibia (2023-2027)[23] approved by the Cabinet in 2022. MTC expanded its fibre optic network to 2,738 kilometres by March 2025,[24] and in September 2025, extended its fixed internet service, Spectra, to towns including Oshifo, Aranos, Maltahöhe, Rietoog, Stampriet, Khorixas, Tsandi, and Otavi.[25] According to the ICT Development Index (IDI) 2025 published by the International Telecommunication Union (ITU)[26],Namibia has increased its overall score on digital development over the period of 2024-2025. In particular, the IDI score of Namibia grew to 73.2% in 2025, whereas universal connectivity improved to 63.0%. Essentially, connectivity indicators showed small increases within the same period. In 2024, the population of Namibia using the Internet was 64.3%[27], and it slightly increased to 64.4% in 2025.

The most significant shift was at the household level: the number of house

16. Telecom activates Equiano Cable connection, The Brief, July 2024, https://thebrief.com.na/2024/07/namibia-activates-equiano-cable-connection/ (Accessed: 19 December 2024)
17. Communications regulator launches Universal Service Fund to boost ICT access https://economist.com.na/96240/technology/communications-regulator-launches-universal-service-fund-to-boost-ict-access/ (Accessed: 19 December 2024)
18. Govt commits N$145 million to bridging rural digital divide https://www.namibian.com.na/govt-commits-n145-million-to-bridging-rural-digital-divide/ (Accessed: 29 November 2025)
19. Govt commits to bridging digital divide https://neweralive.na/govt-commits-to-bridging-digital-divide (Accessed: 29 November 2025)
20. Namibia: Paratus Launches N$600m Nationwide Mobile Network Covering 50 Towns https://allafrica.com/stories/202509030174.html (Accessed: 29 November 2025)
21. Paratus launches N$600m nationwide mobile network covering 50 towns https://thebrief.com.na/2025/09/paratus-launches-n600m-nationwide-mobile-network-covering-50-towns/ (Accessed: 29 November 2025)
22. Telecom Namibia Rolls Out 5G-Ready Base Stations in Nationwide Network Modernisation Drive https://trendsnafrica.com/telecom-namibia-rolls-out-5g-ready-base-stations-in-nationwide-network-modernisation-drive/ (Accessed: 29 November 2025)
23. Strategy In Respect Of Implementation Of Imt-2020 (5g) In The Republic Of Namibia 2023-2027 https://www.lac.org.na/laws/2023/8000.pdf (Accessed: 29 November 2025)
24. MTC expands network capacity with major fibre expansion https://economist.com.na/95750/technology/mtc-expands-network-capacity-with-major-fibre-expansion/ (Accessed: 22 November 2025)
25. MTC expands fiber internet to key towns and settlements https://economist.com.na/100471/technology/mtc-expands-fiber-internet-to-key-towns-and-settlements/ (Accessed: 22 November 2025)
26. Measuring Digital Development The ICT Development Index 2025 https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICT_MDD-2025-1-PDF-E.pdf (Accessed: 19 November 2025)
27. ICT Development Index 2023, ITU,https://trc.gov.jo/EchoBusV3.0/SystemAssets/وريقت%202023_compressed.pdf accessed 19 December 2024

holds with internet access at home increased by 66.3% to 78% which means that home broadband access is becoming more widespread in the country. Mobile access remains at the heart of the Namibian digital ecosystem, as mobile broadband subscriptions hit 58.6 per 100 inhabitants in 2025, and mobile phone ownership rose to 86.6.

Internet coverage is quite dense, with 89% of the population having access to at least a 3G network and 85% of the population covered by 4G/LTE in 2025. The affordability indicators in the index indicate that the price of mobile services, which is a high consumption basket, is at 1.4% of Gross National Income (GNI) per capita, and fixed broadband prices are high at 7.7%, which could explain the high reliance on mobile services.

The 2025 ITU IDI report further shows no data for fixed broadband subscriptions. However, it indicates that Namibia has a 98% mobile data as well as voice high consumption basket price in the percentage of Gross National Income (GNI) per capita and a fixed broadband internet basket price (as % of GNI per capita) of 79.3%. There were efforts recorded to improve cross-border roaming charges with neighbouring countries. Towards the end of 2024, following high-level ministerial talks, Namibia and Botswana agreed to reduce roaming charges effective from August 2024, continuing into the review period.[28] CRAN and Botswana Communications Regulatory Authority (BOCRA) directed mobile network operators in both countries to implement reduced roaming prices to boost cross-border communication and strengthen bilateral relations whilst fostering economic opportunities. Furthermore, Minister of Information, Communication, and Technology Emma Theofelus announced in January 2025 that the Ministry engaged Zimbabwe, Zambia, and Angola on harmonisation of roaming fees,[29] indicating expanding regional cooperation to reduce telecommunications costs. At the beginning of 2025, satellite internet provider Starlink was eyeing Namibia's telecommunications market as part of its broader African expansion, having already established operations in over 20 African countries by mid-2025.[30] However, by July 2025, the Communications Regulatory Authority of Namibia (CRAN) issued a cease-and-desist order to Starlink, demanding the immediate halt of all operations due to the company's failure to obtain the required telecommunications licence.[31] The situation escalated in November 2025 when CRAN confirmed that Starlink had been operating a network within Namibia without proper authorisation, leading to the confiscation of illegal terminal equipment from consumers and the opening of criminal cases with the Namibian Police.[32]

28. Namibia and Botswana cut roaming charges for better cross-border communication https://economist.com.na/91126/technology/namibia-and-botswana-cut-roaming-charges-for-better-cross-border-communication/ (Accessed: 22 November 2025)
29. ICT Minister engages Zimbabwe, Zambia and Angola on harmonization of roaming fees https://www.nbcnews.na/index.php/node/109231 (Accessed: 22 November 2025)

Freedom of expression

In 2025, Namibia was ranked 28th in the World Press Freedom Index,[33] which is an improvement from the 2024 country's global ranking of 34.[34] The Reporters Without Borders ranking cites Namibia's freedom of the press as firmly anchored, and historically one of Africa's best-ranked countries in the Reporters Without Borders (RSF) World Press Freedom Index. The government's response to viral misinformation in April 2025 demonstrated a measured approach. False claims circulated on social media platforms such as Facebook, X (formerly known as Twitter), TikTok and WhatsApp alleging that President Netumbo Nandi-Ndaitwah had ordered the deportation of 500 American citizens. The Presidency issued a public clarification noting "with concern

30. Starlink Expanding in Africa https://blog.telegeography.com/starlink-expanding-in-africa (Accessed: 22 November 2025)
31. Namibia orders Musk's Starlink to shut down https://techpression.com/namibia-orders-musks-starlink-to-shut-down/ (Accessed: 22 November 2025)
32. Starlink's use ruled illegal in Namibia https://www.republikein.com.na/mw-main/starlink%E2%80%99s-use-ruled-illegal-in-namibia2024-12-02142183 (Accessed: 10 November 2025)
33. Press Freedom Index: Namibia Ranks Four Places Higher than the UK, Namibian Org, May 2023, https://namibian.org/news/tourism/press-freedom-index-nambia-ranks-four-places-higher-than-the-uk (Accessed: 4 November 2025)
34. Disappointment as Namibia loses top position on press freedom, The Namibian, May 2024, available at https://www.namibian.com.na/disappointment-as-namibia-loses-top-position-on-press-freedom/ (Accessed:4 November 2025)

the circulation of social media posts and online articles" containing "fabricated quotes and images containing misinformation and disinformation intended to tarnish the image of the President." [35] Whilst no systematic studies on self-censorship were published during the review period, concerning indicators emerged. Reports in May 2025 documented that "verbal attacks on journalists are increasing," [36] potentially creating chilling effects. The case of Namibian Sun Senior Reporter Jemima Beukes, subjected to disciplinary proceedings by her employer in March 2025,[37] raised concerns about internal pressures. The Namibia Media Professionals Union (NAMPU) called for the media house, Namibia Media Holdings (NMH), to "treat one of its reporters like a human being and with dignity." [38] Despite such incidences, no documented cases of arbitrary arrests, detention, or prosecution specifically for online speech occurred during December 2024 to November 2025. The Namibia Media Trust/Foundation (NMT) published research in December 2024 on "The Digital Closet," exposing the impact of online hate speech on Namibia's Lesbian, Gay, Bisexual, Transgender, and Queer (LGBTQ+) community,[39] highlighting how marginalised groups, including gender-diverse persons faced targeted online violence, constraining their public participation. From an AI-generated image Netumbo Nandi Ndaitwah, then-candidate of the ruling party and President-elect falling, to a fake video of Independent Candidate Ally Angula, of "God asking her to withdraw" from the elections,[40] gendered disinformation was at its peak during elections. These and other matters, such as increased news on the health of the Founding President, Sam Nuyoma,[41] had the Minister of ICT calling for responsible use of social media.[42]

Meanwhile, further civil defamation cases have been seen in courts particularly brought and won by the more affluent such as a businessman who sued a citizen to the tune of N$773 000 (US$ 41,300) for questioning, via a social media audio clip, the expenses on his wedding versus public hospitals being left without medicine. The businessman supplies state hospitals with medicines as well as other medical supplies.[43] Another notable case is that of an academic and politician who has taken legal action against a fellow political member and is suing them for N$370,000 (US$ 23,000). The lawsuit stems from a series of allegations made by a citizen through a widely circulated WhatsApp audio clip, which the plaintiff claims is entirely false and defamatory.[44]

Data Protection and Privacy

To safeguard data governance and build national cyber resilience, the Communications Regulatory Authority of Namibia (CRAN) established the Namibia Cyber Security Incident Response Team (NAM-CSIRT) in March 2025.[45] The Namibian government allocated N$20 million (USD 1,25 million)[46] in seed money for the op

35. Nandi-Ndaitwah dismisses social media claims of American deportations from Namibia https://www.namibian.com.na/nandi-ndaitwah-dismisses-social-media-claims-of-american-deportations-from-namibia/ (Accessed: 4 November 2025)
36. Verbal attacks on journalists increasing https://www.observer24.com.na/verbal-attacks-on-journalists-increasing/ (Accessed: 22 November 2025)
37. Media union calls for justice for journalist Jemima Beukes in NMH disciplinary hearing https://www.namibian.com.na/media-union-calls-for-justice-for-journalist-jemima-beukes-in-nmh-disciplinary-hearing/ (Accessed: 22 November 2025)
38. NMH dismisses Jemima Beukes https://www.namibian.com.na/nmh-dismisses-jemima-beukes/
39. Press Statement: New study calls for bold reform of Namibia's media accountability framework https://www.nmt.africa/Media-Centre/Press-Statements (Accessed: 19 November 2025)
40. Election fake news surge in October 2024, Namibia Fact Checker, November 2024, https://namibiafactcheck.org.na/news-item/election-fake-news-surge-in-october-2024/ (Accessed: 4 November 2025)
41. Sam Nujoma Foundation Condemns Fake News on Social Media, Observer, November 2024, https://www.observer24.com.na/sam-nujoma-foundation-condemns-fake-news-on-social-media/ accessed November 2024.
42. Theofelus urges responsible social media use, Namibian Economist, August 2024, available at https://economist.com.na/90062/technology/theofelus-urges-responsible-social-media-use/ accessed November 2024
43. Shapwa Kanyama donates N$773 000 defamation award to cyberbullying victims, Namibian December 2024, https://www.namibian.com.na/shapwa-kanyama-donates-n773-000-defamation-award-to-cyberbullying-victims/ accessed in November 2024
44. Swapo School Lecturer Mubita sues Shipwikineni for defamation, Observer, February 2024, available at https://www.observer24.com.na/swapo-school-lecturer-mubita-sues-shipwikineni-for-defamation/ (Accessed: 22 November 2025)
45. CRAN hosts inaugural NAM-CSIRT Stakeholder Engagement. https://nambusinessexpress.com/?p=9216 (Accessed: 22 November 2025)
46. Government invests N$20 million to strengthen Namibia's cybersecurity. https://nambusinessexpress.com/?p=9216 (Accessed: 22 November 2025)

erationalisation of the NAM-CSIRT[47]. Between January and June 2025, NAM-CSIRT recorded 1,103,784 instances of cyber threats and 1,090,342 vulnerabilities, representing the highest figures logged since the national cybersecurity body was established and underscoring the urgency of comprehensive legislative frameworks.[48] Though such efforts exist, according to various experts, the absence of a robust Data Protection Act was cited as to blame for the massive cyber terrorist attack on the country's key telecommunications provider and other government institutions that took place towards the end of December 2024 and during the year in 2025.[49] The MICT stated on various occasions during the review period that it would table the Data Protection Bill in Parliament in September 2025; however, that did not materialise. [50] The Bill has circulated in various draft forms since 2021-2022 but remained unenacted by November 2025.[51] The Bill, published for consultation in March 2022, aimed to establish a data protection supervisory authority and provide protections aligned with international standards, including principles from the European Union (EU) General Data Protection Regulation (GDPR). Activists continued to urge the government to enact a Data Protection Act, as the legislative gap leaves citizens vulnerable to data misuse and surveillance, especially as technologies like biometric registration and interception systems become more widespread.[52] Article 13 of the Namibian Constitution recognises the right to privacy as a fundamental human right, stipulating that all persons have a right to privacy in their homes and communications. However, this constitutional protection lacks comprehensive statutory implementation through dedicated data protection legislation. The Civil Registration and Identification Act received presidential assent and was published in Government Gazette 8547 on December 30 2024.[53] This legislation, awaiting commencement, would establish a comprehensive civil registration system and provide for the issuance of identity documents using biometric data. An assessment by the Association for Progressive Communications in September 2024 found that whilst "Namibia's newly proposed Civil Registration and Identification Bill has been praised for containing essential elements of data protection," the government still needed "to finalise work on pending efforts to put in place a personal data protection law." [54]

Minister of ICT, Emma Theofelus has issued a warning about the increasing threat of cyber scams and AI-driven deception in Namibia. While addressing lawmakers in the National Assembly, Theofelus detailed the government's response measures, emphasising the need for updated regulations. She highlighted the surge in digital fraud, including synthetic media, deepfakes, and social media scams that leverage AI technologies.[55]

Namibia has not adopted policies and laws on cybercrime, data protection, or the protection of personal identifiable information. While the country has a Child Online Protection Task Force,[56] Namibia has no child online protection policy. In February 2025, private mobile service provider, Paratus Namibia reported a significant breach following a compromised internal user account that disrupted 083 voice services and cloud environments.[57] CRAN classified it as Level Three, signifying serious disruption to the telecommunications sector. This was the most high-profile cybersecurity incident

47. Namibia Strengthens Regional Cooperation In Transport, Ict, Information And Meteorology - Harare, Zimbabwe https://www.cran.na/namibia-strengthens-regional-cooperation-in-transport-ict-information-and-meteorology-harare-zimbabwe/ (Accessed: 4 November 2025)
48. Namibia says detects over 1 mln instances of cyber threats in six months https://english.news.cn/africa/20251009/772ad7399e5a46f8a01ba1c26d731634/c.html (Accessed: 22 November 2025)
49. Lack of oversight and legislation blamed for cyber attack https://www.observer24.com.na/namibia-does-not-negotiate-with-terrorists-shanapinda/ (Accessed: 22 November 2025)
50. Namibia's Data Protection Bill to be tabled in September https://thebrief.com.na/2025/08/namibias-data-protection-bill-to-be-tabled-in-september/ (Accessed: 19 November 2025)
51. Cabinet yet to finalise data protection bill https://www.observer24.com.na/cabinet-yet-to-finalise-data-protection-bill/
52. Namibia Urged to Tackle Digital Privacy Gaps https://www.confidentenamibia.com/namibia-urged-tackle-digital-privacy-gaps (Accessed: 22 November 2025)
53. Civil Registration and Identification Act, 2024 https://namiblii.org/akn/na/act/2024/13/eng@2024-12-30 (Accessed: 22 November 2025)
54. Namibia's new CRVS, national ID system reflects key data protection aspects https://www.biometricupdate.com/202409/namibias-new-crvs-national-id-system-reflects-key-data-protection-aspects (Accessed: 19 November 2025)
55. ICT Minister highlights growing impact of artificial intelligence https://www.nbcnews.na/node/110380 (Accessed: 19 November 2025)
56. Namibians encouraged to protect rights of children in the Digital Realm, NBC, January 2024, https://nbcnews.na/node/101414 accessed January 2025
57. CRAN investigates serious cyber incident at Paratus https://economist.com.na/95702/technology/cran-investigates-serious-cyber-incident-at-paratus/ (Accessed: 19 November 2025)

documented during the review period.

Censorship and content moderation

The decision of the Meta Oversight Board on June 3 2025 found that Meta's adult nudity rules were being applied in a way that disproportionately restricts expression when it comes to images of bare-chested Indigenous women, including Ovahimba women in Namibia.[58] The Board reviewed two Instagram cases from July 2024 showing Ovahimba women in traditional dress (one a tourist's photo, one a video of Himba people dancing). Meta removed the content under its Adult Nudity and Sexual Activity policy after automated and human review. The Board ruled that Meta was wrong in both instances, because bare-chested nudity is a socially and historically accepted part of Himba custom and there were sufficient signs of implicit consent, so a "spirit of the policy" allowance should have applied.[59]

More broadly, the Board said Meta's near-total ban, with only ad hoc exceptions, unjustifiably limits Indigenous people's cultural expression and public access to information about those cultures. It ordered the Ovahimba content restored, criticised the inconsistency with Meta's human rights responsibilities, and recommended that Meta publicly spell out and properly apply a clear exception for Indigenous nudity when it reflects socially accepted customs and is not misrepresented.[60] In July 2025, a Namibian lawyer sued global tech search engine Google for US$10 million (N$180 million) because the company refused to remove some defamatory content. Tech expert Nrupesh Soni says despite the landmark judgement, compelling Google to comply with the court order could be tricky given the lack of Namibia's data protection laws and the absence of Google representation in the country.[61]

Furthermore, between April 2022 and April 2025, the Namibian Police (NAMPOL) recorded 4,835 defamation cases, many involving public figures and social media influencers.[62] According to NAMPOL, six human trafficking cases were also recorded, involving 38 Namibians recruited via online platforms to work abroad, 50 recruited to work within the country, and four foreign nationals recruited to work locally.[63]

Namibia has no domestic laws enforcing content moderation. Data from the Meta Transparency report,[64] covering January to June 2025 as part of Meta's processes to respond to government requests for data in accordance with applicable law and terms of service, indicates there were no requests, legal process requests, emergency disclosure requests, users/accounts requested and finally no requests where some data was produced. The content moderation report by Google[65] indicates that there have been 44 total items named for removal by the Government between 2011 and 2022, while there have been three total removal requests received since 2011. Furthermore, no report has been published by TikTok on content takedown.[66]

The national launch of the Ethical Use of Social Media Campaign was launched during the reviewed period. The initiative is led by the Ministry of Information and Communication Technology (MICT) in partnership with the Namibian Police and Club de Madrid. Emma Theofelus, Minister of ICT, described the initiative as "not just an announcement, but a call to action for all users to contribute to a

58. Ban on Showing Indigenous Nudity Disproportionately Limits Expression https://www.oversightboard.com/news/ban-on-showing-indigenous-nudity-disproportionately-limits-expression/ (Accessed: 19 November 2025)
59. Images of Partially Nude Indigenous Women https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2025/06/OB-Indigenous-Nudity-Women-case.pdf (Accessed: 19 November 2025)
60. 'Indigenous nudity content on platforms needs exception guidelines' https://nimca.africa/2025/06/03/indigenous-nudity-content-on-instagram-facebook-needs-exception-guidelines/ (Accessed: 19 November 2025)
61. Namibian lawyer sues Google over defamatory content https://www.namibian.com.na/namibian-lawyer-sues-google-over-defamatory-content/ (Accessed: 19 November 2025)
62. Over 4 000 Namibians sue each other for online attacks https://www.observer24.com.na/over-4-000-namibians-sue-each-other-for-online-attacks/ (Accessed: 4 November 2025)
63. Unemployed Namibians Targeted in Human Trafficking https://www.thevillager.com.na/national/2025/unemployed-namibians-targeted-in-human-trafficking/ (Accessed: 4 November 2025)
64. Namibia, Government Requests for User Data, Meta, 2024 https://transparency.meta.com/reports/government-data-requests/country/NA/ accessed December 2024
65. Government removal requests by the numbers: Namibia, Google, https://transparencyreport.google.com/government-removals/government-requests/NA (Accessed: 19 November 2025)
66. Transparency Center, Tik Tok, https://www.tiktok.com/transparency/en-us/government-removal-requests-2024-1 accessed December 2024

healthier, more informed digital community." She urged attendees to "think before they post, verify before they share, and engage without causing harm."[67]

Access to Information

Namibia passed the Access to Information (ATI) law in 2022[68] after being drafted in 2016 and tabled in Parliament in June 2020. In February 2025, the Communications Regulatory Authority of Namibia (CRAN) established a dedicated ATI division within the Authority.[69] The division is housed in the communication and consumer relations department, and will be responsible for implementing the Access to Information Act. However, Civil Society Organisations have noted that only once an Information Commissioner is appointed will a critical step towards the full implementation of the Access to Information (ATI) Act of 2022 take place.[70]

AI and Emerging Technologies

In August 2025, the Cabinet approved the drafting of a Space Science and Technology Bill, which will provide a legal and institutional framework to guide Namibia's space-related activities. The proposed legislation is underpinned by Namibia's Space Science and Technology Policy (2021–2030), which aims to transition the country from being a passive user of space-based services to an active participant in the global space industry. The policy calls for the integration of space technologies into national development planning, improved public awareness, institutional capacity-building, and expanded access to commercial space applications.[71] In August 2025, Namibia launched its Artificial Intelligence Readiness Assessment Methodology Report. The assessment represents the country's first structured evaluation towards adapting, developing and governing AI, in line with inclusive and ethical development principles. The project was carried out by the United Nations Educational, Scientific and Cultural Organisation (UNESCO) in collaboration with the National Commission on Research, Science and Technology (NCRST).[72] Namibia is in the process of establishing a National AI strategy under the National Commission on Research, Science and Technology (NCRST). NCRST appointed a pool of AI experts to the Technical Advisory Committees (TACs) to develop the strategy.[73] The use of artificial intelligence (AI) is prevalent in various sectors such as education, health, agriculture and labour as reported by a UNESCO report of 2022 that discusses the benefit of AI towards the country's economy and the potential to bridge the digital divide between Namibia and other developing countries.[74] To date, several AI developments have been noted in the country, including the launch of the AI and Robotics Lab[75] at the Namibia University of Science and Technology (NUST) in partnership with the Bank of Namibia. This partnership is expected to herald a transformative step towards modernising Namibia's educational and technological landscape, placing the nation on the map for AI and robotics innovation.

This and other conversations on AI stem from the 2022 Windhoek Statement on Ar

67. Ethical Use of Social Media Campaign Launch https://www.nust.na/think-you-click (Accessed: 19 November 2025)
68. Access to Information Act, no 8 of 2022, available at http://www.lac.org.na/laws/2022/7986.pdf (Accessed: 19 November 2025)
69. Communications regulator launches access to information division https://www.namibian.com.na/communications-regulator-launches-access-to-information-division/ (Accessed: 4 November 2025)
70. Appointment of information commissioner set to boost procurement transparency https://www.namibian.com.na/appointment-of-information-commissioner-set-to-boost-procurement-transparency/ (Accessed: 4 November 2025)
71. Cabinet approves drafting of Space Science and Technology Bill https://thebrief.com.na/2025/08/cabinet-approves-drafting-of-space-science-and-technology-bill/ (Accessed: 19 November 2025)
72. Artificial intelligence readiness assessment report: Namibia https://unesdoc.unesco.org/ark:/48223/pf0000394686 (Accessed: 22 November 2025)
73. Namibia Kicks Off National AI Strategy Development https://www.facebook.com/ncrst.na/posts/namibia-kicks-off-national-ai-strategy-developmentthe-national-commission-on-res/1280851653827042/ (Accessed: 4 November 2025)
74. AI could bridge Namibia's Digital Gap if challenges are tackled. Namibian Sun, November 2024, available at https://www.namibiansun.com/technology/ai-could-bridge-namibias-digital-gap-if-challenges-tackled2024-11-11 (Accessed: 19 November 2025)
75. NUST, Bank of Namibia Partner Launch AI and Robotics Accelerator, NUST, November 2024 available at https://www.nust.na/nust-bank-namibia-partner-launch-ai-and-robotics-accelerator (Accessed: 19 November 2025)

tificial Intelligence in Southern Africa[76] by UNESCO that sets recommendations on AI and Data Governance, Capacity-Building and Awareness-Raising, Investment and Infrastructure, Education, Research, Development and Innovation, Environment and Disaster Risk Reduction, Gender, Collaboration and Partnerships.

Access to Information

The Universal Service Fund (USF) provides financial support to mobile network operators to mitigate the challenges of expanding services in high-risk, low-return areas. By offering subsidies, the fund facilitates the introduction of advanced technologies in remote regions, ensuring equitable access to digital resources.[77] In November 2025, phase one of the Universal Service Fund (USF) rollout began, with MTC handing over the first completed network tower under the programme.[78] USF rollout will give more than 9,000 Namibians access to 4G, many for the first time. Phase one focuses on remote communities in Kavango West, Kavango East, Kunene, Oshikoto, and Ohangwena. The goal is to reach at least 80% broadband coverage in underserved areas.[79] Namibia is finalising preparations to launch the e-ID in 2026, supported by a significant budget allocation. The new system will be built on the Model Governance Framework's principles of security, inclusion and human rights. Simultaneously, the country is deploying NamX, a data-exchange platform that allows ministries to share information securely, and Nampay, a real-time payment system for instantaneous transfers. When combined, these components will form the backbone of Namibia's digital economy.[80]

The Home Affairs ministry has announced the roll-out of Namibia's first electronic identity card (e-ID), scheduled for launch by July 2026. The move is expected to overhaul identity management and streamline access to both public and private services nationwide. Developed in partnership with the United Nations Development Programme (UNDP) and aligned with its model governance framework for digital legal identity, the e-ID initiative is designed to modernise and ultimately redefine Namibia's civil registration system.[81] The Civil Registration and Identification Act received presidential assent and was published on December 30 2024, representing new legislation enabling the digital ID system. However, it awaited the commencement of implementation.[82] The government announced July 2026 as the rollout date for the national digital ID system in June 2025.[83] Home Affairs Minister Lucia Iipumbu called for "clear timeline" and "strong awareness campaigns" about the system's benefits.[84]

76. Windhoek Statement on Artificial Intelligence in Southern Africa, Windhoek (Namibia), 9 September 2022, UNESCO available at https://unesdoc.unesco.org/ark:/48223/pf0000383197 (Accessed: 19 November 2025)
77. Communications regulator launches Universal Service Fund to boost ICT access https://economist.com.na/96240/technology/communications-regulator-launches-universal-service-fund-to-boost-ict-access/ (Accessed: 19 November 2025)
78. New USF tower brings 4G to Ohangwena community https://www.observer24.com.na/new-usf-tower-brings-4g-to-ohangwena-community/ (Accessed: 19 November 2025)
79. Namibia Launches First Universal Service Fund Tower to Expand Rural Connectivity https://techafricanews.com/2025/11/19/namibia-launches-first-universal-service-fund-tower-to-expand-rural-connectivity/ (Accessed: 4 November 2025)
80. Season 3: Namibia's Digital Identity Journey – From Vision to Reality https://www.undp.org/namibia/blog/season-3-namibias-digital-identity-journey-vision-reality (Accessed: 4 November 2025)
81. Namibia to launch groundbreaking electronic ID by 2026 https://www.namibiansun.com/government/namibia-to-launch-groundbreaking-electronic-id-by-20262025-06-10159527 (Accessed: 4 November 2025)
82. Civil Registration and Identification Act, 2024 https://namiblii.org/akn/na/act/2024/13/eng@2024-12-30 (Accessed: 19 November 2025)
83. Namibia to roll out digital ID card in July 2026 https://www.biometricupdate.com/202506/namibia-to-roll-out-digital-id-card-in-july-2026 (Accessed: 22 November 2025)
84. Namibian govt aims for strong public awareness on digital ID as rollout nears https://www.biometricupdate.com/202504/namibian-govt-aims-for-strong-public-awareness-on-digital-id-as-rollout-nears (Accessed: 4 November 2025)

Conclusion

As a moderately compliant country with the African Commission on Human and Peoples' Rights (ACHPR) Declaration, Namibia has made steps to ensure digital inclusion and combat cyber threats. However, without comprehensive digital rights laws the country still has a lot to do to protect its citizens' online rights. Digitally enabled threats and a significantly expanding threat surface, especially in a consumer market with low levels of security awareness. This remains a challenge for Namibians at an economic level. The lack of sector-related laws has enabled a wide range of cyber threats, with social engineering and phishing attacks topping the list.

The country's provisions of telecommunications surveillance in the current Communications Act, the lack of transparency on the usage of biometrics collected during SIM regulations, and other potential means of surveillance are key concerns for human rights in the digital era. Furthermore, the lack of accountability for internet intermediaries and the lack of mechanisms to promote digital inclusion for children and people with disabilities through the USF remains an inclusion concern. This is in addition to the need for support and sustainability of independent media. Finally, considerable steps need to be enforced by Namibia to ensure the policy for Artificial Intelligence use, amongst others.

Recommendations

The Government should:

- Pass the Data Protection legislation which must ensure that necessary oversight mechanisms are in place in addition to ensuring personal data protection recourse for individuals.
- Make sure that the USF includes previously marginalised groups such as persons with disability, children and indigenous women and girls.
- Adopt specific child laws, policies and measures promoting children's digital safety and privacy online.
- Develop an AI national policy and strategy to address the design, use and deployment of AI in Namibia.
- Require internet intermediaries to ensure that in moderating or filtering online content, they mainstream human rights safeguards into their processes, adopt mitigation strategies to address all restrictions on freedom of expression and access to information online

Private Sector should:

- Ensure transparency on all requests for removal of content, and incorporate appeal mechanisms.
- Collaborate towards improving digital literacy in the country and narrowing data and device access gaps.

Civil Society Organisations should:

- Provide education on Digital Rights and Inclusion
- Continue shedding light on issues of infringements of Digital Rights and Inclusion in the country.

Media should:

- Monitor and report on the implementation of the Universal Service Fund (USF), including its effectiveness in the expansion of internet access to underserved communities.
- Report on and turn digital rights into real-life stories that people can relate to
- Follow-up on the Data Protection Bill and other digital laws

The Score Index

Nigeria, 2025

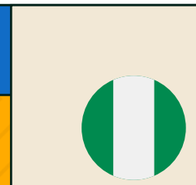
1 = Totally non-compliant; 2 = Mildly compliant; 3 = Moderately compliant;
4 = Considerably compliant; 5 = Fully compliant

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	5	5	No internet shutdowns were recorded.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	2	4	Namibia launched the Universal Service Fund (USF) to provide financial support to mobile network operators to mitigate internet access challenges. Phase one of the Fund was rolled out and will give more than 9,000 Namibians access to 4G, many for the first time.
False News Criminalisation	P22(2)	4	4	Namibia has no laws that criminalise the publication of false news.
Sedition Legislation	P22(2)	5	5	Namibia has no laws that criminalise sedition, insult and publication of false news.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	4	3	While the State has guaranteed the safety of journalists and other media practitioners. There were a few cases of harassment of journalists such as Jemima Beukes. However, the state has not taken measures to prevent attacks on journalists and other media practitioners, including various forms of ill-treatment, such as, intimidation, threats and unlawful surveillance undertaken by State and non-State actors.
Data Protection Legislation.	P42	4	4	The State has not adopted laws for the protection of personal information of individuals in accordance with international human rights law and standards and individuals have no legal recourse to effective remedies in relation to the violation of their privacy and the unlawful processing of their personal information.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	4	4	There is no evidence that the State required internet intermediaries to proactively monitor content which they have not authored or otherwise modified.
States interfere and require the removal	P38 and P39(4)	4	4	There is no evidence that the State required internet intermediaries to proactively monitor content which they have not authored or otherwise modified.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
of online content by internet intermediaries				
Invasion of Privacy of Communications	P41	4	4	Part 6 of the Communication Act 8 of 2009, institutes interceptions of telecommunications. This provision gives indication that states engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	3	3	While there has been proactive disclosure by public institutions even in the absence of a specific request, to proactively publish information of public interest, including information about their decisions such as regular Cabinet Decision announcements and budgets, expenditure and other information relating to their activities more can be done for full disclosure on public spending.
AI and Emerging Technologies national strategies	P39(6)	2	2	While the country is developing a National AI Strategy, it has not yet completed the development of the framework on the development, use and application of artificial intelligence, algorithms and other similar technologies. The use of such by internet intermediaries is governed and compelled to be compatible with inter

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
				national human rights law and standards, nor is there a requirement for such not to infringe on the rights to freedom of expression, access to information and other human rights.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P39(6)	2	2	While the Draft Cybercrime bill makes provision for the protection of Children online, no other existing laws are in place to ensure the safety of children. A Child Online Protection Task Force however is in place overseeing serious cases, working without cases.
Digital Inclusion	P37(3)	4	3	The Universal Service Fund became fully operationalised and has been rolled out in remote places such as the Kavango regions. In 2025, Paratus Group became Namibia's first privately-owned mobile network in September 2025. Backed by a N$600 million (US$ 37,7 million) investment and built entirely on 4G LTE technology, the network covered 50 major towns. Furthermore, the move challenged the longstanding duopoly of the state-owned Mobile Telecommunications Company (MTC) and Telecom Namibia, introducing new competitive dynamics that could benefit coverage expansion and service quality.
Total (out of 60):	2024: **39**		**2025 42**	



Nigeria

By Khadijah El-Usman and Muhammed Bello Buhari

Executive Summary

In 2025, Nigeria's digital rights landscape reflected a mix of slow recovery, persistent structural weaknesses, and emerging reforms. Connectivity improved modestly after the disruptions caused by the government-mandated requirement that all SIM cards should be linked to the owner's National Identity Number (NIN), with broadband penetration reaching 49.34%.[1] However, this recovery remains fragile, affordability-constrained, and unevenly distributed, falling significantly short of the National Broadband Plan target of 70% by 2025. Although there is no concrete proof that the sub-national network shutdown experienced in Nigeria's Zamfara state was ordered by the government, access was also constrained by the first increase in the cost of telecommunications services since 2013 and uneven network quality.

Freedom of expression remained fragile, shaped by overlapping laws, opaque con

tent-removal practices, informal state pressure on platforms, and a pattern of state-level arrests and institutional sanctions that cumulatively undermine legality, necessity, and proportionality standards under the African Commission on Human and Peoples' Rights' Declaration of Principles of Freedom of Expression and Access to Information in Africa, deepening self-censorship. In spite of this, a landmark Supreme Court ruling affirming the full applicability of the Freedom of Information Act, including for sub-national governments, is worth celebrating. Progress in data protection included stronger oversight by the Nigeria Data Protection Commission (NDPC), yet recurrent data leaks and non-compliance by government agencies highlighted critical gaps. Surveillance expanded through new drone and AI-powered monitoring systems without corresponding transparency or safeguards.

Nigeria also advanced emerging technology governance through a National AI strategy, the launch of Nigerian Atlas for Languages & AI at Scale (N-ATLAS), and legislative momentum on AI regulation. At the same time, digital inclusion efforts progressed through child online safety reforms and assistive technology initiatives, despite persistent accessibility barriers. Universal service interventions continued, but delayed USPF reporting (the latest annual report available is from 2022) significantly constrained transparency and prevented a credible assessment of whether these interventions reduced access gaps for underserved communities. The report utilised Paradigm Initiative's TheScore Index to assess Nigeria's compliance with the Declaration. With an overall score of 35/60, Nigeria is moderately compliant, reflecting meaningful developments but significant risks that require urgent regulatory, institutional, and rights-protective reforms.

1. Nigerian Communications Commission (NCC) Industry Statistics, as reported in "BROADBAND: Nigeria Unlikely to Achieve 2025 Target as Penetration Stands at 49.34%," TechEconomy (November 2025). Available at: https://techeconomy.ng/broadband-nigeria-unlikely-to-achieve-2025-target-as-penetration-stands-at-49-34the full applicability of the Freedom of Information Act/

Introduction

Since 2016, Nigeria's digital rights environment has evolved through a mix of state-led reforms and advocacy-driven pressure. Broadband access rose from 20.95% in 2016 to 49.34% in 2025, mainly driven by government initiatives such as the National Broadband Plan and spectrum expansion for 4G and 5G. Key legal reforms also emerged, including the passage of the Nigeria Data Protection Act (2023) and the amendment of the Cybercrimes Act (2024), both state-driven responses influenced by sustained advocacy highlighting gaps in privacy and digital safety. Several advancements, however, were secured through civic action rather than state initiative. An example of this is that after an 11-year legal battle led by journalists and civil society, the Supreme Court affirmed full Freedom of Information Act (FOIA) applicability across the federation in 2024, strengthening access to information. Progress on child online protection also reflected combined legislative action and years of advocacy around online harms. Disability inclusion gained momentum through the Disability Act (2018) and subsequent pressure for assistive technology and accessibility standards.

Despite these gains, persistent challenges illustrate the imbalance of power between the State and users. Restrictions on freedom of expression continued through arrests of online critics, reliance on criminal defamation laws and security-driven regulation. Surveillance capacity expanded significantly through drones, AI-powered monitoring and biometric upgrades without commensurate transparency or oversight. Nigeria's trajectory from 2016 to 2025, therefore, reflects both progress and ongoing systemic risks, with state-driven reforms often competing with patterns of overreach, while advocacy-driven wins fill accountability gaps.

Internet Access And Disruptions

Reporting Connectivity in the 2024 Londa report was shaped by the final enforcement of the NIN–SIM linkage policy, which resulted in millions of disconnections and a steep decline in the number of active mobile users. The situation was compounded by proposed tariff hikes across the sector, including a 97% increase announced by Starlink, signalling growing pressure on consumers.

By the end of December 2025, the sector had begun a slow recovery. Active mobile subscriptions rose by 10.3 million over the year to reach 179.64 million, pushing teledensity upward to 82.87%,[2] though still well below the numbers reported before the government forced citizens to connect their National Identity Numbers (NIN) to independently registered SIM cards. Broadband access also saw steady progress, with internet subscriptions pushing official broadband penetration to 51.97%. However, because this metric counts total active SIM cards rather than unique individual subscribers, it inherently overstates actual human connectivity due to the high prevalence of multiple SIM card ownership in Nigeria. Even with this inflation, reaching 51.97% penetration for broadband and non-broadband connections means the country falls critically short of the 70% broadband connectivity target set out in the National Broadband Plan for 2025.

Furthermore, the technological distribution of these connections shifted toward higher-capacity networks by year-end. 4G solidified its dominance at 52.95% of total connections (serving roughly 95 million users), while 5G adoption rose to 3.77%. Conversely, legacy networks lost share, with 2G dropping to 37.37% and 3G falling to 5.91%.[3] Because 2G infrastructure provides narrowband connectivity (often capping around 500kbps) rather than true broadband, this data highlights a severe quality-of-service gap. This uneven distribution limits meaningful access for underserved communities; reliance on 2G significantly restricts the ability to exercise rights online, including access to information, economic participation, education, and essential digital services, compared to urban 4G-dominant areas. Meanwhile, national data consumption surged past 13.2 million terabytes in 2025, a 35% increase over 2024, underscoring a rapidly growing appetite for digital services that the current infrastructure struggles to equitably match.[4]

On affordability, a 50% tariff hike was announced by telcos in January, and it took effect in February 2025. This is the first time approval has been granted for an increase in prices since 2013. Nigerian Communications Commission (NCC) capped the tariff adjustment at 50%, below the 100% requested by the telcos, yet it still represented a substantial affordability shock for low-income users, with limited evidence of accompanying consumer-protection or subsidy measures.[5]

Notably, the 2024 Londa report's warning of an impending tariff hike materialised in early 2025, reinforcing concerns about affordability. While regulatory intervention moderated the increase, and Nigeria's internet remains relatively cheap compared to many countries on the continent, affordability pressures are still deepening for many users.[6] Compounding this financial barrier is the uneven network distribution; as previously noted, the continued reliance on legacy 2G networks continues to limit meaningful access and the full enjoyment of rights online. However, in a positive step for consumer protection against financial friction, the NCC collaborated with the Central Bank of Nigeria (CBN) to facilitate refunds exceeding NGN10 billion, approximately US$739 000 000, to subscribers for failed airtime and data recharge transactions.[7]

In terms of disruptions, no government-ordered shutdowns or throttling were documented; rather, apart from a

2. Adeyemi Adepetun, "Nigeria's active telephone users hit 179.6m as data consumption surges," The Guardian Nigeria (February 4, 2026). Available at: https://guardian.ng/news/nigerias-active-telephone-users-hit-179-6m-as-data-consumption-surges/
3. ITPulse, "Nigeria: Subscribers favour 4G as 2G and 3G continue to lose share," ITPulse (January 6, 2026). Available at: https://itpulse.com.ng/nigeria-subscribers-favour-4g-as-2g-and-3g-continue-to-lose-share/
4. Adepetun, "Nigeria's active telephone users hit 179.6m," The Guardian Nigeria. (See Footnote 2).
5. The Cable, "AT A GLANCE: 50% telecom tariff hike, 15% port charge levies adjusted, introduced under Tinubu's administration", (2025) https://www.thecable.ng/at-a-glance-50-telecom-tariff-hike-15-port-charges-levies-adjusted-introduced-under-tinubus-administration/ (Accessed December 03, 2025)
6. TechNext "50% data hike: How Nigeria's internet prices compare against 7 African countries" (2025) < https://technext24.com/2025/02/18/nigerias-internet-costs-and-7-countries/> (Accessed January 11,2025)
7. Adeyemi Adepetun, "NCC removes 450 illegal signal boosters, reassigns spectrum," The Guardian Nigeria (January 30, 2026). Available at: https://guardian.ng/business-services/ncc-removes-450-illegal-signal-boosters-reassigns-spectrum/

disruption that affected Zamfara state in Nigeria but could not be ascertained as government-ordered,[8] other disruptions stemmed from fibre cuts, power outages and other infrastructure failures, underscoring structural weaknesses in network resilience,[9] driving sustained advocacy throughout 2025 for the strict enforcement of Critical National Information Infrastructure (CNII) protections to treat telecom assets as protected national security infrastructure.

Online Freedom of Expression and Access to Information (Indicator 2, 3, 4, 5)

In 2025, Nigeria's online freedom of expression environment remained fragile despite positive gestures by statutory bodies such as the National Human Rights Commission issuing an advisory reaffirming the constitutional right to free expression, which served as a soft accountability mechanism rather than an enforceable restraint. In effect, some rights exist in law and policy but are enforced inconsistently. This fragility is further shaped by provisions in the Cybercrime Act, the Nigerian Broadcasting Code, state-level criminal defamation statutes, and ambiguous "false information" provisions that fall short of international human rights standards. The rights impact is systemic; although constitutionally protected, online speech is restricted through overlapping laws, allowing authorities to use whichever tool is most convenient. This is evident from Nigeria's global ranking of 122 out of 180 on the 2025 Reporters without Borders Press Freedom Index.[10]

Censorship and content removal requests continued through opaque mechanisms. Google's transparency data for the first half of 2025 shows six takedown requests via court orders, two requests from government officials, and one from the police, with compliance ranging from 50% to 100%.[11] Furthermore, Meta has now published its government data requests report for the first half of 2025, shedding some light on state interactions with the platform.[12] However, TikTok had not published its updated 2025 transparency report at the time of review. Despite Meta's recent disclosure, the broader transparency gap across certain platforms continues to limit public accountability and makes it harder to assess the true scale of content restriction.

More concerning for rights protection, however, is the shift from formal legal restrictions to informal state pressure, which operates outside judicial oversight and undermines transparency and due process safeguards required under Principles 22 and 38 of the Declaration, as illustrated by the Department of State Services (DSS) publicly flagging posts by Omoyele Sowore, a digital publisher, activist and politician, themselves[13] and urging platforms to remove them, and the banning of musician Eedris Abdulkareem's protest song.[14] The year has also seen a pattern of arrests at the state level, which often escape the national spotlight. In Mohammed Abubakar Isah's case in Niger State, police arrested and arraigned him in October 2025 for a social media post criticising the Governor.[15] Similarly, in Jigawa State, Abba Mu'azu Abiyos was remanded in prison for criticising a local government empowerment programme.[16] 2025 also saw schools and smaller state agencies adopting punitive measures

8. Access Now and the #KeepItOn Coalition. "Authorities in Nigeria must reconnect people in Zamfara, North West Nigeria now." Access Now Press Release. Available at: https://www.accessnow.org/press-release/keepiton-authorities-in-nigeria-must-reconnect-people-in-zamfara-north-now/
9. Intelpoint " Fibre cuts caused 52% of mobile network outages in Nigeria between April and July 2025" (2025), https://intelpoint.co/insights/fibre-cuts-caused-52-of-mobile-network-outages-in-nigeria-between-april-and-july-2025/ (Accessed October 25 2025)
10. Reporters without Borders. "RSF World Press Freedom Index 2025: economic fragility a leading threat to press freedom" (2025), https://rsf.org/en/rsf-world-press-freedom-index-2025-economic-fragility-leading-threat-press-freedom (Accessed December 2nd 2025)
11. Google Transparency Report. "Government requests to remove content: Nigeria (January – June 2025)." Available at: https://transparencyreport.google.com/government-removals/by-country/NG
12. Meta Transparency Center, "Government Data Requests: Nigeria" (H1 2025). Available at: https://transparency.meta.com/reports/government-data-requests/country/NG/
13. PRNigeria, "DSS Demands Retraction, Apology from Sowore Over Comments on Tinubu " (2025). https://prnigeria.com/2025/09/07/dss-demands-retrac tion-apology/ (Accessed Novermber 30 2025)
14. https://www.vanguardngr.com/2025/05/nigeria-and-the-eclipse-of-press-freedom/ (Accessed (December 03 2025)
15. Premium Times, "Police arrest student activist days after criticising Niger governor over insecurity, propaganda" (2025) https://www.premiumtimesng.com/regional/north-central/830487-police-arrest-student-activist-days-after-criticising-niger-governor-over-insecurity-propaganda.html(Accessed Decembder 4 2025)
16. The Whistler, "Amnesty International Condemns Arrest Of Activist For Criticising LG Chairman" (2025) https://thewhistler.ng/amnesty-international-condemns-arrest-of-activist-for-criticising-lg-chairman/ (Accessed Novermber 30 2025)

against online criticism, including reprimanding university students who questioned the First Lady,[17] and a National Youth Service Corp (NYSC) member[18] who criticised governance and was subsequently denied her service certificate. The cumulative effect of these developments has contributed to a climate of self-censorship, particularly among journalists, human rights defenders, and students who increasingly moderate their online expression out of fear of reprisal, justifying the country's low compliance score under Principle 20 on protection from arbitrary arrest and harassment.[19]

Overall, these developments show not only restrictions on speech but a broader governance model of deterrence: state and quasi-state actors deploy legal threats, administrative sanctions, and platform pressure to regulate dissent. This undermines constitutional guarantees of expression and narrows civic space, particularly at state and institutional levels where accountability is weakest.

Access to Information

The Freedom of Information Act (FOIA) in Nigeria remains in force, yet journalists continue to report significant challenges in accessing public information despite the law's guarantees.[20] In encouraging news, however, the Supreme Court has delivered a landmark judgment after an 11-year legal battle, decisively affirming the validity of the FOIA and its applicability to all arms and levels of government.[21]

17. The Whistler, "Nursing Student Video Queried Over Viral Video On First Lady Remi Tinubu" (2025) https://thewhistler.ng/nursing-student-queried-over-viral-video-on-first-lady-remi-tinubu/ (Accessed December 1 2025)
18. Premium Times, "Why corps member Rayes discharge certificate was witheld - NYSC" (2025) https://www.premiumtimesng.com/news/top-news/813307-why-corps-member-rayes-discharge-certificate-was-withheld-nysc.html (Accessed December 1 2025)
19. Human Angle Media, "Strangled in silence: The Unseen Forces Stifling Nigeria's Press Freedom" (2025) https://humanglemedia.com/strangled-in-silence-the-unseen-forces-stifling-nigerias-press-freedom/ (Accessed November 30 2025)
20. News Agency Of Nigeria, "FOI Act: How journalists struggle to access public information in Kwara" (2025) https://nannews.ng/2025/06/03/foi-act-how-journalists-struggle-to-access-public-information-in-kwara/ (Accessed august 05 2025)
21. Premium Times, "Freedom of Information (FOI) Act applicable to 36 states, Supreme Court rules" (2025) https://www.premiumtimesng.com/news/787268-freedom-of-information-foi-act-applicable-to-36-states-supreme-court-rules.html (Accessed August 05 2025)

This ruling represents a major victory for transparency, accountability, and press freedom in Nigeria. However, its practical impact will depend on proactive implementation by Ministries, Departments and Agencies (MDAs) and enforcement mechanisms for non-compliance.

Data Protection And Cybersecurity

Nigeria's data protection landscape continued to evolve in 2025 under the Nigeria Data Protection Act (NDPA) 2023, which remains the country's primary privacy legislation to date and its accompanying Authority. The Commission strengthened compliance mechanisms first through the General Application and Implementation Directive (GAID), which took effect in September 2025,[22] and by publishing a public list of 789 non-compliant organisations asking them to comply with the GAID within a short timeframe,[23] signalling a shift toward more active regulatory oversight. These developments indicate that privacy is increasingly being treated as an enforceable right in Nigeria, with the regulator moving toward deterrence-driven accountability. Still, persistent breaches and non-compliance by public institutions undermine regulatory credibility and public trust. Moreover, the legitimacy of this shift will depend on consistent due process, clear enforcement standards, and stronger public awareness of data subject rights.

Despite these developments, persistent and recurring personal data leaks of Nigerian accounts are reported, highlighting the structural weakness of the system.[24] Nigerian government institutions were also reported to flaunt directives by the Presidency to comply with the Nigerian Data Protection Act, revealing weak internal accountability and reinforcing concerns that the state itself remains a leading privacy violator. Compounding into a pattern of breaches previously highlighted

22. Law Pavilion, "NDP Act 2023 GAID 2025: A comprehensive Guide to Nigeria's New Data Protection Landscape" (2025) https://lawpavilion.com/blog/ndp-act-2023-gaid-2025-a-comprehensive-guide-to-nigerias-new-data-protection-landscape/ (Accessed December 01 2025)
23. DNL, "NDPC Publishes List of 789 Non Compliant Banks, Insurance Firms; Gives 21 Days to Comply" (2025)
24. https://dnllegalandstyle.com/dnl/ndpc-publishes-list-of-789-non-compliant-banks-insurance-firms-gives-21-days-to-comply/ (Accessed December 03 2025)

in the 2024 Londa report, this indicates a system in which laws and policy architecture expand faster than accountability and enforcement capacity, with the State itself possibly among the weakest duty-bearers, undermining the right to privacy and public trust in the NDPA regime.

The 2021 National Cybersecurity Policy and Strategy (NCPS 2021) and the Cybercrimes Act 2015 (amended in 2024) currently form the core of Nigeria's cybersecurity and cybercrime governance framework. The Nigerian Senate, however, has proposed expanding this framework by introducing a dedicated Cybersecurity Act, rather than relying solely on legislation focused on cybercrime. To advance this effort, the Senate has already hosted two consultative engagements with stakeholders.[25]

Following these developments, Nigeria proceeded to sign the United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Electronic Evidence of Serious Crimes in Hanoi in October 2025.

Nigeria's move toward a dedicated Cybersecurity Act, alongside its signing of the UN Convention against Cybercrime in Hanoi in October 2025, signals a shift from a narrow cybercrime framework to broader cybersecurity governance, with the potential to improve technical resilience, close systemic vulnerabilities, and strengthen international cooperation on electronic evidence. In principle, these developments could enhance protection for Nigerians, particularly given recurrent data breaches and weak institutional safeguards. However, Nigeria's track record of misusing cyber-related laws to restrict civic space means these reforms do not automatically guarantee the protection of rights. Without clear safeguards grounded in legality, necessity and proportionality, independent oversight, and strong privacy and due process guarantees, expanded cybersecurity powers could deepen surveillance, enable political targeting, and further chill online expression.

25. IT edge news, "Data breaches: 152k Nigerian Accounts leaked in 2025 so far, study reports" (2025) https://www.itedgenews.africa/data-breaches-152k-nigerian-accounts-leaked-in-2025-so-far-study-reports/ (Accessed December 03 2025)enate committee on ICT and Cybersecurity,"Senate Legislative-Stakeholders' Summit on ICT and Cybersecurity 2025" (2025) <https://ict.cybersecurity.senate.gov.ng/civicrm/event/info?id=1&reset=1> (Accessed December 19 2025)

Privacy and Surveillance

In 2025, Nigeria's privacy and surveillance landscape remains largely unchanged, characterised by a patchwork of constitutional guarantees and sector-specific statutes rather than a unified surveillance governance framework. This fragmentation weakens the rule-of-law test for surveillance by reducing clarity on who can intercept communications, under what conditions, and with what oversight. The primary legal protection for privacy is contained in Section 37 of the 1999 Constitution, which guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. This constitutional safeguard is supported by several statutory instruments, including the Nigeria Data Protection Act (NDPA) 2023, the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, the Nigerian Communications Act 2003, the Terrorism (Prevention and Prohibition) Act 2022, and regulatory frameworks such as the Lawful Interception of Communications Regulations. The combined effect is a surveillance architecture that is security-heavy and light on rights, failing to meet legality, necessity, and proportionality standards under Principle 41.

As with previous years, reports indicate that the Nigerian government and associated security sectors continue to invest heavily in surveillance technologies without corresponding improvements in transparency, oversight, or accountability. On November 25 2025, UrSafe signed a memorandum of understanding with Klass Security, a company providing services to agencies including the Nigerian Ports Authority, Nigerian Maritime Administration and Safety Agency (NIMASA), and APM Terminals at Onne Port in Rivers State. Under this agreement, UrSafe will supply drone surveillance technology to augment Klass Security's existing workforce of 150 security personnel.[26] In addition to drone deployment, a new tender was announced for the procurement of an Artificial Intelligence-powered surveillance system for the Corporate Affairs Commission, signalling Nigeria's continued move toward automated monitoring systems capable of large-scale, real-time

26. Techcabal, "Can AI and drones protect Nigeria's school children? UrSafe thinks so" (2025) https://techcabal.com/2025/11/28/can-ai-and-drones-keep-nigerian-schools-safe-ursafe-thinks-so/#:~:text=When%20agencies%20procure%20entire%20fleets,initial%20assessment%20and%20development%20phase.%E2%80%9D (Accessed December 04, 2025)

data analysis.[27] In line with this, the National Identity Management Commission (NIMC) is also seeking a consulting firm to strengthen the security and resilience of its digital identity infrastructure,[28] an acknowledgement of vulnerabilities within a system that already holds sensitive biometric and demographic data of millions of Nigerians.

Despite constitutional and statutory protections for privacy, surveillance practice in 2025 is increasingly diverging from a rights-based approach. Nigeria continues to expand surveillance capacity through drones, AI-powered monitoring systems, and stronger digital identity infrastructure, without corresponding improvements in public transparency, judicial oversight, or accountability, all of which risk normalising intrusive monitoring.

Developments in ICT and Emerging Technologies

In 2024, Nigeria experienced accelerated momentum in its artificial intelligence ecosystem following the launch of the country's new National AI Strategy.[29] This renewed focus on AI set the stage for significant developments in 2025.

A major milestone came with the launch of N-ATLAS, an open-source language model built specifically for Yoruba, Hausa, Igbo, and Nigerian-accented English.[30] Developed through a collaboration between the Federal Government and Lagos-based startup Awarri, N-ATLAS represents a significant step for linguistic inclusion and localisation in AI systems.

27. Nigeria Tenders, "Procurement Of Artificial Intelligence-Powered Surveillance System Software" (2025) https://www.nigeriatenders.com/tender/procurement-of-artificial-intelligence-powered-surveillance-system-software-6e6000b.php#:~:text=Tender%20for%20Procurement%20Of%20Artificial%20Intelligence%2DPowered%20Surveillance,Deadline:%2027%20Mar%202025.%20Ref%20No:%20115736587. (Accessed December 04, 2025)
28. National Identity Management Commission (NIMC), "Request for Expression of Interest (REOI) Engagement of Consultant to Enhance NIMS Security and Resilience," Hometown Development Initiative (HDI). Available at: https://www.publicprocurement.ng/national-identity-management-commission-nimc-request-for-expression-of-interest-reoi-engagement-of-consultant-to-enhance-nims-security-and-resilience/
29. Ncair nitda, "National Artificial Intelligence Strategy" (2025) https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf (Accessed December 04, 2025)
30. https://www.google.com/search?q=https://techpoint.africa/2024/10/29/nigeria-n-atlas-open-source-language-model/ (Accessed December 04, 2025)

Legislative interest also grew. The Senate advanced a Bill to establish an Artificial Intelligence and Innovation Centre in Ekiti State, signalling growing government interest in building institutional capacity for AI development.[31]

In parallel, Nigeria introduced the National Digital Economy and e-Governance Bill 2025, considered Africa's first comprehensive legislative attempt to govern digital transformation across government sectors.[32] It seeks to promote the adoption of digital technologies across all sectors by strengthening legal recognition for electronic communications, records, and contracts. Importantly, it also aims to ensure ethical, transparent, and risk-based governance of emerging technologies, including Artificial Intelligence. This Bill has strong value for digital transformation and consumer protection. Still, in its current form, it also concentrates broad power in the regulator, introduces punitive enforcement linked to vague directives, and creates a supremacy regime that could weaken checks and balances. The Bill is therefore rights-positive in intent but rights-risky in structure, unless strengthened with clear safeguards, oversight mechanisms, and limits on regulatory discretion.

Together, these developments reflect Nigeria's continued efforts in 2025 to shape an AI-ready ecosystem through innovation, policy, and legislation.

Digital Inclusion

In 2025, progress has been recorded with the Child Online Access Protection Bill 2023, which has now passed its third reading in the House of Representatives and been transmitted to the Senate for further consideration.[33] The Bill represents one of Nigeria's most significant legislative efforts to establish a rights-based, structured framework for protecting children online, including obligations on platforms, regulators, and caregivers.

31. National Assembly Library Trustfund, "Senate Advances Bill to Establish Artificial Intelligence and Innovation Centre in Ekiti State" (2025) https://naltf.gov.ng/senate-advances-bill-to-establish-artificial-intelligence-and-innovation-centre-in-ekiti-state/ (Accessed December 04, 2025)
32. Federal Ministry Of Communications, Innovation and Digital Economy, "Driving Economic Growth Through Digital Technology and Innovation" (2025) https://fmcide.gov.ng/public-hearing-on-national-digital-economy-and-e-governance-bill-2025-holds-in-abuja/#:~:text=The%20National%20Digital%20Economy%20and%20e%2DGovernance%20Bill%202025%2C%20which,Tinubu's%20Renewed%20Hope%20Agenda. (Accessed December 04, 2025)

Millions of Nigerians with disabilities continue to face barriers to digital inclusion due to poor design, limited accessibility features, and the high cost of assistive technologies. NITDA has acknowledged that the National Digital Literacy Framework did not adequately include persons with disabilities and has pledged to revise implementation to address these gaps as part of Nigeria's broader goal of achieving 95% digital literacy by 2030. [34] This recognition is a great entry point for reform and a potential for mainstreaming disability inclusion, but measurable outcomes will depend on whether revised frameworks result in accessible design standards, budgetary allocations, and enforcement.

In parallel, other MDAs such as the Federal Ministry of Health have intensified efforts to expand access to assistive technologies. Recent initiatives aim to support over 30 million Nigerians living with disabilities, improving the availability of devices, training, and support systems necessary for meaningful digital participation.[35]

Universal Service Fund (USF)

Nigeria's Universal Service Provision Fund (USPF) remains established under the Nigerian Communications Act 2003 and is administered by the Nigerian Communications Commission (NCC) through a Universal Service Provision Board and Secretariat within the Commission.

The Fund has recently released a 2023–2027 Strategic Management Plan (SMP) that frames the mission as "to facilitate universal service and access to ICT, through partnerships to stimulate development in rural, unserved and underserved communities".[36]

The SMP provides a detailed picture of USPF programmes and projects. The three core focus areas introduced in the plan are connectivity infrastructure, access and end-user projects, ICT for development (ICT4D) and innovation. The most recent full-fledged report is from 2022, where the 2022 Annual Report financial statements give a recent snapshot of the Fund's scale, notably the total revenue for 2022 totals NGN11.51 billion (approximately US$25 million), largely from a NGN 10 billion (approx. US$21.7 million) contribution from NCC, plus interest income and transfers from accumulated funds and total expenditure in 2022 standing at NGN10.17 billion (approximately US$22.1 million). Total assets were reported at the end of 2022 at NGN20.95 billion (approximately US$45.4 million), mainly cash and receivables.[37][38] Reliance on outdated reporting during the 2025 review period constitutes a significant transparency and accountability gap under Principle 37.

An industry-focused Stakeholders' Engagement session was hosted in 2025, and a report was released by the Fund. The engagement, themed "Fostering Connectivity and Access in Unserved and Underserved Communities: Collaborating for Sustainable Growth", aimed to strengthen collaboration among relevant stakeholders in the telecommunications sector to develop sustainable strategies for expanding connectivity and enhancing digital inclusion in Nigeria's underserved and unserved communities.[39]

Although the 2025 industry-focused Stakeholders' Engagement report is the most recent publicly available publication, it offers limited value for delivery and impact assessment because it does not clearly outline specific actions taken, outcomes achieved, implementation timelines, or follow-up measures arising from the engagement. Overall, the USPF demonstrates strong policy intent and planning, but insufficient public reporting prevents a credible evaluation of delivery and impact.

33. Vanguard, " Reps advance bill to protect children against online violence, abuse" (2025) https://www.vanguardngr.com/2025/12/reps-advance-bill-to-protect-children-against-online-violence-abuse/ (Accessed December 03,2025)
34. Premium Times, "NITDA to support digital inclusion for Persons with special needs" (2025) https://www.premiumtimesng.com/health/health-news/799202-itda-to-support-digital-inclusion-for-persons-with-special-needs.html (Accessed december 4 2025)
35. Federal Ministry Of Health and Social Welfare, " https://health.gov.ng/fg-stakeholders-leads-drive-to-expand-assistive-technology-access-for-30-million-nigerians-living-with-disabilities/ (Accessed Decemer 04, 2025)
36. Universal Service Provision Fund, "Strategic Management plan 2023-2027" (2024) https://www.uspf.gov.ng/custom_files/Documents/RevisedSMP20232027.pdf (Accessed Decemer 04, 2025)
37. Universal Service Provision Fund, "Annual Report 2022" (2022) https://www.uspf.gov.ng/custom_files/Documents/AnnualReport2022.pdf (Accessed Decemer 04, 2025)
38. USD equivalents are calculated using the Central Bank of Nigeria (CBN) official exchange rate applicable at the end of the 2022 reporting period (approx. ₦461/US$1) to accurately reflect the historical value of the fund.
39. Universal Service Provision Fund, " REPORT ON THE INDUSTRY-FOCUSED STAKEHOLDERS' ENGAGEMENT SESSION OF THE UNIVERSAL SERVICE PROVISION FUND (USPF) - 2025" (2025) https://www.uspf.gov.ng/images/files-temp/Report%20on%20the%20Industry-Focused%20Stakeholders%20Engagement%20Session%20of%20the%20USPF%202025.pdf (Accessed Decemer 04, 2025)

Conclusion

Nigeria's digital rights landscape in 2025 presents a complex dichotomy between progressive policy development and persistent enforcement deficits. While the country has made measurable strides in broadband penetration, artificial intelligence governance, and legislative frameworks for data privacy and child online protection, these gains are consistently undermined by structural and institutional realities. The continued reliance on legacy 2G networks, compounded by rising tariffs, widened the digital divide and limited meaningful access for underserved populations. Furthermore, the online civic space remains heavily contested, as state and quasi-state actors increasingly bypass formal judicial processes. The reliance on informal state pressure, arbitrary arrests of online critics at the sub-national level, overlapping cyber laws, and opaque surveillance technologies continues to stifle dissent and foster a pervasive climate of self-censorship. Earning a moderate compliance score of 35/60, down from 36 in the previous year, Nigeria's trajectory indicates that while the foundational frameworks for a robust digital economy are largely in place, realising this potential requires an urgent pivot from mere regulatory expansion to genuine, rights-respecting enforcement, transparent institutional accountability, and the consistent protection of constitutional freedoms.

Recommendations

The Government should:

- Review the implementation of the National Broadband Plan and release a report on achievements and a plan for reaching new goals, based on lessons from the implementation of the last plan.
- Strengthen the governance, transparency, and monitoring of the Universal Service Provision Fund (USPF) by publishing annual audited reports, disaggregated project data, and independent impact evaluations aligned with access-gap assessments.
- Publish specific disaggregated data on USPF-funded projects (location, cost, beneficiaries, status) and align future funding with connectivity gaps revealed in access-gap studies.
- Operationalise the Presidency's directive on implementing the Nigerian Data Protection Act by government agencies.
- Issue clear directives to security agencies and state institutions prohibiting the use of criminal law to punish online criticism, particularly against journalists, HRDs, students, and critics on social media.
- Implement the Supreme Court judgment on FOIA by issuing circulars to all ministries, departments and agencies (MDAs) and establishing sanctions for non-compliance with access-to-information obligations.
- Adequately resource and guarantee the independence of the Nigeria Data Protection Commission (NDPC) so it can enforce obligations against both public and private entities.
- In expanding the cybersecurity framework (including any new Cybersecurity Act and implementation of the UN Cybercrime Convention), embed strong safeguards for human rights, judicial oversight, and clear limits on data retention and interception.
- Ensure that deployment of surveillance technologies (including drones and AI-powered systems) is subject to mandatory human rights impact assessments, public procurement transparency and parliamentary and judicial oversight.

The Media should:

- Increase in-depth reporting on digital rights issues, including tariff hikes, connectivity gaps, USPF performance, online censorship, data breaches, and the human impact of surveillance technologies.
- Continue to systematically track and report cases of arrests, intimidation and disciplinary sanctions arising from online speech, especially at state and local levels where incidents are often overlooked.
- Use explainer pieces, talk shows and data visualisations to demystify complex issues such as the NDPA, AI governance, cybersecurity, child online safety and digital inclusion for the general public.

Civil Society Organisations should:

- Continuously document cases of online censorship, arrests, intimidation, data breaches, surveillance deployments and connectivity barriers, producing periodic public briefings and shadow reports.
- Engage the legislature and relevant committees to push for rights-respecting reforms to the various laws, with a focus on digital rights and digital inclusion.
- Monitor USPF implementation, analyse budget and project data, and advocate for community-driven priorities in fund allocation, especially for rural, low-income and marginalised communities.
- Pursue strategic litigation to Challenge abuses on freedom of expression online, enforce FOIA compliance and Data privacy obligations

The Private Sector should:

- Regularly publish comprehensive transparency reports detailing government requests for user data, content takedowns, and network disruptions. Platforms must insist on formal judicial orders and push back against informal or extralegal state pressure for content moderation.
- Strengthen internal cybersecurity measures to prevent recurring data breaches and ensure strict compliance with the Nigeria Data Protection Act (NDPA) and the newly enforced General Application and Implementation Directive (GAID).
- Prioritise the expansion of 4G and 5G infrastructure in underserved and rural areas to phase out reliance on legacy 2G networks, while exploring pro-consumer data packages and models to ease the burden of recent tariff hikes on low-income users.
- Ensure that the design and deployment of new technologies, including AI systems and surveillance tools, are subject to rigorous human rights impact assessments prior to market introduction or government partnership.

The Score Index

Nigeria, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	3	3	There were no documented government-ordered internet shutdowns or throttling in 2025. While a localised disruption affected Zamfara state, it could not be verified as a state directive. All other network disruptions throughout the year stemmed from infrastructure failures, such as fibre cuts and power outages, rather than deliberate government interference.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	4	4	Nigeria has a robust broadband plan, and the Universal Access and Universal Service Regulations 2007.
False News Criminalisation	P22(2)	3	2	Disinformation is not criminal in Nigeria; however, the Criminal Code Act prohibits “publication of false news with intent to cause fear and alarm to the public” (Section 59)
Sedition Legislation	P22(2)	1	1	The legislation exists
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	There have been various documented arrests of journalists and dissenting voices
Data Protection Legislation.	P42	4	4	There is active legislation (NDPA 2023) and an accompanying regulatory agency. In 2025, the regulator demonstrated a shift toward active enforcement (e.g., issuing the GAID and publishing a list of 789 non-compliant organizations).
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	4	3	While documented takedown requests to internet intermediaries (such as Google) appear numerically low, the true scale of state-led content removal remains obscured by opaque legal mechanisms and incomplete transparency reporting across all major platforms
Invasion of Privacy of	P41	3	3	Demonstrated pattern of surveillance

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Communications				Act (2022), but broad "national security" provisions and limited independent oversight of intelligence agencies remain. Smart-city surveillance expansion lacks a dedicated regulatory framework.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	2	3	Reports of Government not adhering to the legal requests under the Freedom of Information Act by journalists, but the Judgement in favour of the Act is a significant improvement
AI and Emerging Technologies national strategies	P39(6)	4	4	There is a National AI strategy, a National Centre for Artificial Intelligence and Robotics and a bill for AI regulation
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P39(6)	3	3	A non-binding child online protection policy and strategy exists, and specific legislation has made strides in the nation.
Digital Inclusion	P37(3)	4	4	There is a law focused on PWDs, and government has indicated interest in improving accessibility.

Total (out of 60):	2024: **36**	2025 **35**

Moderately compliant.

Sierra Leone

Jonette-Ann Matilda O. Greene

Executive Summary

This report is informed by information from diverse sources, reports from media rights organisations, government institutions' websites, articles, and press statements. The country report is assessed using the TheScore Index by Paradigm Initiative, which evaluates compliance with the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information. It examines key thematic areas, including internet access and digital inclusion; online freedom of expression and access to information; data protection and cybersecurity; privacy and surveillance; developments in ICT and Emerging Technologies; and the Universal Service Fund.

The findings highlight notable progress in stakeholder engagement on emerging legislation, such as the Data Protection Bill, amendments to the Right to Access Information Act, and the expansion of internet penetration supported by national digital policies. However, the analysis also identifies persistent challenges, including the misuse of the 2021 Cybersecurity and Crime Act, which restricts online expression; recurring internet disruptions during politically sensitive periods; growing privacy concerns related to biometric systems; and deep inequalities in digital access for rural populations, women, and low-income groups.

To strengthen digital rights protection, the report recommended amending provisions that limit citizens' rights in cybersecurity laws, adopting and enforcing a comprehensive data protection framework, increasing transparency around state surveillance, expanding affordable connectivity, and prioritising inclusive digital literacy initiatives.



Introduction

Since 2016, Sierra Leone has made notable progress in strengthening digital rights within the broader context of democratic reforms. One of the most significant milestones was the repeal of Part V of the 1965 Public Order Act in 2020, which decriminalised libel and seditious libel. This reform contributed to a substantial improvement in the country's press freedom environment, reflected in its rise in the World Press Freedom Index from 85th in 2019 to around 46th by 2024. Digital connectivity has also expanded, with internet penetration increasing from about 13% in 2018 to over 30% by 2025,[1] supported by initiatives such as the National Digital Development Policy (NDDP). Between 2023 and 2025, there were no internet shutdowns recorded, including during the 2023 elections, indicating a modest progress in internet disruption in the country. There is also improved engagement between government and civil society in policy processes, as seen in more inclusive consultations on emerging digital legislation, as well as in the ongoing development of the Data Protection Bill.[2]

Despite these advances, Sierra Leone continues to face persistent and structural challenges to digital rights. The 2021 Cybersecurity and Crime Act has been frequently used to target online speech, leading to arrests and investigations that have contributed to a climate of self-censorship among journalists, bloggers, and human rights defenders. The digital divide remains a significant barrier to inclusive digital transformation, with rural communities, women, and low-income groups disproportionately excluded from affordable, reliable internet access.

Furthermore, the rapid expansion of biometric ID systems and digital surveillance capabilities has heightened concerns about privacy and data protection in the absence of a comprehensive legal framework. Although ongoing policy initiatives signal a commitment to strengthening digital governance, gaps in enforcement, limited institutional capacity, and socio-economic inequalities continue to limit Sierra Leone's alignment with regional and international human rights standards, including the African Charter on Human and Peoples' Rights (ACHPR).

Internet Access

Internet connectivity is improving slowly but with notable transformation. Early 2025, 1.80 million people used the Internet, which increased the online penetration to 20.7%, and 1.15 million (13.2%) were social media users, mobile phones are the primary means of access yet an estimated 79% remains offline due to low effective internet use and multiple SIM ownership.[3] A strong urban and rural divide persist, with 45% of the population living in urban centres, mainly Freetown and provincial capitals, benefiting from better coverage, faster speeds, multiple ISPs and fixed broadband options such as fibre or fixed wireless,[4] while 55% in rural areas rely on 2G networks that support only limited browsing or messaging.[5] The 4G population coverage rose to 79% by 2025 (from about 70%),[6] improving access in semi-rural areas, and operators like Africell and Orange continue network upgrades, including Orange's 5G pilot Freetown's central business district launched in September 2023.[7]

Affordability

The cost of access is high, and mobile data prices are roughly five times higher than the UN's recommended affordability threshold. The cheapest smartphone costs about four months of the average salary around Le800 (approximately US$33).[8] In late 2022, Sierra Leone's NATCOM announced a nationwide mobile data increase of over 150%,[9] triggering

1. Ministry of Information and Civic Education https://moice.gov.sl/moice-press-conference-tuesday- 21st-january-2025/ (accessed on 12 January 2026).
2. Ministry of Information and Civic Education https://moice.gov.sl/moice-concludes-final-national-validation-of-the-data-protection-and-right-to-access-information-bill-2025 (accessed on 12 January 2026).
3. DataReportal https://datareportal.com/reports/digital-2025-sierra leone?ts2.tech#:~:text=,include%20access%20to%20the%20internet (accessed on 6 November 2025).
4. Sierra Leone National Broadband Strategy 2023-2028 https://mocti.gov.sl/wp-content/uploads/2024/12/National-Broadband-Strategy. (accessed on 6 November 2025).
5. Internet Society Pulse https://pulse.internetsociety.org/en/reports/sl/ (accessed on 6 November 2025).
6. As above, n-5.
7. The Calabash Newspaper "Orange Sierra Leone Launches 1st 5G Trial Technology in Freetown" (2023) https://thecalaba shnewspaper.com/orange-sierra-leone-launches-1st-5g-trial-technology-in-freetown/ (accessed on 29 October 2025).
8. Broadband Commission for Sustainable Development https://www.broadbandcommission.org/advocacy-targets/2-affordability/ (accessed on 5 November 2025).
9. National Communications Authority https://www.natca.gov.sl/wp-content/uploads/2023/11/Public-Notice-23.pdf (accessed on 5 November 2025).

public backlash and a temporary suspension,[10] yet prices still rose in 2023, further burdening users. As of November 2023, Africell charges Le 2 (approx. US$0.08) for 100 MB (one day), Le 20 (approx. US$0.81) for a 1 GB monthly, Le 120 (approx. US$4.8) for 6 GB, and Le 300 (approx. US$12) for 15 GB,[11] with Orange offering similar bundles (e.g., 2.6 GB for around Le 52, roughly US$2)[12]. Although these prices appear low per GB, they are unaffordable in a very low-income country like Sierra Leone.[13] Despite these gains, mobile internet remains a luxury for many Sierra Leoneans, who often limit use to low-data services such as Facebook Basics and WhatsApp.

Digital connectivity and network infrastructure has made gradual progress, with expanded coverage and improved reliability, particularly in provincial areas, under the government's Digital Transformation Programme. The Programme extended the national fiber-optic backbone from eight to 14 districts and increased mobile network sites from 798 in 2019 to 1,405 in 2025.[14] Performance improved in 2023, with Ookla reporting a 52% increase in internet speeds, and with average downloads of about 17.63 Mbps for both mobile and fixed broadband.[15] In 2024–2025, Orange and Africell showed mixed results average speeds of 16.40 Mbps (Orange) and 12.15 Mbps (Africell) in January 2024,[16] rising to 16.95 Mbps for Orange but falling to 7.57 Mbps for Africell by January 2025.[17]

The digital divide is both a coverage gap and an affordability gap. Even where network coverage exists outside urban areas, many rural residents cannot afford smartphones or data plans. By early 2025, rural internet penetration remained in the single digits, while urban penetration was significantly higher due to better network quality and higher incomes.[18] Addressing urban–rural disparities remains a key policy challenge, as reflected in government strategies and donor-supported rural connectivity programs.[19]

Findings from the 2021 Sierra Leone Demographic and Health Survey (DHS) Analytical Studies No. 83 revealed that only 12% of women and 21% of men used the internet at least once per week, while 43% of women and 64% of men owned a mobile phone.[20] The rural and urban divide is particularly stark; 24% of rural women owned mobile phones compared to 65% of urban women, and 50% of rural men compared to 81% of urban men.[21]
Nationally, just 27% of the population has access to mobile internet, and 12% to broadband internet as of 2021, meaning internet users accounted for less than one-third of the total population.[22] These figures highlight persistent inequalities in digital access and the urgent need for inclusive policies to address both affordability and coverage gaps.

Internet disruptions

In March 2018, authorities shut down the Internet and all mobile communication services following the closure of polling stations during the Presidential runoff, reportedly to prevent result sharing.[23] In August 2022, a nationwide internet shutdown occurred amid protests over the high cost of living and food shortages,[24]

10. Sierraloaded 'NATCOM Suspends New Internet Data Prices' (2022) https://sierraloaded.sl/news/natcom-suspends-new-internet-data-prices/ (accessed on 2 November 2025).
11. Sierraloaded 'Data Prices Surge in Sierra Leone as Mobile Companies Secure Government Agreement' https://sierraloaded .sl/news/data-prices-surge-sierra-leone-mobile-companies-government-agreement/ (accessed on November 2025).
12. As above, n – 14.
13. African Future with AUDA-NEPAD https://futures.issafrica.org/geographic/countries/sierra-leone/ (accessed on 7 November 2025).
14. Ministry of Information and Communications 'National Digital Transformation Programme Progress Report' (2025) https://mocti.gov.sl/wp-content/uploads/2025/08/Lite-2025-Sierra-Leone-Innovates-Digital-Government-Summit-Newsletter.pdf
15. Ookla (2024). Speedtest Global Index: Sierra Leone Internet Performance Data. https://www.speedtest.net/global-index (accessed on 29 October 2025).
16. SpeedChecker Insights (2024). Mobile Data Speed Report: Sierra Leone https://insights.speed checker.com/africa/sierra-leone/sl-january-2024/ (accessed on 29 October 2025)
17. SpeedChecker Insights (2024). Mobile Data Speed Report: Sierra Leone https://insights.speedchecker.com/africa/sierra-leone/sl-january-2025/ (accessed on 29 October 2025).
18. World Bank (2024). Sierra Leone Digital Economy Diagnostic Report. https://documents.worldbank.org/en/publication/docu ments-reports/documentdetail/185761624271466646/sierra-leone-digital-economy-diagnostic (accessed on 7 November 2025).
19. Ministry of Information & Communications 'National Digital Transformation Strategy (2023–2027)' 2023 https://www.mots. gov.zm/wp-content/uploads/2023/10/National-Digital-Transformation-Strategy.pdf (accessed on 7 November 2025).
20. Statistics Sierra Leone (Stats SL) 'Sierra Leone Demographic and Health Survey (DHS) Analytical Studies No. 83' 2021 https://www.statistics.sl/index.php/sierra-leone-demographic-and-health-survey.html (accessed on 7 November 2025).
21. As above, n – 37.
22. International Telecommunication Union (ITU) 'ICT Development Index and Internet Penetration Statistics' 2023 https://www.itu.int/itu-d/reports/statistics/idi2023/ (accessed on 7 November 2025).
23. ARTICLE 19 'Authorities shut down the internet around protests and elections' https://www.article19.org/reader/global-expression-report-2018-19/regional-overviews/africa-regional-overview/authorities-shut-down-the-internet-around-protests-and-elections/ (accessed on 27 October 2025).
24. CNN 'Internet cut off as protesters shared images of police brutality. CNN investigates' https://edition.cnn.com/videos/world/2022/08/24/sierra-leone-protests-internet-cut-off-pkg-polglase-intl-l dn-vpx.cnn (accessed on 27 October 2025).

coinciding with clashes between protesters and police that resulted in casualties and property damage. While authorities cut access as events unfolded, Zoodlabs Sierra Leone attributed the shutdown to emergency technical maintenance, a claim widely questioned due to its timing.[25]

Between 2023 and 2025, no internet shutdowns were recorded, including during the 2023 elections, indicating modest progress. However, despite the reduced frequency of shutdowns, compliance with the African Charter on the right to information remains weak.[26]

Online Freedom of Expression and Access to Information

Freedom of expression online is increasingly under threat, with arrests of journalists, activists, and bloggers creating a climate of fear. The Constitution of Sierra Leone 1991, Section 25(1),[27] guarantees freedom of expression, including the right to hold opinions and impart information without interference, Section 25(2) permits restrictions in the public interest, provided they are necessary and proportionate, such as Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

The repeal of Part 5 of the Public Order Act 1965 in 2020 marked a significant advancement in upholding online freedom of expression in Sierra Leone, as it removed criminal penalties for defamatory-seditious libel and the publication of false news that had historically been used to suppress dissent and journalism, and was widely welcomed by the media as aligning national law international standards favouring civil remedies over criminal sanctions.[28] However, the progress is tempered by continuing restrictions under the Cyber Security and Crime Act, Section 44 on cyberstalking and cyberbullying, which has been applied to arrest and prosecute social media users for online content deemed abusive or insulting,[29] including expressions critical to the government.

These issues got the attention of the Sierra Leone Association of Journalists (SLAJ), the Media Reform Coordinating Group (MRCG), the Right to Access Information Commission (RAIC), and the Independent Media Commission (IMC), who raised concerns that the Cyber Crime law has infringed on the fundamental right to free speech, and that the law should not be used to suppress dissent, noting its use in intimidation and arrests related to online expression.[30]

The Right to Access Information Act 2013 strengthens transparency by granting citizens the right to information held by public authorities and establishing the Right to Access Information Commission (RAIC) to oversee implementation and handle complaints.[31] The Act is currently under amendment to further strengthen the Commission. Between December 2024 and May 2025, RAIC recorded 92 information requests nationwide, surpassing the previous year's total of under 40. Requests were distributed as follows: Western Region (37, 80% approved); Southern Region (16, 1 denial); Eastern Region (25, 90% approved, 2 pending); and Northern Region (15, 10 successful). These figures reflect growing public awareness and improved compliance, as recognised at the 2025 International Conference of Information Commissioners (ICIC).[32]

The RAIC expanded public engagement through media outreach, including the bi-weekly "RAIC Hour" on SLBC TV,[33] appear

25. Zoodlabs Sierra Leone https://twitter.com/ZoodlabsS/status/15574329535417221 (accessed on 2 November 2025).
26. African Charter on Human and Peoples' Rights, Art 9.
27. The Constitution of Sierra Leone 1991, s 25(1) https://www.sierra-leone.org/Laws/constitution1991.pdf (accessed on 7 November 2025).
28. Media Foundation for West Africa 'Major Boost for Press Freedom as Sierra Leone scarps Criminal Libel Law after 55 Years' 2020 https://mfwa.org/major-boost-for-press-freedom-as-sierra-leone-scraps-criminal-libel-law-after-55-years/ (accessed on 7 November 2025).
29. Sierra Leone State House https://statehouse.gov.sl/sierra-leones-president-julius-maada-bio-signs-cybersecurity-and-crime-law-praises-bipartisan-support-in-parliament/ (accessed on 7 November 2025).
30. Sierraloaded 'SLAJ Raises Concern Over Implementation of Cyber Law' https://sierraloaded.sl/news /slaj-raises-concern-implementation-cyber-law/ (accessed on 7 November 2025).
31. Right to Access Information Act 2013 https://www.sierra-leone.org/Laws/2013-02.pdf (accessed on 1 November 2025).
32. RAIC Sierra Leone Excels in Africa Regional Report at ICIC 2025 in Berlin https://raic.gov.sl/index.php/all-categories-list/press-release/raic-sierra-leone-excels-in-africa-regional-report-at-icic-2025-in-berlin (accessed on 1 November 2025).
33. Right to Access Information Commission 'RAIC Signs MOU with SLBC to Promote Access to Information' https://raic.gov.sl /index.php/all-categories-list/news/raic-signs-mou-with-slbc-to-promote-access-to-information (accessed on 1 November 2025).

ances on AYV, regional outreach visits,[34] and plans for nationwide public lectures at universities. Digitally, the Commission launched an online request platform covering 50 Ministries, Departments, and Agencies (MDAs), enabling simultaneous submission to MDAs and RAIC, with plans for nationwide expansion.

The RAIC maintained strong collaboration with the Ministry of Information and Civic Education on amendments to the Act and the Data Protection Bill. In June 2025, the High Court upheld RAIC's authority by fining the Bank of Sierra Leone Le70,000,000 (approx. US$2,848,418) for non-compliance.[35] The Commission also fined Freetown City Council Le70,000 (approx.US$2,848) following a complaint over failure to respond to an FOI request concerning the Ephraim J. Robinson Municipal School recreation field.[36]

Despite these achievements, key challenges persist. A pervasive culture of secrecy in public institutions continues to hinder transparency. Furthermore, low proactive disclosure remains an issue for 79 institutions engaged last year; only slightly over 50 met complete compliance requirements, and many institutions lack websites or digital platforms for sharing public data.[37] While the RAIC framework broadly aligns with international standards, such as the African Charter on Human and Peoples' Rights, implementation gaps continue to limit its effectiveness.

Censorship and Content Removal

The transparency reports from Facebook documented four government-ordered requests between 2021 and 2023, in 2021 there were three requests; one was done under a legal process, while the other two were requested under emergency disclosure. In 2023, there was one documented government request. In addition, Google

34. Right to Access Information Commission 'RAIC's Regional Offices Join 10th Anniversary Celebration' https://raic.gov.sl /index./all-categories-list/press-release/raics-regional-offices-join-10th-anniversary-celebration (accessed on 1 November 2025).
35. Right to Access Information Commission 'RAIC Secure Legal Victory Over Bank of Sierra Leone' (2025) https://raic.gov. sl/index.php/all-categories-list/press-release/raic-secures-legal-victory-over-bank-of-sierra-leone-in-landmark-freedom-of-information-case (accessed on 1 November 2025).
36. 'RAIC Fines Freetown City Council Le 70.000 for Failing to Release Information' https://raic.gov.sl/index.php/all-categories-list/news/raic-fines-freetown-city-council-le-70-000-for-failing-to-release-information (accessed on 1 November 2025).
37. 'RAIC Engages Stakeholders on Digital Access to Information and Compliance in Makeni' https://raic.gov.sl/index.php/ all-categories-list/press-release/raic-engages-stakeholders-on-digital-access-to-information-and-compliance-in-makeni (accessed on 1 November 2025).

reported one request from the Sierra Leone Police on December 31 2012 seeking the removal of 60 YouTube videos related to violence.[38] Such actions may be justified under the Cybercrime Act 2020 as the law grants broad discretionary powers to restrict content deemed "offensive" or "threatening" without clear safeguards for necessity, proportionality, transparency, or oversight.

Internet disruptions

Self-censorship is widespread among individuals, journalists, and human rights defenders, particularly women journalists, due to fear of arrest, harassment, or reprisals under laws such as the Cybercrime Act. A notable case is that of journalist Umu Thoronka, who was dismissed from the Sierra Leone Broadcasting Corporation (SLBC) in July 2024 after posting a TikTok video showing a woman questioning President Julius Maada Bio about rising living and food costs at a Presidential Town Hall Meeting. SLBC management deemed the video critical of the President.[39]

Following her dismissal, Thoronka reported intimidation, online death threats, and unidentified individuals visiting her home. After complaints to SLAJ, Women in the Media Sierra Leone (WIMSAL), and other bodies yielded no government response, she fled the country. WIMSAL and RFK Human Rights subsequently filed a petition on her behalf before the ECOWAS Community Court of Justice. Incidents such as this have intensified self-censorship among women journalists and activists, creating a chilling effect that undermines constitutional protections and international standards on free expression.[40]

38. Google Transparency Report 'Government requests to remove content – Sierra Leone' https://transparencyreport.google. com/government-removals/overview?hl=en (accessed on 17 November 2025).
39. Forum News Sierra Leone https://forumnews-sl.com/ecowas-court-petition-highlights-the-pervasive-challenges-faced-by-women-journalists-in-west-africa/ (accessed on 4 November 2025).
40. Robert F. Kennedy Human Rights https://www.facebook.com/RFKHumanRights/posts/-case-updatesierra-leonean-journalist-umu-thoronka-endured-years-of-sexual-haras/1229387102567248/ (accessed on November 2025).

Freedom of expression and access to information

Between 2020 and 2025, arrests and prosecutions for online expression occurred sporadically, often under provisions of the Cybercrime Act or legacy laws. In the 2024 World Press Freedom Index, Sierra Leone ranked 64th out of 180 countries (score 64.27), a 10-place drop from 2023,[41] with Reporters Without Borders noting increased political pressure on the media.[42]

Documented cases include:

- Thomas Dixon (June 2024): Subjected to online attacks and threats over commentary on the First Lady; SLAJ condemned the intimidation.[43]
- Joy Bayoh Esq. (June 2024): Arrested for alleged cyberstalking following a Facebook post; released on bail and case dismissed.
- Mayor Yvonne Aki-Sawyerr (October 2025): Publicly threatened with removal from office following remarks criticising government priorities during a radio program.[44]

These cases demonstrate a pattern of selective enforcement and intimidation, reinforcing self-censorship and weakening protections for freedom of expression and access to information in Sierra Leone.

Gendered Disinformation

Gendered disinformation is an increasing concern in Sierra Leone, primarily circulated through social media to target and discourage women in politics and other high-profile professions. This form of disinformation often involves false, exaggerated, or inflammatory content that undermines women's competence and morality, often through sexualisation and psychological harm. A 2022 study by the Sierra Leone Association of Women in Journalism (SLAWIJ) found that 64% of women journalists experienced threats, harassment, or violence, much of it occurring online.[45] In December 2021, rapper Alhaji Amadu Bah (LAJ) posted a Facebook video insulting Radio Democracy Director Asmaa James in response to her station's reporting and issuing a threatening remark. Reporters Without Borders condemned the comments as "obscene, disgraceful, irresponsible and dangerous," using the incident to call for an end to online harassment of journalists in Sierra Leone.[46]

Although Sierra Leone has committed to several international frameworks on gender equality, such as the African Union Convention on Cybersecurity and Personal Data Protection, the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), and adopted national laws and strategies such as the Cybersecurity Act 2021, Data Protection Strategy 2022, National ICT Policy 2011, and National Telecommunications Act 2006, these frameworks remain broad and lack specific provisions addressing the distinct challenges and violations faced by women in the digital space.[47]

Data Protection and Cybersecurity

Sierra Leone does not yet have a comprehensive data protection law. The Data Protection Bill 2025 has completed final national validation and is awaiting passage.[48] In the interim, partial safeguards exist under Article 22 of the 1991 Constitution (right to privacy) and the Telecommunications Act of 2006, which provides limited protection for telecommunications data.

In June 2025, during a national digital policy engagement, the Minister of Information and Civic Education, Chernor Bah, reaffirmed the government's com

41. https://wadr.org/sierra-leone- falls-10-places-in-2024-world-press-freedom-index/ (accessed on November 2025).
42. Reporters Without Borders (RSF) https://rsf.org/en/rsf-world-press-freedom-index-2025-economic-fragility-leading-threat-press-freedom (accessed on 8 November 2025).
43. Media Reform Coordinating Group 'thirteenth edition of Press Freedom report' https://mrcgonline.org/wp-content/ uploads/2025/05/THIRTEENTH-EDITION-PRESS-FREEDOM-RE PORT-2024.pdf (accessed on 21 October 2025).
44. https:///.www.globalparliamentofmayor (accessed on 3 November, 2025).
45. Sierralii 'The state of Cyber-Bullying in Sierra Leone: Where is the law?' https://sierralii.gov.sl/articles/ 2023-12-08/Hump hrina/the-state-of-cyber-bullying-in-sierra-leone-where-is-the-law .(accessed on November 2025).
46. Sierra Leone Association of Women in Journalism (2022) 'Threats Against Public-Facing Women in SL' https:///.www.internewslocalvoices,globalchange (accessed on 3 November, 2025).
47. Media Foundation for West Africa 'Women's rights online in Sierra Leone: national policy gaps and recommendations' 2023 https://mfwa.org/publication/womens-rights-online-in-sierra-lone-national-policy-gaps-and-recommendations/ (accessed on November 2025).
48. Ministry of Information and Civic Education 'MoICE Concludes Final National Validation of the Data Protection and Right to Access Information Bill 2025' https://moice.gov.sl/moice-concludes-final-national-validation-of-the-data-protection-and-right-to-access-information-bill-2025/ (accessed on November 2025).

mitment to press freedom, privacy, and responsible journalism, announcing that the Media and Information Policy and the Records and Archives Policy had been tabled before Cabinet for approval following nationwide consultations.[49]

Sierra Leone currently lacks a dedicated data protection authority. Enforcement and investigation responsibilities are handled by the Criminal Investigation Department (CID), the Cyber Crime Unit, and the National Cyber Security Coordination Center (NCSCC). The proposed Data Protection Bill is expected to establish an independent authority and provide mechanisms for individual redress once enacted.

The Cyber Security and Crime Act of 2021 criminalises unauthorised access, interference, and deletion of computer data and identity theft, with penalties of up to five years imprisonment and fines of up to Le 500 million.[50]

In August 2025, the All People's Congress (APC) reported an alleged data breach in its Diaspora membership portal, citing unauthorised deletion, alteration, and insertion of member records, raising serious concerns about data integrity and personal data security.[51] Additionally, during the arrest of Sylvia Blyden, her laptop and phone were reportedly seized and accessed, raising concerns over unauthorised data access.

The Cybercrime Act contains overly broad investigative powers that raise concerns regarding human rights. Section 10(5) allows authorities to extend searches to connected systems without fresh judicial authorisation, risking intrusive digital raids. Sections 13 and 14 permit real-time interception of traffic and content data without clear safeguards or independent oversight.

Section 44(2)(b) criminalises electronic messages deemed "insulting," "annoying," or causing "ill-will,"[52] using vague terms that may restrict legitimate criticism and dissent. In early 2025, social media influencer Hawa Hunt was arrested under the Act for allegedly transmitting "insulting messages" critical of the President and First Lady.[53]

Sierra Leone signed the AU Convention on Cybersecurity and Personal Data Protection, also known as the Malabo Convention, in 2016, but has not yet ratified it.[54] While the country currently relies on the Telecommunications Act 2006 for limited safeguards, the Data Protection Bill, finalised on 7 November 2025 after nationwide consultations, aims to align national law with international best practices and strengthen digital rights protections.[55]

Digital IDs and Human Rights Implications

In 2021, Sierra Leone launched its first biometric driver's licenses in the country by issuing the President of Sierra Leone a biometric driver's license.[56] According to the Sierra Leone Road Safety Authority (SLRSA), the license includes a smart chip, QR code, enhanced security features, and integration with the National Civil Registration Authority database. While these measures strengthen authenticity and road safety monitoring, they also raise important considerations regarding privacy, data protection, and potential misuse in the absence of a comprehensive data protection framework.[57]

Privacy and Surveillance

The Cybersecurity Act authorises state surveillance but lacks clear requirements for necessity and proportionality, raising potential conflicts with Article 4 of the African Charter on Human and Peoples' Rights (ACHPR). The Data Protection Act is still under development, and there is no comprehensive regulatory framework governing biometric or facial data, da

49. Ministry of Information and Civic Education 'Minister Reaffirms Commitment to Press Freedom and Digital Rights at National Policy Dialogue' https://moice.gov.sl/minister-reaffirms-commitment-to-press-freedom-and-digital-rights-at-national-policy-dialogue-organised-by-paradigm-initiative-and-the-media-reform-coordinating group/ (accessed 27 October 2025).
50. Cyber Security and Crime Act of 2021, Part V, S 33. https://mocti.gov.sl/wp-content/uploads/2024/12/Sierra-Leone-Cyber-Crime-Act-2021.pdf (accessed on November 2025).
51. Forum News Sierra Loene https://forumnews-sl.com/alleged-data-breach-and-identity-theft-in-apc -diaspora-membership-portal-a-crisis-that-demands-swift-action/ (accessed on 23 October 2025).
52. Media Foundation West Africa https://mfwa.org/how-sierra-leon-is-hiding-behind-the-fight-against-cybercrime-to-abuse-digital-rights/? (accessed on November 2025).
53. The Guardian 'Fears grow for health of social media influencer arrested on live TV in Sierra Leone' https://www.theguardian. com/global-development/2025/feb/10/social-media-influencer-sierra-leone-hawa-hunt? (accessed on November 2025).
54. African Union Convention on Cybersecurity and Personal Data Protection https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed on 23 October 2025).
55. Ministry of Information and Civic Education 'Nationwide Consultations Begin on Sierra Leone's First Data Protection Law' https://moice.gov.sl/nationwide-consultations-begin-on-sierra-leones-first-data-protection-law/ (accessed on 27 October 2025).
56. Sierra Leone President receives biometric driver's licence https://statehouse.gov.sl/sierra-leone-road-safety- authority-presents-biometric-drivers-license-to-president-julius-maada-bio/ (accessed on 23 October 2025).
57. As above, n -75.

ta-sharing, or algorithmic accountability.[58] These gaps create serious human rights concerns, increase the risk of mass surveillance, and privacy breaches.

On January 16 2025, the police officially announced the CCTV surveillance systems across Freetown and other major provincial areas in the country, described in local media as "smart video" installations intended for crime prevention, a deployment that implicitly enables the use of facial recognition in public spaces.[59]

In 2024, the government expanded facial biometric systems through the National Civil Registration Authority (NCRA) and the Sierra Leone Police. The NCRA launched a biometric national ID system combining fingerprints and facial data, with mobile enrollment beginning in December 2024 and nationwide verification checks starting in January 2025.[60] By mid-2025, over 90% of citizens were reportedly enrolled, making it one of the country's largest facial biometric databases, with significant implications for privacy, non-discrimination, and freedom of assembly.[61]

There are no publicly documented cases of systematic government-requested content takedowns. However, in 2022, the National Cyber Security Coordination Center (NCSCC) announced stricter monitoring of social media content to address fake news, incitement, cyberterrorism, and online abuse.[62] Framed as a cybersecurity measure, this signalled increased scrutiny of online political discussions, viral content, and private messaging platforms under existing cybercrime and ICT laws.

Sierra Leone has a legal framework for the oversight of its intelligence/surveillance apparatus, providing both Parliamentary and Judicial oversight. Parliament exercises oversight through committees such as the Parliamentary Oversight Committee on Defence, Internal and Presidential Affairs and the Committee on Communication, Technology, and Innovation,[63] which reviews security-sector operations, laws, and budgets.[64] Judicial oversight exists through a complaints tribunal for grievances against the Central Intelligence and Security Agency (CISA), and the Supreme Court adjudicates disputes over intelligence activities and information disclosure on national security grounds.

Developments in ICT and Emerging Technologies

AI Policy development

There is no existing AI bill or policy in Sierra Leone yet, but the Government is taking a proactive approach by developing its first comprehensive AI strategy through an "AI Readiness Assessment.[64] This report is called the Technological Need Assessment - Sierra Leone,[65] which will serve as the foundational blueprint for a national AI policy and regulatory framework. This effort aligns with the National Digital Development Policy (2021), which promotes the use of emerging technologies to address national challenges in education, healthcare, and public administration.[66]

In 2019, the GOSL, through the Directorate of Science, Technology, and Innovation (DSTI), published a 10-year National Innovation and Digital Strategy (NIDS). The strategy includes AI as a key component, prioritising a "country-as-AI-lab" model, aiming to leverage AI and data science to address societal challenges and improve government decision-making and service delivery.[68]

58. Ministry of Information and Communication https://moice.gov.sl/nationwide-consultations-begin-on-sierra-leones-first-data-protection-law/ (accessed on 5 November 2025).
59. Sierra Leone Police (SLP) http://www.police.gov.sl/uncategorized/slp-rolls-out-cctv-cameras-in-bo-city-to-combat-crime/ (accessed on 5 November 2025).
60. National Civil Registration Authority (NCRA) https://ncra.gov.sl/ (accessed on 5 November 2025).
61. https://www.biometricupdate.com/202506/sierra-leone-reaches-93-percent-national-id-coverage-80-percent-services-digitized (accessed on 5 November 2025).
62. Sierra Leone Observes https://slobserver.org/wp-content/Library/220811%20NCCC%20%20warns%20public%20against% 20engaging%20in% 20cyber%20terrorism.pdf. (accessed on 5 November 2025).
63. https://www.ndi.org/sites/default/files/Sierra-Leone-MP-Roles-Responsibilities-Manual-2008.pdf (accessed on 19 November 2025).
64. https://www.cpahq.org/directory/sierraleone/#:~:text=The%20Parliament%20of%20Sierra%20Leone%20website%20is:, *%20Public%20Petition%20Committee%20*%20Supervisory%20Committee (accessed on 19 November 2025).
65. Ministry of Communication, Technology and Innovation 'Sierra Leone Takes a Purpose-Driven Approach to AI' https://ia frica.com/sierra-leone-launches-national-ai-readiness-assessment-with-world-bank-support/ (accessed on 14 November 2025).
66. sierra_leone_technology_needs_assessment_final.pdf https://www.un.org/technologybank/sites/www.un.org.technologybank /files/sierra_leone_technology_needs_assessment_final.pdf (accessed on 16 March 2026).
67. Ministry of Communication, Technology and Innovation https://mocti.gov.sl/wp-content/uploads/2024/10/S_L_Digital-Development-Policy.pdf (accessed on 14 November 2025).
68. Eta & Associates 'The AI Regulatory Framework in Africa: A Focus on Sierra Leone and Nigeria' https://etaandassociates. com/our-thinking/the-ai-regulatory-framework-in-africa-a-focus-on-sierra-leone-and-nigeria/ (accessed on 14 November 2025).

Facial Recognition and Other Emerging Technologies

Sierra Leone had implemented facial recognition technologies primarily for civil registration through its national ID cards and for security and efficiency in areas like pension management and border control.[69] The University of Management and Technology (UNIMTECH) in Sierra Leone has commissioned a facial recognition system to "automate facial data of students" for tracking their status.[70] Mobile service has been launched for Biometric ID issuance to expand access to these cards.[71]

The Government developed its National Innovation & Digital Strategy (NIDS) 2019 - 2029, that aims at guiding Sierra Leone's investments, policies, and governance frameworks for present and future development, making references to emerging technologies such as Internet of Things (IoT), Blockchain, Quantum.[72] In 2018, a blockchain-based digital voting solution was piloted during the presidential election, using a permissioned blockchain to enhance transparency. While innovative, this initiative sparked debates about trust, accessibility, and technical oversight.[73] In July 2024, EON Reality established Sierra Leone's first Spatial AI Center, marking a significant step toward equipping students and professionals with advanced skills in virtual, augmented, and spatial AI technologies for sectors such as mining, agriculture, and renewable energy.[74]

Sierra Leone has made efforts to incorporate multi-stakeholder consultations in digital policy development through working groups, public forums, and national events. The National Digital Development Policy (2021) benefited from validation exercises and expert consultations across infrastructure, digital skills, and emerging technologies.[75]

Also, the Digital Transformation Project, led by the Ministry of Communication, Technology, and Innovation (MoCTI), featured public engagement through workshops, digital summits "Sierra Leone Innovates,"[76] and awareness initiatives, including the publication of a YouTube video on the National Fibre Backbone II project.[77]

Digital Inclusion

According to the 2015 Population and Housing Census (PHC), persons with disabilities accounted for 1.3% of the national population (93,129 individuals), with the Northern Region recording the highest number, with 32,849 persons with disabilities, representing 35.3% of the country's disabled population. Disease or illness is identified as the leading cause of disability, followed by congenital conditions (16.2%), other unspecified causes (10.5%), accidents (8.8%), and natural ageing (8.1%).[78]

The Government has taken steps to enhance digital inclusion through policies such as the Assistive Technology (AT) Policy and Strategic Plan.[79] In September 2025, the Directorate of Science, Technology, and Innovation (DSTI) and the National Commission for Persons with Disabilities (NCPD) signed an MoU to expand digital literacy and inclusion.[80] This initiative resulted in the training of 1,000 persons with disabilities in basic and intermediate digital skills through DSTI Digital Learning Hubs in Bo, Kenema, Freetown,

69. 'Sierra Leone partners to build blockchain-powered digital ID system' https://www.biometricupdate.com/202511/sierra-leone-partners-to-build-blockchain-powered-digital-id-system (accessed on 14 November 2025).
70. The University of Management and Technology 'UNIMTECH, The Mother of Innovation and Technology in Sierra Leone' https://unimtech.edu.sl/7794/ (accessed on 15 November 2025).
71. https://www.biometricupdate.com/202412/sierra-leone-launches-mobile-service-to-expand-biometric-id-issuance? (accessed on November 2025).
72. As Above, n -88.
73. World Economic Forum 'The world's first blockchain-powered elections have just happened in Sierra Leone' https://www.weforum.org/stories/2018/03/the-world-s-first-blockchain-powered-elections-just-happened-in-sierra-leone/ (accessed on 15 November 2025).
74. EON Reality 'EON Reality Announces National Rollout in Sierra Leone with the Launch of Spatial AI Center and Introduction of 10,000 Tailored Courses' https://eonreality.com/eon-reality-announces-national-rollout-in-sierra-leone-with-the-launch-of-spatial-ai-center-and-introduction-of-10000-tailored-courses/ (accessed on 15 November 2025).
75. Ministry of Communication, Technology and Innovation 'MoCTI hosts a one-day stakeholder engagement to review the state of digital public services in Sierra Leone' https://mocti.gov.sl/mocti-hosts-a-one-day-stakeholder-engagement-to-review-the-state-of-digital-public-services-in-sierra-leone/ (accessed on 15 November 2025).
76. MoCTI https://mocti.gov.sl/wp-content/uploads/2025/08/Lite-2025-Sierra-Leone-Innovates-Digital-Government-Summit-Newsletter.pdf (accessed on 15 November 2025).
77. MoCTI https://mocti.gov.sl/sierra-leone-digital-transformation-project/ (accessed 15 November 2025).
78. https://at2030.org/assistive-technology-policy-and-strategic-plan/&opi=89978449&psig= AOvVaw1YO pB23Y-lUtAy2gdp 1YEpz&ust=1763330813326000 (accessed on 15 November 2025).
79. As above, n- 100.
80. DSTI and NCPD Sign MoU to Advance Digital Inclusion for Persons with Disabilities https://www.linkedin.com/comp any/the-directorate-of-science-technology-and-innovation/posts?lipi=urn %3Ali%3Apage%3Adflagship-3detail_base% 3BH4u62qixSDmjPnWI%2Bog%2B6A%3D%3D (accessed on 21 October 2025).

and Makeni, improving pathways to employment and entrepreneurship

Furthermore, the Government, together with DSTI, has also developed the "Leh We Tok" app, designed to empower people living with speech and hearing impairments.[81] The Technical Director of the DSTI noted that digital platforms will be adapted with accessibility features to enhance participation, stressing that the initiative will ensure inclusivity and co-creation at every stage of design and implementation.[82]

Child Online Safety

There is no specific law on online child violations; however, the existing national laws relevant to Online child violations include the Child Rights Act, the Sexual Offences Act 2019, and the Cybersecurity and Crime Act 2021. Article 47 of the Cybersecurity Act criminalises online child abuse and child sexual exploitation, which is punishable by law.[83] These laws don't explicitly and fully criminalise all forms of OCSEA-related offences nor include provisions that explicitly recognise the rights and gendered risk faced by girls.

Over the year, there has been a rapid increase in OCSEA in Sierra Leone. Studies show that 20% of girls aged 15–19 have experienced online sexual exploitation,[84] 24% of teenagers have faced cyberbullying, and 17% of young women have been affected by cybercrime.[85] In response, the Comprehensive School Safety Policy (2023) introduced guidelines on online safety.[86]

81. 'DSTI develops Lek We Tok App, an assistive technology for people living with speech and hearing impairments' https://lnkd.in/druWWz74 (accessed on 21 October 2025).
82. https://thecalabashnewspaper.com/ncpd-dsti-ink-historic-mou-to-empower-persons-with-disabilities-in-digital-space/ (accessed on 22 October 2025).
83. Cybersecurity and Crime Act 2021, Art 47
84. 'Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa' https://ecpat.org/wp-content/uploads/2025/02/GYW-Led-Assesment-Report-on-OSEA-and-Tech-Facilitated-GBV.pdf (accessed on 17 November 2025).
85. As above, n-106.
86. Ministry of Basic and Senior Secondary Education https://mbsse.gov.sl/wp-content/uploads/2023/03/2023_Comprehensive-School-Safety-Policyvf-1.pdf (accessed on 17 November 2025).

Privacy and Surveillance

In Sierra Leone, the Universal Service Fund is referred to as the Universal Access Development Fund (UADF),[87] which was established by the Government of Sierra Leone, entrusted with a mandate to ensure equitable access to mobile and broadband internet services across the nation. The UADF aims to bridge connectivity gaps in underserved communities. In 2023, UADF installed towers in Yoryeama (Moyamba District) and Sogbaleh (Bonthe District), extending connectivity to communities of approximately 5,000 and 3,500 residents, respectively. In 2024, 47,000 people in 14 communities, 30 schools, and 10 community health centres across Sierra Leone have now benefitted from UADF's rural connectivity initiative. Complementary initiatives, such as Mobile Phone E-Money and Charging Kiosks, the Tokeh Community Digital Services and Hotspots Centre, and ICT hubs, have improved access to ICT services, supported SMEs, and empowered women in agriculture. The primary sources of funding for UADF's projects and activities included revenue from the service levy imposed on licensed service providers and financial contributions from the National Communications Authority (NATCA).

However, transparency remains a concern. UADF did not formally respond to information requests regarding fund allocations, citing internal approval processes. Available information was sourced from its 2023 annual report.

87. Universal Access Development Fund https://uadf.gov.sl/ (Accessed on 23 October 2025).

Conclusion

Sierra Leone has demonstrated notable progress in digital transformation, policy innovation, and inclusion initiatives. Improvements in press freedom, digital governance, and civic participation signal political commitment to reform. However, gaps persist between policy commitments and implementation. Weak data protection, limited oversight of emerging technologies, uneven enforcement of cybersecurity laws, and persistent digital inequalities continue to undermine trust and the protection of rights.

To strengthen its digital rights environment, Sierra Leone must accelerate passage of the Data Protection Bill, embed human rights safeguards in AI and emerging technology governance, enhance independent oversight, and invest in equitable access and digital literacy. With sustained reforms, the country is well-positioned to consolidate gains and advance toward a more inclusive, rights-respecting digital future.

Recommendations

The Government should:

- Amend the Cybersecurity and Crime Act (2021) to remove provisions that criminalise legitimate online expression and align enforcement with regional and international human rights standards.
- Adopt and enforce a comprehensive Data Protection Law, including the establishment of an independent, well-resourced data protection authority with investigative and redress powers.
- Guarantee non-disruptive access to the internet by prohibiting shutdowns and throttling except under strictly lawful, necessary, and proportionate circumstances.
- Introduce clear safeguards, judicial oversight, and public reporting on surveillance technologies, procurement processes, and data-handling practices.
- Invest in affordable and reliable internet infrastructure, particularly in rural and underserved areas, and strengthen the effective use and transparency of universal access funds.
- Provide human-rights-based training for ministries and security agencies on privacy and digital rights, and institutionalise meaningful multi-stakeholder consultations in digital policy development.

Civil Society Organisations should

- Expand digital rights awareness campaigns and systematically document and report violations, including misuse of cybercrime laws, surveillance abuses, and internet disruptions.
- Build coalitions across human rights, media, legal, and technology sectors to coordinate advocacy, share expertise, and respond effectively to digital rights threats.
- Provide digital security training for journalists, activists, and human rights defenders; advocate for transparency and safeguards in biometric and surveillance systems; and support strategic public-interest litigation.
- Contribute expert, rights-based input into draft legislation and national digital policies, particularly on data protection, AI, and cybersecurity.

The Media should:

- Enhance digital literacy, cybersecurity, and data protection skills among journalists to improve online safety and secure reporting practices.
- Increase investigative journalism on digital governance, surveillance, data protection, internet shutdowns, and online child safety issues.
- Uphold ethical standards in online reporting, counter disinformation, and actively participate in policy debates on digital laws and press freedom.
- Strengthen media associations to provide legal aid, advocacy, and support networks for journalists facing digital threats, and produce public-facing content on online safety, privacy rights, and responsible digital use.

The Score Index

Sierra Leone, 2025

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

Indicator	ACHPR Principle	2025 Score	2025 Justification
Internet Shutdowns	P38(2)	5	In 2025, there were no internet shutdowns, even during the 2023 elections, indicating a modest progress in internet disruption.
Inexistent laws, policies, and other measures to promote universal, equitable, affordable, and meaningful access to the internet	P37	3	There is an existing law, the National Communications Authority Act 2022, and the Government, through the Universal Service Fund, also known as the Universal Access Development Fund, has implemented many initiatives to bridge the digital divide in the country.
False News Criminalisation	P22(2)	2	Sierra Leone's existing law continues to criminalise online speech, leading to arrest and prosecution sporadically between 2020 and 2025.

Indicator	ACHPR Principle	2025 Score	2025 Justification
Sedition Legislation	P22(2)	5	The Sedition and Libel provision in Part V of the Public Order Act was repealed in 2020.
Arbitrary Arrests and Harassments of the Media, HRDs, and Citizens	P20(1) & (2)	2	There has been a high rate of threats, harassment, assault, and intimidation of journalists, human rights defenders, and activists in 2024 and 2025.
Data Protection Legislation.	P42	3	Sierra Leone does not have a comprehensive data protection law yet, but the final national validation of the Data Protection Bill 2025 has been completed, which is still awaiting passage.
Online Content Removal Without Process	P38 and P39(4)	3	Sierra Leone has no documented cases of government-ordered blocking or filtering by Meta or TikTok in 2024 and 2025. However, between 2020 and 2023, there were four recorded government requests for content takedowns from Sierra Leone.
Invasion of Privacy of Communications	P41	2	The Cybersecurity Act authorises surveillance but lacks clear requirements for necessity and proportionality, raising potential conflicts with Article 4 of the African Charter on Human and Peoples' Rights (ACHPR).
Failure by the government to proactively disclose and disseminate information on digital technologies.	P29(3)	3	The websites of most government institutions are not regularly updated to fully comply with the Access to Information Act, 2013 by proactively disclosing and disseminating information.
AI and Emerging Technologies national strategies	P39(6)	2	There is no existing AI bill or policy in Sierra Leone yet, but the Government is taking a proactive approach by developing its first comprehensive AI strategy through an "AI readiness assessment. This report is called the technological Need Assessment -Sierra Leone.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	1	Sierra Leone does not have a specific law or policy focused on children's digital safety. However, there are existing national laws that criminalise online child violations.
Digital Inclusion	P37(3)	2	The Government has implemented a lot of initiatives and strategies towards digital inclusion and advancement in the country.
Total (out of 60):		2025 33	

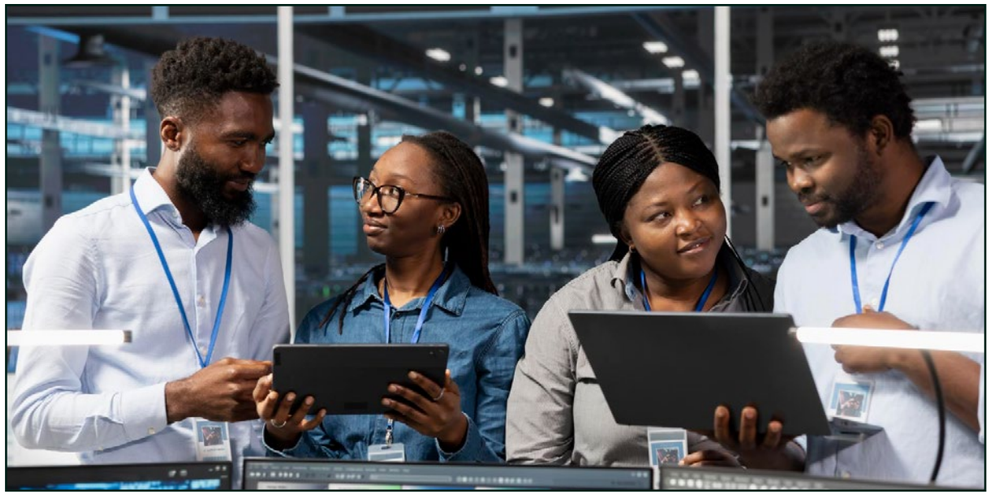
SENEGAL

By Moussa Waly Sene

Executive Summary

In 2024, Senegal joined the 17 African countries that have launched at least one GAINDESAT-1A satellite into orbit. It joined countries like South Africa and Egypt, which each have 13 satellites, as well as Nigeria, which ranks third with 7 satellites. President Bassirou Diomaye Diakhar Faye stated that this initiative represents a significant step towards Senegal's "technological sovereignty".[1]

In 2025, this satellite entered full operational status, enabling the deployment of agricultural remote sensing and natural resource monitoring services. The government announced the development of a second satellite, GAINDESAT-1B, as part of the New Deal for Technology, with a launch planned for 2027.[2] However, technological sovereignty must result in tangible advantages for citizens' digital rights; it cannot be limited to the ownership of space infrastructure. However, no evidence that is currently accessible to the public indicates that the GAINDESAT-1A satellite has helped close the digital divide, make the internet more affordable, or provide connectivity to underserved rural areas. This report on Senegal's digital rights and inclusion has been updated and rewritten in light of this. Internet access, freedom of speech, data protection and privacy, content censorship and moderation, information access, artificial intelligence and new technologies, digital inclusion, and the Universal Service Fund were all examined in the study that served as the foundation for this report. This report has shown that there is still more work to be done in the area of press freedom.



1. GAINDESAT-1A, the first Senegalese satellite, successfully launched:https://www.jeuneafrique.com/1599726/politique/gaindesat-1a-premier-satellite-senegalais-lance-avec-succes/ (Accessed on November 28, 2024).
2. Senegalese Space Agency (ASENA), 2025 Annual Activity Report, Dakar, 2025Ministry of Digital Affairs and Telecommunications, New Deal for Technology — Space Roadmap, February 2025

Introduction

Senegal launched a digital strategy called "New Technological Deal" in 2025.[3] This new strategy aims to transform the country into a digital hub by 2034, with a planned investment of 1,097 billion CFA francs. Objectives include reducing dependence on foreign technologies, strengthening cybersecurity, digitising public services, promoting tech entrepreneurship and positioning Senegal among the top three African exporters of digital services. The plan also includes training 100,000 graduates in the digital field, achieving 95% internet connectivity, and creating more than 500 certified startups by 2034.[4]

To boost the digital sector, Senegal, under the leadership of the president of the Republic, has embarked on an ambitious digital transformation initiative called the "New Technological Deal."[5] This strategy aims to position the country as a leader and catalyst for digital innovation in Africa.

In relation to the digital economy, Senegal's General Directorate of Taxes and Domains (DGID)[6] has declared that value-added tax (VAT) will henceforth apply to digital services offered by international online service providers and digital platforms. An important development in its digital tax policy is the new 18% VAT on services rendered by digital platforms. The goal of this project is to govern Senegal's digital services industry.

Although the New Deal for Technology is a declared goal, an examination of it exposes a number of significant flaws. First, in terms of budgetary transparency, Senegal's commitments under the Open Government Partnership (OGP), of which it has been a member since 2018, are in conflict with the announced 1,097 billion CFA francs since there is no public mechanism for tracking disbursements or performance indicators available to citizens. Furthermore, neither an evaluation of the impact on basic rights nor a recourse mechanism for persons denied internet access is specifically included in the strategy for human rights protections.

Lastly, in terms of execution, earlier digital strategies, most notably the Digital Senegal Strategy 2016–2025 failed to meet its goals of universal access without providing a public evaluation. While the introduction of VAT on foreign digital services aims to broaden the tax base, it risks increasing the cost of access to digital platforms for low-income users, thereby exacerbating already documented inequalities in access. No impact assessment on affordability was published before this measure.[7]

Internet Access and Disruption

According to the official website of the Telecommunications and Postal Regulatory Authority (ARTP),[8] in March 2025, Senegal's internet penetration rate reached 125.67%, reflecting massive adoption through the use of mobile and fixed devices. Due to the multiple connections per individual, the figure exceeds the total population. By early 2025, 11.3 million internet users represented 60.6% of the population.

These two figures are not contradictory but measure distinct realities that need to be clarified to guarantee the credibility of the analysis:

The rate of 125.67% (ARTP, 2025) corresponds to the number of active SIM cards

3. https://stcc-ssi.sn/lancement-de-la-strategie-numerique-du-senegal-new-deal-technologie-24-fevrier-2025-aucicad/
4. https://www.presidence.sn/fr/actualites/new-deal-technologique-une-ambition-nationale-pour-faire-du-senegal-un-leader-de-leconomie-numerique-en-afrique
5. With its new technological deal, Senegal aims to become a leader in digital innovation in Africa.https://www.rts.sn/actualite/detail/a-la-une/new-deal-technologique-le-senegal-ambitionne-de-devenir-leader-de-linnovation-numerique-en-afrique (Accessed on November 28, 2024).
6. Order No. 10698 of June 27, 2024, concerning the application of their Article 355-bis of the CGI.
7. Open Government Partnership (OGP), Senegal National Action Plan 2023-2025, Washington DC, 2023OECD, Principles on Digital Governance, Paris, 2020 — Budgetary transparency and accountability in national digital strategiesITU, World Telecommunication Development Report 2024 — Assessment of National Digital Strategies in Sub-Saharan AfricaAfrican Commission on Human and Peoples' Rights (ACHPR), Declaration of Principles on Freedom of Expression and Access to Information in Africa, Principle 37(3), 2019 — obligation of States to promote universal, equitable and affordable access to the Internet
8. https://artp.sn/

relative to the total population. It exceeds 100% because an individual can hold several SIM cards simultaneously (professional/personal use, multiple operators). This figure measures mobile subscription penetration, not actual internet access.[9]

The 60% rate (DataReportal, 2024) measures the proportion of individuals who actually used the internet in the last three months, regardless of the number of SIM cards they own. This indicator reflects effective individual internet access.[10]

The gap between these two rates reveals a structural digital divide: nearly 40% of the Senegalese population remains without effective internet access despite seemingly satisfactory network coverage. The main causes are the prohibitive cost of mobile data, estimated at 2.8% of the average monthly income, above the 2% affordability threshold set by the Alliance for Affordable Internet (A4AI), and the low rate of device ownership in rural areas.

This distinction is fundamental in a rights-based analysis: the right of access to the Internet, as recognised by the United Nations Human Rights Council, implies effective and affordable individual access, not simply the existence of formal subscriptions.

In Senegal, according to the Internet Tariff Observatory's report for the first quarter of 2025, mobile internet offers resemble a constantly evolving market, catering to both the public and professionals. For individuals, operators offer customisable passes, tailored to each user's needs. Orange, for example, offers a wide range of options, from small daily passes at 50 CFA francs (approximately $0.09) for a few hours of use to monthly or 5G plans capable of supporting heavy usage. Expresso, on the other hand, focuses on diversity with offers ranging from very short-term options—such as the "Golden Hour," 2 GB for one hour—to monthly subscriptions of up to 200 GB (approximately $354). YAS adopts a simpler but targeted approach, with affordable monthly passes (2000 F ≈ $3.54 to 15000 F ≈ $26.55) and even seasonal offers for Ramadan (500 F ≈ $0.89 to 2000 F ≈ $3.54).

On the business side, the landscape is changing: the focus is less on flexibility and more on reliability. Operators are structuring their plans with or without a contract, offering larger data allowances and often with bonuses, particularly for 5G. Orange offers plans ranging from a few gigabytes for small teams (3098 F ≈ $5.48) to over 80 GB for more intensive use (49560 F ≈ $87.60), while Expresso and YAS complete this segment with Business or Pro offers tailored to the needs of SMEs. Some plans even include dedicated solutions, such as Expresso's 4G mini-routers, capable of reaching up to 500 GB (100000 F ≈ $177). However, the high cost of internet access should be noted, as this significantly contributes to the difficulties citizens face in accessing ICT services. Financial accessibility to the internet in Senegal constitutes a structural obstacle to the full realisation of digital rights.

A comparative regional analysis helps to measure the scale of the challenge:

In Senegal, 1 GB of mobile data costs on average 2.8% of monthly gross national income (GNI) per capita (2024), which is above the 2% affordability threshold set by the Alliance for Affordable Internet (A4AI).[11]

By comparison, this ratio is 1.2% in Morocco, 1.7% in the Ivory Coast, 1.9% in Ghana and 0.9% in South Africa, placing Senegal among the African countries where the internet remains the least financially accessible.[12]

The average cost of one gigabyte of mobile data worldwide is USD 4.68; in Senegal, it is roughly USD 1.20. For most people, the cost is still disproportionate when compared to average income, especially in rural areas where average income is 40% lower than in metropolitan areas. According to ARTP, rural women, the elderly and low-income populations are most affected by this cost; the internet penetration rates in rural areas are 35 points lower than in urban areas.[13] Access to fixed broadband internet (24.39% penetration) remains almost

9. ARTP Senegal, Electronic Communications Market Observatory — Quarterly Report Q1 2025, Dakar, 2025
10. DataReportal, Digital 2024: Senegal, Kepios Analysis, January 2024
11. Alliance for Affordable Internet (A4AI), Affordability Report 2024, Washington DC, 2024 — Regional comparative data on the cost of the Internet in Africa
12. World Bank, World Development Indicators 2024 — GNI per capita, Senegal and comparator countries

exclusively urban, further widening territorial inequalities.

Principle 37 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa (ACHPR, 2019) requires governments to take specific steps to ensure universal, equitable, and affordable access to the internet. This data indicates a failure to meet these obligations. Although the Universal Telecommunications Service Development Fund (UTSDF) was created specifically to meet this need, its effect on cost reduction is still not well-documented or publicly assessed.

Freedom Of Expression

Despite initial pledges by the PASTEF government to restore liberties, there is growing concern over freedom of expression in Senegal in 2025 due to the arrest of journalists, closure of media outlets, and summoning of opposition members. Since May 2024, the situation has hardened, according to observers, and the judicial reforms that were pledged at the national justice conference have not been implemented.

Arrests of Journalists

- Maimouna Ndour Faye, the director of 7TV, was taken into custody by gendarmes in Dakar on October 28, 2025, when she was interviewing an opposition politician.
- Television pundit Badara Gadiaga was arrested on July 10, 2025, for his on-air criticism of the Prime Minister, who is charged with defaming the head of state and disseminating false information. He is still being held.
- In September 2025, at least two columnists were detained pending trial for disseminating false information.

Media Closures and Suspensions

On April 22, 2025, Ministerial Order No. 011059/MCTN issued by Minister Alioune Sall ordered the cessation of activities of 381 media companies for non-compliance with the press code, a decision deemed illegal by the Supreme Court (ruling of April 11, 2024, limiting ministerial powers). This includes the suspension of advertising contracts by the Prime Minister's Office and jeopardises the survival of entire newsrooms.

The Senegalese Constitution[14] guarantees freedom of expression. Senegalese law places great importance on freedom of expression. For reference, see Law No. 2008-10 of January 25, 2008, the Framework Law on the Information Society (LOSI),[15] the 2017 Press Code, and Law No. 2018-28 of December 12, 2018, the Electronic Communications Code. To strengthen human rights, the government has drafted a law on the Promotion and Protection of Human Rights Defenders.

The aforementioned acts are more than just media-related situations; they involve the Senegalese state's international obligations under several legally binding agreements.

From the perspective of universal international law, Article 19 of the International Covenant on Civil and Political Rights (ICCPR), ratified by Senegal, guarantees freedom of expression and only permits restrictions if they cumulatively meet three conditions: they must be prescribed by law, pursue a legitimate aim, and be necessary and proportionate. The arrest of journalists for "spreading false news" and "insulting the Head of State" clearly fails to meet this three-part test: the United Nations Human Rights Committee explicitly stated in its General Comment No. 34 that laws on "false news" and the offence of insulting leaders are incompatible with Article 19 of the ICCPR when used to suppress legitimate criticism.

From the perspective of African regional law, Principle 20 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa (ACHPR, 2019) expressly prohibits the arbitrary arrest of journalists and digital rights defenders.

Principle 22(2) requires states to repeal

13. ARTP Senegal, Internet Tariff Observatory — Q1 2025 Report, Dakar, 2025

14. JORS, No. 5963 of January 22, 2001.
15. JORS, No. 6406 of May 3, 2008, p. 419 et seq.

laws criminalising sedition, insulting leaders, and disseminating false news when these laws are used to suppress freedom of expression. Article 9 of the African Charter on Human and Peoples' Rights enshrines the right to receive and impart information without arbitrary restriction.

In light of the decisions by the ECOWAS Court of Justice: The ECOWAS Court of Justice condemned Senegal on May 14, 2025, in the ASUTIC case. The Republic of Senegal established a direct regional precedent: the state has already been found guilty of violations of the rights to freedom of expression and to work related to digital restrictions. The documented arrests of journalists in 2025 fall within this same pattern of repression, exposing Senegal to further proceedings before this court.

These acts constitute clear and documented violations of Senegal's international and regional obligations regarding digital rights and freedom of expression. Their systematic repetition reveals not isolated incidents but a pattern of deliberate restriction of digital civic space, incompatible with the commitments made by the state.

Access to information

In 2025, access to public information in Senegal will undergo a major advancement with the promulgation of Law No. 14/2025[16] on access to information on September 25, 2025. This law guarantees every citizen an expanded right to access documents held by public administrations, with exceptions such as national security or privacy. Any individual may submit a written request for access to information. The relevant organisation must respond within eight clear days, which may be extended to fifteen days if necessary. Access will be free of charge, except for costs related to the reproduction or transmission of documents.[17]

The promulgation of Law No. 14/2025 on access to information on September 25, 2025, marks a historic turning point in the Senegalese legal framework. For over two decades, the absence of such a law had constituted a structural obstacle to transparency and public accountability. This adoption brings Senegal into partial compliance with the African Union Model Law on Access to Information (2013) and with the commitments made within the framework of the Open Government Partnership (OGP) since 2018.

However, the formal adoption of the law is not enough to guarantee the effectiveness of the right: several conditions must be met for implementation in accordance with international standards:

- The establishment of an independent supervisory authority responsible for handling appeals
- The training of public officials on disclosure obligations
- The establishment of sanction mechanisms in the event of unjustified denial of access
- The allocation of sufficient budgetary resources for effective implementation

The African Union adopted a model law for Africa on access to information in 2013, which aims to guide member states in developing national legislation on the matter.[18] Access to information law enables state authorities to be accountable, transparent and to strengthen trust in public institutions. Access to law information allows citizens to participate fully in public life.

Data Protection And Confidentiallity

In 2025, a major case made headlines: Ms. Awa Ndiaye,[19] former president of the CDP, was accused by the Association of ICT Users (ASUTIC) of having authorised the mass collection of personal data with

16. https://www.presidence.sn/fr/actualites/communique-du-conseil-des-ministres-du-mercredi-03-septembre-2025
17. https://walf-groupe.com/blog/2025/08/07/acces-a-linformation-le-senegal-veut-franchir-un-cap/
18. Model Law for Africa on Access to Information 2013: https://achpr.au.int/fr/node/873 (accessed 28 November 2024).

out consent (95,814 endorsements for a candidate in the elections), sparking a serious controversy over respect for privacy in the electoral process. The case led to the announcement of a complaint before the ECOWAS Court for alleged violations of data protection rights.

The draft law of 2019,[20] which has not yet been adopted, reforming Law No. 2008-12 of January 25, 2008, on the protection of personal data,[21] proposes major innovations, including the creation and operation of a Personal Data Protection Authority (APDP) and the establishment of specific regimes for the processing of medical data, employee data, biometric data, the Internet of Things, and artificial intelligence.

These innovations aim to modernise the personal data protection system by adapting it to Additional Act A/SA.1/01/10, relating to the protection of personal data within the ECOWAS region and to the African Union Convention on Cybersecurity and the Protection of Personal Data.

In addition, there is the National Data Strategy project, which has the vision of "making data an engine of socio-economic growth, inclusivity, innovation and openness to the international community, by 2028 in Senegal."

In early October 2025, the Directorate General of Taxes and State Property (DGID) suffered a ransomware cyberattack[22] claimed by "Black Shrantac," paralysing tax systems for approximately a week (early October). The hackers exfiltrated 1 terabyte of sensitive data (tax, administrative, and taxpayer) and encrypted servers, blocking tax returns, payments, and collections; losses were estimated at 11 billion FCFA per day. The initial ransom was €10 million (6.5 billion FCFA), reduced to 4 billion FCFA with an ultimatum of October 10 (4:00 PM); authorities denied negotiations, and the DGID[23] denied the official claims.

From a cybersecurity perspective, this incident reveals structural weaknesses—lack of network segmentation and insufficient offline backups—consistent with trends identified by INTERPOL regarding African tax[24], administrations and underscores the urgent need to ratify the Malabo Convention on Cybersecurity.[25] In terms of transparency, the lack of official communication regarding the extent of the breach violates NIST and ENISA standards for incident notification[26] and raises questions about its compatibility with the obligations of Law No. 2008-12 of January 25, 2008.[27] Regarding data protection, the CDP is legally obligated to investigate the DGID's data security practices, thus strengthening the case for the expedited adoption of the 2019 draft law creating an APDP with enhanced sanctioning powers.[28] Finally, the prolonged paralysis of a central digital public service risks permanently eroding public trust in the dematerialisation of state services, compromising the ambitions of the Technological New Deal, as demonstrated by comparable studies on the impact of government data breaches on the adoption of online services.

Censorship And Content Moderation

Developments on Content Censorship and Moderation in 2025

According to Ministerial Decree No. 011059/MCTN of April 22, 2025, 381 media outlets were closed in Senegal in 2025 for violating the press code, and journalists were arrested for "spreading false news" (e.g., Maimouna Ndour Faye arrested on October 28, 2025, in Dakar; Badara Gadiaga detained since July 10, 2025). To achieve a "balance" between freedom of expression and moderation against "hate speech", the PASTEF gov

19. https://cybersecuritymag.africa/violation-protection-donnees-senegal-presidente-commission-accusee-ASUTIC/
20. Draft law to overhaul the system for the protection of personal data by repealing and replacing law no. 2008-12 of 25 January 2008.
21. https://www.cdp.sn/sites/default/files/protection.pdf (Accessed on November 28, 2024).
22. https://lemondedunumerique.com/2025/10/03/cyberattaque-contre-la-dgid-ce-quil-sest-passe-qui-est-derriere-et-pourquoi-ca-nous-concerne-tous/
23. https://fr.allafrica.com/stories/202510030138.html
24. Senegalese media sources (Seneweb, RFM, Le Soleil), October 2025; no official DGID report published at the time of writing.
25. AU, Malabo Convention on Cybersecurity and Data Protection, June 27, 2014, signed but not ratified by Senegal.
26. NIST, Cybersecurity Framework 2.0, 2024 ; ENISA, Guidelines on Cyber Incident Reporting, 2023.
27. Law No. 2008-12 of 25 January 2008 on the protection of personal data, art. 39, JORS No. 6406.
28. Republic of Senegal, Draft law to reform law no. 2008-12, 2019 providing for the creation of the APDP.

ernment, led by Bassirou Diomaye Faye, tightens regulations through the 2025 National Dialogue without creating a new, updated penal code.

Internet outages in 2025

On May 14, 2025, in Lagos, the ECOWAS Court condemned previous incidents (2021-2024, such as mobile restrictions in March 2021 and June 2023 during the Sonko protests) and awarded 250,000 CFA francs in damages to each plaintiff (ASUTIC, Ndiaga Guèye) for violations of the rights to freedom of expression and the right to work. In contrast, the New Deal for Technology places a high priority on connectivity, with no recent blackout measures and a 95% coverage target by 2034.

There were two internet disruptions in Senegal in 2024. These limitations apply to mobile data internet access on February 4th and February 13th, 2024. The Ministry of Communication, Telecommunications and Digital Economy asserts in a statement that “mobile data internet is suspended this Tuesday during certain time periods due to the dissemination on social networks of several hateful and subversive messages which have already provoked violent demonstrations with deaths and significant material damage.”

AI And Emerging Technologies

National AI Strategy

In 2025, Senegal unveiled a national artificial intelligence strategy, integrated into the New Technological Deal and the Senegal 2050 Vision, with a budget of 7 billion CFA francs[29] over two years for research and applications in agriculture, health, education, and infrastructure.

It aims for ethical AI, data protection, and digital sovereignty, in partnership with Meta for an AI computing center.

Senegal is currently developing a National Artificial Intelligence (AI) Strategy.[30] Its vision is “For ethical and trustworthy AI, a catalyst for the Emerging Senegal Plan, youth employment, economic performance, public sector transformation, sovereignty, and Senegal’s attractiveness. “ Senegal intends to make AI an exemplary national collective project, serving the common good, anticipating climate risks, and improving economic performance, while playing a leading role in sub-regional technological cooperation.

The state has acquired a supercomputer with a peak power of 537.6 TFlops, a distributed memory capacity of 1.2 PB, and 8064 computing nodes.[31] This infrastructure provides Senegal with a powerful tool to support the development of artificial intelligence.

Digital Inclusion

The State of Digital Inclusion in 2025

With a focus on rural areas, the informal economy, and educating 100,000 graduates to reduce inequality, Senegal’s digital inclusion is making substantial progress in 2025, thanks to the introduction of the New Technological Deal on February 24, 2025, which aims for 95% universal internet coverage by 2034.

Major National Initiatives

- Digital Inclusion Volunteer Program:[32] Launched on September 2, 2025 at the Place du Souvenir Africain (Dakar); 20 volunteers deployed in 24 communities across 6 departments for digital training, literacy programs, and modernization of administrative archives with local partners.
- Digital Strategy for Education 2025-2029:[33] Official launch on October 6, 2025, for the integration of AI and digital tools in education, promoting equitable access.
- Digital Economy Acceleration Project (PAEN):[34] Expands climate-resilient broadband connectivity, improving public services and businesses.
- National Digital Council (CNN):[35] Established on October 2, 2025, for co

29. https://d4dhub.eu/fr/news/le-senegal-devoile-sa-nouvelle-strategie-ia-un-effort-collaboratif-avec-lequipe-europe
30. https://www.numerique.gouv.sn/mediatheque/documentation/la-strat%C3%A9gie-ia (Accessed on November 28, 2024).
31. Artificial Intelligence, Challenges for Senegal and Africa, National Academy of Sciences and Techniques of Senegal (ANSTS), January 8, 2024.
32. https://letechobservateur.sn/linclusion-numerique-en-marche-le-senegal-lance-son-programme-de-volontariat/

- ordination, inclusion, and sovereignty.

Senegal's digital inclusion is further enhanced by the digital identification policy. The National Digital Identity project has a shared vision: "the existence, by 2024, in Senegal, of an operational, reliable, secure, and accessible digital identity for the benefit of all users." [36]

The main objectives[37] of this project are as follows:

- Facilitate administrative procedures and rapid access to government information;
- Facilitate the interoperability of government information systems;
- Facilitate the exchange of data on individuals and businesses;
- Facilitate the inclusion of all citizens to achieve sustainable development goals and create wealth.

Although this project is still in the phase of gradual deployment in 2025, its strategic relevance in terms of inclusion is reinforced by the fact that it is now a part of a larger vision, pushed by the New Deal on Technology. There hasn't been an official identification of any significant legal measures aimed at protecting youngsters online. However, the increased integration of digital tools into the education system, particularly through the Digital Education Strategy 2025–2029, is a significant factor.[38] This makes the issue more urgent.

The lack of specific policies on:

- online risk prevention (cyberbullying, exploitation, exposure to inappropriate content),
- Digital citizenship education for children,
- and appropriate reporting mechanisms,

These constitute a significant gap in the overall framework of digital inclusion.

Senegal's digital inclusion is moving towards a more integrated approach, but it is still lacking, especially when it comes to safeguarding the most vulnerable users and effectively translating policies into quantifiable effects on the ground.

Universal Service Fund

The Universal Telecommunications Service Development Fund (FDSUT),[39] whose management, missions, and objectives are defined by Decree No. 2019-593 of February 14, 2019, aims to develop community telecommunications networks to bridge social inequalities and create conditions of equity.

As part of its policy to combat disparities between urban areas and underserved rural communities, Senegal has initiated collaborative models between operators, symbolised by infrastructure sharing and digital development across the country.

To this end, for the development of rural areas, the FDSUT has inaugurated the Living Lab.[40] It is now fully operational.[41] This project, with a total estimated budget of 60 million CFA francs,[42] also covers the regions of Kaolack, Saint-Louis, and Ziguinchor. Its objective is to introduce digital technology into the primary sector (Agriculture, Livestock, Fishing) through an innovation methodology based on the cooperation of public and private actors, companies, associations, and individual actors.[43]

33. https://www.education.sn/posts/le-senegal-engage-une-nouvelle-ere-educative-lancement-officiel-de-la-strategie-du-numerique-pour-leducation-2025-2029
34. https://paens.sn/2025/
35. https://cybersecuritymag.africa/le-senegal-installe-officiellement-un-conseil-national-du-numerique/
36. Senegal will have a digital identity in 2024.
37. Feasibility study of the national digital identity (INN) project:https://identitenumerique.sn/wp-content/uploads/2022/08/INN-Rapport-Final-inputs-MENT.pdf (Accessed on November 28, 2024).
38. https://www.education.sn/posts/le-senegal-accelere-la-transformation-numerique-de-son-education-signature-dun-partenariat-strategique-entre-le-men-et-le-mesri
39. https://fdsut.sn/salles-multimedias/ (Accessed on November 28, 2024).
40. Socioeconomic development of the terroirs: FDSUT inaugurates the Living Lab: https://fdsut.sn/category/living-glab/ (accessed on November 28, 2024).
41. Implementation of the operational phase of the living lab, August 22, 2024.
42. https://letechobservateur.sn/developpement-socioeconomique-des-terroirs-le-fdsut-inaugure-le-living-lab-de-ndangalma/ .
43. Living Lab FDSUT or Living Laboratory: https://fdsut.s/living-lab-fdsut-innovation-numerique-secteur-primaire/ (accessed November 28, 2024).
44. https://fdsut.sn/
45. http://www.jubanti.sn digital ministry
46. https://www.education.sn/posts/le-senegal-accelere-la-transformation-numerique-de-son-education-signature-dun-partenariat-strategique-entre-le-men-et-le-mesri

Conclusion

Senegal's evaluation under the **LONDA 2025** framework reveals a mixed but generally favourable development in the area of digital rights and inclusion. The overall score rises from **34 in 2024 to 38 in 2025,** indicating quantifiable growth, especially in the areas of government openness, internet access stability, and the reinforcement of specific legal protections.

The year 2025 stands out in particular for the absence of internet shutdowns, in contrast to previous years. This development, combined with the ECOWAS Court of Justice's condemnation of Senegal for the 2023 shutdowns, marks a significant turning point in the recognition of the fundamental nature of internet access.

It demonstrates a relative improvement in compliance with the principles of the Declaration of the African Commission on Human and Peoples' Rights.

However, these advances coexist with persistent challenges. The continued criminalisation of spreading false news, the lack of reform to sedition laws, and the arrests of journalists and the planned closure of media outlets in 2025 all point to the ongoing fragility of online freedom of expression. These factors indicate that institutional progress has not yet fully translated into practice.

Furthermore, although Senegal has a universal service mechanism and ambitious digital inclusion initiatives, particularly through the New Deal for Technology, significant limitations remain. The lack of transparency in the management of the Universal Telecommunications Service Development Fund (FDSUT) and the absence of detailed public data on its impact hinder a comprehensive assessment of the effectiveness of inclusion policies.

Finally, the lack of significant development in the legal framework for data protection and the protection of children online, as well as the inadequacy of specific policies on gendered disinformation, shows that certain essential dimensions of digital rights remain insufficiently taken into account.

Thus, Senegal is positioned in **2025 within a dynamic of moderate but incomplete progress,** characterised by significant strategic and institutional advances, but hampered by inconsistencies between the regulatory framework and its effective implementation. Consolidating these gains will require targeted legal reforms, greater institutional transparency, and a strengthening of mechanisms for protecting fundamental rights in the digital space.

Recommendations

The Government should:

- Revise the provisions of the Penal Code relating to the dissemination of false news, sedition and opinion offences to align them with Principle 22 of the Declaration of the African Charter on Human and Peoples' Rights (ACHPR).
- Establish a clear legal framework that complies with human rights to govern any restriction of internet access, incorporating the standards of legality, necessity and proportionality.
- Strengthen transparency in the management of the Universal Telecommunications Service Development Fund (UTSDF), in particular through the regular publication of detailed reports, including the amounts collected, the projects financed and their impact.
- Accelerate the revision of the law on the protection of personal data to align it with international standards and strengthen the powers of the regulatory authority.
- Develop and adopt a national strategy dedicated to the protection of children online, including mechanisms for prevention, education and reporting of abuse.
- Establish mechanisms for monitoring and publishing data related to arrests and prosecutions linked to online expression in order to strengthen accountability.

For the attention of the media

- Strengthening journalists' capacity in digital rights, fact-checking and coverage of issues related to disinformation.
- Promote ethical practices in online information processing in

- order to limit the risks associated with the dissemination of sensitive or unverified content.
- Develop initiatives to raise public awareness about digital rights and freedom of expression.

For the attention of the Private Sector (digital operators and platforms)

- Improve transparency in content moderation practices, including by publishing detailed reports on content removal requests from public authorities.
- Strengthen mechanisms to protect users, especially women and children, against online harassment and disinformation.
- Collaborating with authorities and civil society to develop solutions promoting affordable and inclusive access to the Internet.

To the attention of Civil Society

- Intensify advocacy for reform of laws restricting freedom of expression online.
- Strengthen initiatives to monitor and document violations of digital rights, including arrests, cases of censorship and breaches of privacy.
- Develop digital education programmes targeting vulnerable populations, including women, youth, and people living in rural areas.
- Promote research and the production of independent data on the impact of digital policies, particularly in terms of inclusion and universal service.

The Score Index

Senegal, 2025

1. Totally non-compliant. 2. Slightly compliant: This is a slight attempt at compliance with critical deficiencies. 3. Moderately compliant – where there are areas for improvement. 4. Largely compliant – Minimal areas for reform. 5. Fully compliant – No issues

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Internet Shutdowns	P38(2)	1	4	No internet outages in 2025 Senegal was condemned by the ECOWAS Court of Justice on May 14, 2025, for internet shutdowns during the period of electoral tension.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	3	3	In Senegal, the Universal Telecommunications Service Development Fund (FDSUT)[44]This constitutes the main funding mechanism for universal access to digital services. However, despite the existence of this institutional framework, transparency regarding the use of the fund's resources and the impact of funded projects remains limited, which restricts the effective assessment of its contribution to bridging the digital divide.
Criminalizing fake news	P22(2)		1	Spreading false news is considered an offense. Article 255 of Law No. 77-87 of August 10, 1977, amending the Penal Code of 1965. The rating remains in place because many arrests of journalists and columnists have been motivated by this offense.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Legislation on sedition	P22(2)	3	3	Articles 181 and 183 of the Penal Code refer to sedition, while according to Principle 22(2), states shall repeal laws that criminalise sedition, insults, and the publication of false news. The rating remains unchanged because there has been no evolution or development in that direction.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	3	1	In 2025, despite a new government that brought much hope, the Ministry of Communication, through a decree, closed 381 media outlets, and more than 4 journalists were arrested for defamation or opinion offences.
Data Protection Legislation.	P42	4	4	Data protection legislation has existed since 2008. A bill has existed since 2019 which brought major innovations, including the creation of a Personal Data Protection Authority (APDP). The rating remains unchanged as there are no new developments regarding this law. However, many problems justify its revision.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	2	3	We are seeing a strengthening of freedom of expression and access for opposition parties to state media. The state is not removing content but has still shut down some media outlets.
Invasion of Privacy of Communications	P41	4	4	Senegal protects privacy and the confidentiality of communications through the Constitution and the law on the protection of personal data. Privacy protection is particularly strengthened in the digital sphere. People are more sensitive to the concepts of image rights and consent, and no cases of state surveillance have been reported.
Failure by the government to proactively disclose and disseminate information on digital technologies.	P29(3)	4	4	The new government proactively discloses and disseminates information of public interest, including functions, powers, structure, officials, decisions, budgets, and expenditures, in the interest of transparency. There has been an improvement in the transparency of public information. The government has implemented digital platforms for consultation and contribution. www.jubanti.sn[45] for major reforms. Law No. 2025-15 on access to information in Senegal was promulgated on September 25, 2025, after 15 years of advocacy. It enshrines the right of any individual or legal entity to access public data held by public entities and certain private entities, thereby strengthening transparency, democracy, and the fight against corruption.
AI and Emerging	P39(6)	3	3	Senegal has a draft national strategy on artificial intelligence (AI). With the launch of the New Deal for Technology,

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Technologies national strategies				the role of AI in the digital transformation of public services is more visible, with an AI strategy structured around urgent needs such as education, health, training, and notably the strengthening of the AI workforce with 100,000 people trained in AI.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	4	4	No major legislative changes specifically dedicated to the protection of children online have been formally identified. However, the increased integration of digital tools into the education system, particularly through the Digital Education Strategy 2025–2029, is a significant development.[46]
Digital Inclusion	P37(3)	4	4	The State of Senegal has adopted laws, policies, and other measures to guarantee universal, equitable, and affordable access to the internet, without discrimination. The government is making considerable efforts to digitise educational curricula. Internet coverage is almost universal, even in rural areas.
Total (out of 60):	2024: **34**	2025 **38**		

Somalia

By Ayaan Khalif and Abdifatah Ali

Executive Summary

In 2025, Somalia's digital ecosystem was shaped by rapid expansion and growing complexity, with significant developments across key thematic areas including internet access; freedom of expression and access to information; data protection and cybersecurity; privacy and surveillance; censorship and content moderation; digital inclusion and AI; and emerging technologies. Internet connectivity has expanded at an unprecedented pace, driven largely by mobile broadband growth and the introduction of satellite internet services, accelerating Somalia's transition toward mass connectivity. However, governance frameworks, institutional oversight, and rights protections have not evolved at the same rate. Using The Score Index[1], developed by Paradigm Initiative and grounded in the principles described in the African Commission on Human and Peoples' Rights' Declaration of Principles on Freedom of Expression and Access to Information.[2] Somalia scores

32 out of 60 in 2025, reflecting modest progress from the previous assessment while highlighting persistent gaps in enforcement, accountability, and equitable access. Key challenges remain in data protection implementation, platform governance, surveillance safeguards, and meaningful digital inclusion. Alongside emerging risks linked to AI adoption in the absence of finalized regulatory frameworks. The report recommends strengthened enforcement of existing digital laws, finalization of the National AI Strategy with human rights safeguards, integration of digital inclusion targets into national development planning, enhanced platform accountability and transparency, expanded public–private partnerships for connectivity, and a stronger role for civil society and the media in monitoring rights violations, promoting access to information, and advancing digital literacy and public-interest advocacy.

Introduction

Since 2016, Somalia's digital landscape has undergone a profound transformation. At that time, internet access was extremely limited, largely confined to major urban centers, with weak infrastructure, minimal regulatory oversight, and low levels of digital adoption. Over the years, sustained private-sector investment and increased demand for mobile services have driven rapid expansion, making mobile internet and mobile money central to everyday communication, commerce, and service delivery. By 2025, Somalia had moved from fragmented connectivity toward mass internet adoption. A notable shift in this trajectory occurred in 2025 when Starlink[3] received regulatory approval to operate in Somalia, introducing satellite-based internet services that were non-existent in previous years. While satellite internet remains unaffordable for most households and is not yet a widespread solution, its entry into the market signals a diversification of connectivity options and a new phase in Somalia's digital infrastructure development.

At the governance level, Somalia has articulated growing policy ambition, including the adoption of national digital strategies and sectoral regulations. Yet enforcement remains inconsistent, and institutional capacity continues to lag behind the expanding influence of global technology platforms and domestic telecom operators. Issues such as data protection, cybersecurity, content moderation and surveillance are increasingly salient, particularly as digital tools become embedded in governance, elections, service delivery, and public debate. This report moves beyond access metrics to examine the structural conditions shaping online freedoms, inclusion, and accountability. By doing so, it seeks to contribute to evidence-based discussions on how Somalia can balance rapid digital growth with the protection of fundamental rights in 2025 and beyond.

1. The Score Index framework: https://paradigmhq.org/londa-score-index/
2. The principles described in the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information: https://achpr.au.int/en/node/902
3. Starlink in Somalia: https://spaceinafrica.com/2025/04/13/somalia-grants-operational-license-to-starlink-expanding-internet-access-across-the-nation/

Internet Access And Disruptions

Somalia's digital ecosystem in 2025 was defined by speed. Internet access has expanded at an unprecedented rate, reshaping how citizens communicate, access services, participate in civic life and engage with the state. National internet penetration has doubled, from 27.6% in early 2024[4] to approximately 55% in 2025. Over the past year, connectivity shifted from being a privilege for urban populations to an increasingly mainstream service, although deep inequalities persist. Internet access is now central to civic participation, economic activity, access to information and the broader digital rights landscape in the country.

As of early 2025, Somalia has an estimated 10.7 million internet users.[5] Representing approximately 55% of the population, this growth has been largely driven by the widespread availability of mobile broadband, with most users accessing the Internet through smartphones using 3G and 4G LTE networks. With 11.3 million cellular mobile connections[6] in a population of 19.3 million, mobile usage is extensive. Fixed broadband remains limited, meaning that mobile internet continues to serve as the primary gateway to the digital space for most Somalis. Infrastructure developments have also shaped this expansion. Local telecommunications companies have continued to invest in network coverage, particularly in major urban centers such as Mogadishu, Hargeisa, and Garowe.

Despite these gains, digital literacy gaps, unreliable electricity supply and limited regulatory enforcement further constrain meaningful access.[7] Recognising these challenges, the Federal Government of Somalia has articulated a Digital Transformation Strategy (2025–2030), emphasising expanded infrastructure, digital public services and inclusive access as pillars of national development.[8] How these commitments translate into equitable rights respecting internet access remains a critical issue for governance and accountability in 2025 and beyond. Similar to 2024, Somalia did not experience any nationwide, government-imposed internet shutdowns in 2025. While earlier periods were marked by instability and infrastructure related connectivity disruptions, these were not the result of deliberate nationwide shutdowns. However, there have been targeted platform restrictions, such as the 2023 bans[9] on Telegram, TikTok, and 1xBet, which illustrate selective censorship that could disrupt certain forms of digital engagement and civic communication.

Freedom of Expression and Access to Information in Somalia

Freedom of expression remained under sustained pressure in 2025, affecting both physical and digital spaces. While the Provisional Constitution[10] guarantees the right to freedom of expression and access to information, the practical exercise of these rights continues to be constrained by restrictive legal frameworks, security driven enforcement practices, and weak institutional safeguards for media independence.

2025 saw notable institutional developments with potential implications for the protection of human rights, including freedom of expression. On July 3 2025, the Somali Cabinet approved nine members of the National Independent Human Rights Commission (NIHRC)[11], advancing the long delayed operationalisation of a constitutional oversight body. This process was further consolidated on December 10 2025, when the President of Somalia signed into law the establishment of the Independent National Human Rights Commission, formally granting it a legal mandate[12]. The presidential endorsement

4. Internet penetration in 2024: https://datareportal.com/reports/digital-2024-somalia
5. Number of internet users in Somalia: https://datareportal.com/reports/digital-2025-somalia
6. Mobile connections in Somalia 2025: https://datareportal.com/reports/digital-2025-somalia
7. Digital literacy and inclusion gaps – Hivos Somalia Country Focus Report: https://eusee.hivos.org/assets/2025/11/Somalia-Country-Focus-Report.pdf
8. Digital Inclusion Policy: https://moct.gov.so/en/wp-content/uploads/2025/08/Somalia-Digital-Inclusion-Policy_High-Level-Policy-document.pdf
9. The 2023 Somalia platforms ban: https://www.aljazeera.com/news/2023/8/26/outcry-in-somalia-over-government-decision-to-ban-tiktok-telegram
10. The Provisional Constitution of the Federal Republic of Somalia 2012: https://www.wipo.int/wipolex/en/legislation/details/14305
11. National Independent Human Rights Commission (NIHRC): https://sonna.so/en/somali-cabinet-approves-nine-candidates-for-national-independent-human-rights-commission/
12. Signing the law of the Independent National Human Rights Commission: https://www.hiiraan.com/news4/2025/

coincided with Somalia's commemoration of International Human Rights Day, situating the enactment within the broader context of national human rights observances. While these steps represent progress compared to previous years, the extent to which the NIHRC will meaningfully protect freedom of expression and access to information will depend on its independence, resourcing, and ability to act without political interference.

The legal and regulatory environment governing media practice continues to shape the operating conditions for journalists. Somalia's Media Law of 2019, amended in 2020[13], remains the principal framework regulating broadcast and print media. However, the law has consistently failed to comply with international standards on freedom of expression, and the amended version did little to address these shortcomings. Key concerns include provisions that criminalise expression and aspects of the journalism profession itself, restrictive criteria determining who may practice journalism, and the imposition of state-dictated ethical guidelines. The law also raises serious questions regarding the independence and composition of the Somali Media Council, as well as the judicial prosecution of vaguely defined media offences. Provisions relating to the issuance of press cards and the imposition of undetermined fines on journalists and media organisations further entrench state control.[14]

In 2025, journalists continued to face arbitrary interference in the performance of their professional duties. Monitoring reports produced by Safe Reporters of Somalia (SRS) documented multiple incidents throughout the year involving intimidation, short-term detention, obstruction, and the confiscation of journalists' electronic devices by security agencies and local authorities.[15] These incidents were recorded across several months, indicating a recurring pattern rather than isolated events. Such practices, often implemented without formal charges or judicial oversight, contribute to self-censorship and undermine journalists' ability to report freely, particularly on governance, security, and accountability issues.

Media institutions, especially community and regional outlets, also remained vulnerable to administrative restrictions. In 2025, Radio Marka, a local radio station serving communities in Lower Shabelle, announced a temporary suspension of operations[16] following pressure and restrictions imposed by authorities. The suspension illustrates the fragile operating environment for independent media at the subnational level, where radio remains a primary source of information for the public. Actions against media outlets are frequently carried out without transparent procedures or effective avenues for appeal, thereby undermining media pluralism and limiting access to diverse viewpoints.

The Official Information Bill (OIB), approved by the Council of Ministers in 2024[17], remained pending parliamentary consideration throughout 2025. As a result, Somalia continues to lack a dedicated legal framework governing access to public information. The prolonged delay has sustained uncertainty around information governance and limited opportunities for public scrutiny of state action. In the absence of parliamentary debate and approval, constitutional provisions have not been translated into operational mechanisms accessible to journalists, civil society organisations, or the wider public.

Public debate on the Bill continued during the year, including reflections from policy actors involved in its early development. In a public commentary published after leaving office, a former National Security Advisor underscored the importance of passing an access to information law while cautioning against provisions that could undermine transparency or expand discretionary secrecy.[18] These perspectives echo broader concerns raised by media and civil society actors regarding vague exemptions, weak safeguards

Dec/203885/somali_president_signs_law_establishing_independent_national_human_rights_commission.aspx

13. AmendedSomalia's Media Law: https://sonna.so/en/the-president-of-fgs-signs-into-law-somalia-media-law/ (Accessed on
14. Statement on the amended media law: https://nusoj.org/2020/08/26/statement-on-the-amended-media-law-signed-by-the-president-of-somalia/
15. Monitoring reports produced by Safe Reporters of Somalia (SRS): https://srssomalia.org/wp-content/uploads/2025/11/SRS-QUARTERLY-REPORT-2.pdf
16. Temporary suspension of Radio Marka: https://en.kaabtv.com/marka-fm-somalia-announces-temporary-suspension-of-operations/
17. Criticism on the Information Bill: https://shabellemedia.com/somalias-democracy-at-risk-global-outcry-over-official-information-bill/
18. Commentary published after leaving office, a former National Security Advisor: https://husseinsheikhali.substack.com/p/why-somalia-must-pass-the-official

against abuse, and the risk of discouraging legitimate information-seeking.

The developments observed in 2025 indicate limited progress in strengthening freedom of expression in Somalia. The persistence of restrictive legal provisions, combined with documented patterns of arbitrary enforcement and insufficient safeguards for journalists' physical and digital security, underscores enduring gaps between constitutional guarantees and lived realities. Without reforms to ensure independent regulation, due process, and alignment with regional and international human rights standards, freedom of expression remains fragile and unevenly protected nationwide.

Data Protection and Cybersecurity

In 2025, Somalia's data protection and privacy landscape reflected measured legal and institutional progress alongside persistent implementation challenges. The Data Protection Act, enacted in March 2023[19] remains the country's primary legal framework governing the collection, processing, and protection of personal data across public, private, and non-profit sectors. The Act establishes core rights for data subjects, including the rights to access, rectify, delete, and object to the processing of personal data, as well as safeguards against certain forms of automated decision making. It also imposes obligations on data controllers and processors to implement appropriate security measures, conduct risk assessments, and notify the relevant authorities of data breaches. The Data Protection Authority continued its institutional establishment phase. Efforts focused on developing and implementing regulations, engaging legal and technical expertise, and initiating awareness activities aimed at public and private institutions. While these steps demonstrate progress toward operationalisation, enforcement capacity remains limited. In practice, institutions continue to face challenges in interpreting and applying the law, compounded by limited access to practical guidance and regulatory materials necessary for compliance.

Alongside these challenges, steps have been taken to strengthen technical capacity related to data security and cyber resilience. The National Communications Authority (NCA) is actively working on strengthening national cybersecurity and launched the Global ACE Cybersecurity Certification with SIMAD University and CyberSecurity Malaysia[20] which aligns the establishment of SomCIRT[21], a national Computer Emergency Response Team, to improve incident response and coordination. While these initiatives contribute positively to the broader data protection ecosystem, their effectiveness will depend on coordination with the Data Protection Authority, transparency, and the development of accessible compliance guidance.

19. 2023 Data Protection Act: https://moct.gov.so/en/wp-content/uploads/2023/07/Somalia-Data-Protection-Act-2.pdf

Privacy and Surveillance

In late 2025, a serious security breach of Somalia's newly launched e-visa platform exposed the personal data of thousands of visa applicants, with at least 35,000 records compromised[22]. This breach raised questions about governance, accountability and the protection of sensitive personal information collected through digital public services. Concerns about data privacy also extended to the rollout of Somalia's national ID system. Public debate in 2025 highlighted fears over the storage and handling of personal information associated with the new National Identification and Registration Authority (NIRA) IDs[23], including uncertainty about who manages, accesses, and stores personal data. Some members of the public expressed distrust over the lack of transparency around data management practices, especial

20. Launch of Global ACE certification: https://nca.gov.so/nca-and-simad-university-launch-global-ace-cybersecurity-certification-in-somalia/
21. SomCIRT: https://somcirt.gov.so/
22. The 2025 E-Visa breach: https://www.aljazeera.com/news/2025/12/18/new-somalia-evisa-security-puts-passport-details-of-thousands-at-risk
23. Concerns on the new National Identification system: https://garoweonline.com/en/news/somalia/somalia-s-new-national-id-system-raises-data-privacy-fears

ly where data might be stored abroad.

While comprehensive data on formal state surveillance powers in 2025 are sparse, civil society reporting indicates that digital harassment and interference with journalists' communications were serious issues. Women journalists and media workers faced online attacks and content censorship, these cases reflect how content moderation and account management can have the effect of silencing journalists' digital expression, intersecting with privacy implications for individuals who rely on online platforms for their work.[24]

Censorship and Content Moderation

Censorship and content moderation practices in Somalia continued to pose challenges to freedom of expression, particularly for journalists and media workers. Evidence documented by the National Union of Somali Journalists (NUSOJ) shows that authorities repeatedly interfered with journalistic content through intimidation, arrests, and pressure to censor or remove reporting[25]. These actions contributed to a restrictive environment in which journalists faced reprisals for publishing critical content, reinforcing widespread self censorship. NUSOJ noted that such measures were often justified on national security grounds, yet were implemented without adequate transparency or judicial safeguards, raising concerns about compliance with international standards on freedom of expression.

Content moderation on digital platforms also emerged as a growing concern, especially for women journalists. The Somali Media Women Association (SOMWA) reported an increase in censorship and online restrictions targeting women journalists[26], including the suspension or disabling of social media accounts used for professional reporting and public engagement. These actions directly limited journalists' ability to disseminate information, engage audiences, and maintain visibility in public discourse. SOMWA highlighted that the lack of clarity around content removal or restricted accounts intensified fear and uncertainty, further discouraging free expression online.

Available evidence indicates that censorship in Somalia during 2025 was characterised not by nationwide internet shutdowns, but by targeted and inconsistent practices affecting media content and online expression. The combined impact of state pressure on journalistic content and opaque platform level moderation continued to restrict civic space, particularly for journalists who rely on digital platforms as primary tools for reporting and communication.

AI and Emerging Technologies

Somalia's engagement with artificial intelligence (AI) and emerging technologies has progressed significantly from informal experimentation toward institutional development and strategic planning, moving from early AI exploration toward structured ecosystems supported by government institutions, strategy development, academic engagement, and international involvement. These developments mark a significant shift from earlier years when AI discussion was largely academic or ad hoc, but realising the full socio-economic and governance potential of emerging technologies will require stronger regulatory mechanisms, ethical safeguards, and implementation strategies. In 2025, Somalia advanced this momentum with the development of a National AI Strategy (2025–2030) intended to guide implementation, regulation, and cross sector AI adoption, although the final strategy document is still being formalised within broader digital policy frameworks, such as the Digital Transformation Strategy (2025–2030)[27]. Consultations on national digital policy, supported by the Ministry of Communications and Technology (MoCT) and the National Communications Authority (NCA) in collaboration with the International Telecommunication Union (ITU), reflect increased alignment of AI planning with national development priorities.

On the global stage, Somalia has actively participated in international discussions on AI ethics, including the 3rd Global Fo

24. Content censorship on media workers: https://allafrica.com/stories/202509160087.html
25. National Union of Somali Journalists: https://nusoj.org/2025/09/15/no-democracy-without-media-freedom-in-somalia-nusoj-says/
26. Censorship and online restrictions targeting women journalists: https://somwa.org/the-somwa-report-warns-of-rising-attacks-censorship-and-discrimination-against-women-journalists-in-somalia/
27. Digital Transformation Strategy (2025–2030): https://nca.gov.so/somalia-launches-national-consultation-on-the-digital-transformation-strategy-2025-2030/

rum on the Ethics of Artificial Intelligence co-hosted by UNESCO[28], where Somali officials engaged in dialogues on ethical AI governance and readiness assessments, noting Somalia's selection among countries to pilot UNESCO's AI governance readiness tools, a significant step toward aligning national efforts with global ethics frameworks. Additionally, UNESCO's call for a Lead National Expert to support implementation of the UNESCO Recommendation on the Ethics of AI[29] signals early movement toward integrating ethical principles into national AI governance structures.

Alongside the institutional growth is the establishment of the Somalia National AI Center (SNAIC)[30], a government-affiliated body dedicated to AI research, innovation, capacity building, and policy advisory functions. Local ecosystem development is further supported by community initiatives like AI Somalia[31], which champions AI training, workshops, and talent development in collaboration with universities and industry partners. Academic engagement is also expanding, with the SIMAD AI Institute[32] at SIMAD University becoming a national hub for AI research and education, a development that was not present in prior years.

Emerging technologies beyond AI, such as blockchain, virtual reality (VR), facial recognition technologies (FRTs), and similar innovations, are not yet widely deployed or regulated in national policy, though discussions around technology cooperation including a collaboration framework with Saudi Arabia on AI and space technologies indicate an expanding scope for future technology governance and infrastructure cooperation.[33]

28. Somalia's selection among countries to pilot UNESCO's AI governance readiness tools: https://sonna.so/en/somalia-participates-in-3rd-global-forum-on-the-ethics-of-artificial-intelligence/
29. UNESCO'S call for Lead National Expert for Somalia: https://www.unesco.org/en/articles/call-expression-interest-lead-national-expert-somalia-unesco-regional-office-eastern-africa-social
30. Somalia National AI Center: https://snaic.gov.so/
31. AI Somalia Community: https://aisomalia.ai/
32. SIMAD AI Institute: https://ai.simad.edu.so/
33. Somalia and Saudi Arabia Partner to Advance AI and Space Technology: https://sonna.so/en/somalia-and-saudi-arabia-partner-to-advance-ai-and-space-technology/

Digital Inclusion

In 2025, Somalia's digital inclusion agenda gained significant policy traction and multi-stakeholder engagement, yet persistent gaps continue to shape how equitably people can participate in the digital society. A major milestone early in the year was the formal approval of the Somalia Digital Inclusion Policy and the Accelerated Governance Strategy by the Federal Government's Council of Ministers.[34] This landmark policy explicitly targets long-standing barriers to equitable ICT access, focusing on affordability, infrastructure expansion, digital literacy, and targeted outreach to marginalised groups, including women, youth, rural populations, and persons with disabilities. Its objectives include improving access to affordable and reliable internet services, enhancing digital skills development, and ensuring that underserved communities can benefit from digital tools and services.

Complementing this policy, the National Communications Authority (NCA) has undertaken outreach and capacity-building initiatives to promote digital inclusion in concrete ways. NCA hosted Universal Acceptance Day 2025 in Mogadishu, a multi-stakeholder event aimed at ensuring that all valid domain names and email addresses are usable across internet-enabled systems.[35] This technical focus on inclusivity highlights the importance not just of connectivity but of an internet environment that is accessible, locally relevant, and linguistically diverse.

Digital inclusion efforts are also reflected in Somalia's broader digital governance landscape. The Digital Transformation Strategy (2025–2030), currently under national consultation with partners like the International Telecommunication Union (ITU) underscores inclusive growth and capacity development as strategic pillars.[36] These consultations emphasise the need for coordinated policies to expand infrastructure, build human capital, and foster public–private partnerships that support participation in the digital

34. Digital Policy and the Accelerated Governance Strategy:https://moct.gov.so/en/the-council-of-ministers-approves-the-inclusive-digital-policy-and-the-accelerated-governance-strategy-mogadishu-somalia-23rd-january-2025
35. Universal Acceptance Day: https://nca.gov.so/nca-hosts-universal-acceptance-day-to-promote-digital-inclusion/
36. Consultation Workshop to validate Somalia's Digital Transformation Strategy (2025–2030): https://nca.gov.so/somalia-launches-national-consultation-on-the-digital-transformation-strategy-2025-2030/

economy.

On the ground, partnerships between private sector actors and humanitarian organisations are helping to extend inclusion beyond traditional access metrics. A notable example is the strategic collaboration between Hormuud Telecom and Save the Children Somalia, which aims to increase digital literacy and connectivity for children and their families in underserved areas.[37] The initiative focuses on using mobile technologies to improve education, health messaging, emergency communication, and youth empowerment.

Somalia does not currently have a standalone child online protection law that explicitly criminalises child exploitation, cyberbullying, online abuse, or other child-specific harmful conduct in the digital environment. However, earlier ICT policy frameworks such as the National ICT Policy Strategy (2019–2024)[38] recognised the need for child online protection measures, though these were largely aspirational and not codified into law. The government has committed to drafting a new, comprehensive ICT policy within the next two years, which is expected to explicitly address consumer and child protection policy.[39] However, this commitment, which was set out in a policy document whose term ended in 2024, has not been implemented.

Despite these advances, structural barriers remain. Independent assessments note that rural communities, women, persons with disabilities, and linguistic minorities still experience lower levels of meaningful access due to infrastructure gaps, high data costs, and limited digital skills. While connectivity has improved, the utility and impact of access are uneven, and many citizens lack the training and capacity to use digital tools effectively for education, employment, and civic engagement.[40]

37. Hormuud Telecom and Save the Children Somalia MoU: https://hormuud.com/blog/hormuud-telecom-partners-with-save-the-children-somalia-to-bridge-digital-divide
38. National ICT Policy Strategy: https://moct.gov.so/en/wp-content/uploads/2019/11/National-ICT-Policy-Strategy-2019-2024.pdf
39. Strategic goals on consumer and child protection policy on page 17: https://moct.gov.so/en/wp-content/uploads/2019/11/National-ICT-Policy-Strategy-2019-2024.pdf
40. Independent assessments: https://eusee.hivos.org/assets/2025/07/Somalia-EE-baseline-snapshot-1.pdf

Universal Service Fund

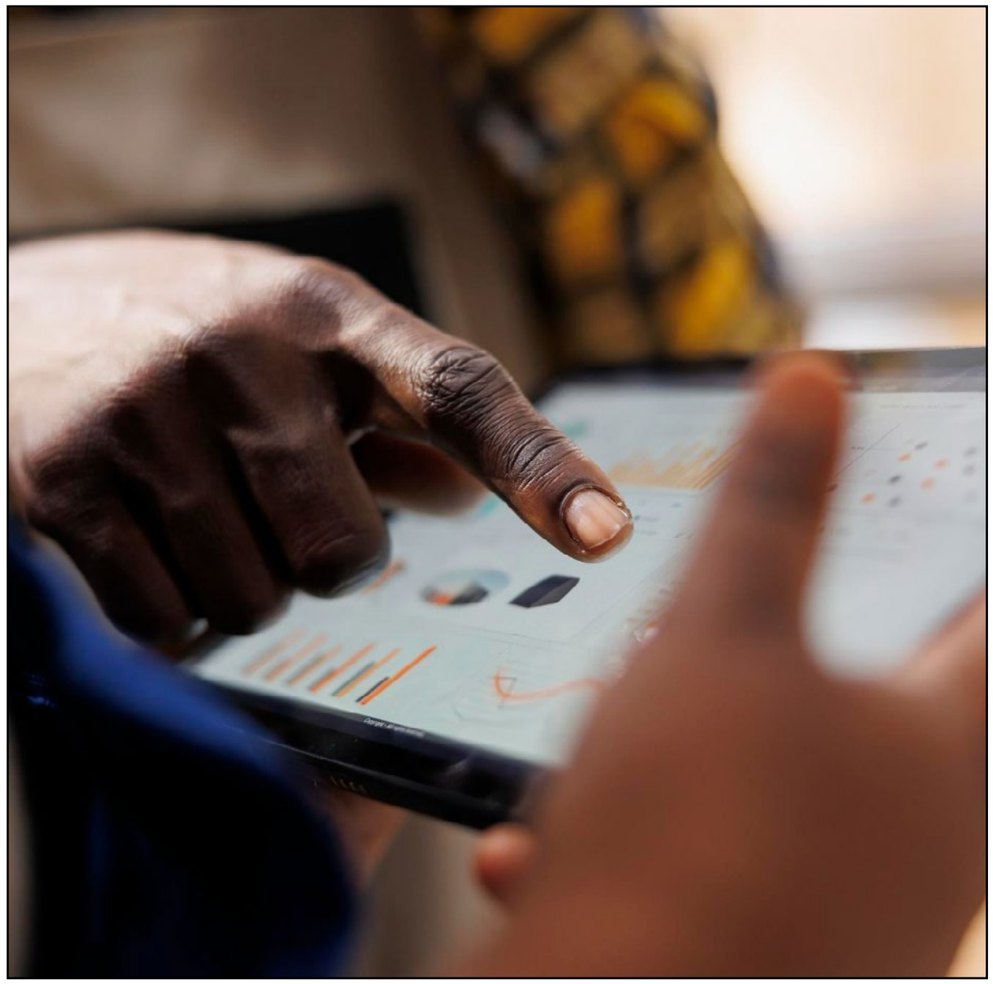
Somalia does not yet have an operational Universal Service Fund (USF) or a formally established Universal Access Fund dedicated to subsidising connectivity in underserved and rural areas, a mechanism that many countries use to bridge digital access gaps. The principle of universal service appears in Somalia's historical ICT policy frameworks and regulatory strategy documents, which outline the need for ensuring broadband and voice services reach underserved populations.[41] These policy documents define a Universal Access Fund (UAF) concept intended to support ICT access in rural and underserved areas, but they do not indicate that an active fund has been operationalised or financed.

Conclusion

Somalia's digital trajectory in 2025 reflects meaningful progress alongside persistent structural challenges. Rapid growth in internet access, emerging frameworks for AI and other technologies, and a rise in the Score Index to 32 out of 60 highlight the potential of aligned policy, market innovation, and multi-stakeholder engagement. Yet, progress remains uneven, connectivity has outpaced governance, leaving gaps in enforcement, accountability, and rights protection, while digital inclusion for women, rural communities, persons with disabilities, and other marginalised groups remains inconsistent. Institutional developments such as the Somalia National AI Centre, the Digital Transformation Strategy (2025–2030) and the drafting of the National AI Strategy (2025–2030) show ambition, but their impact will depend

41. The principle of universal service: https://moct.gov.so/en/wp-content/uploads/2025/08/Somalia-Digital-Inclusion-Policy_High-Level-Policy-document.pdf

on embedding ethical safeguards, data protection, and human rights from the outset. Somalia's digital future will hinge on bridging policy and practice, investing in inclusive infrastructure and skills, and establishing enforceable rights-based frameworks, with sustained collaboration between government, regulators, civil society, the private sector, and international partners essential to ensure a resilient, equitable, and democratic digital ecosystem.



Recommendations

The Government should:

- Strengthen enforcement of existing digital laws, particularly data protection and cybersecurity frameworks, by allocating resources to regulatory bodies and establishing independent oversight mechanisms.
- Finalise and implement the National AI Strategy (2025–2030) with explicit human rights safeguards, including principles on transparency, accountability, non-discrimination, and responsible data use.
- Integrate digital inclusion indicators into national development and ICT policies, ensuring women, youth, persons with disabilities and displaced communities are explicitly targeted.
- Develop a national framework for platform accountability, including transparency reporting requirements for content moderation requests made to social media and digital platforms.
- Ensure that emerging technology and AI policies incorporate freedom of expression and privacy-by-design principles, preventing surveillance-driven or discriminatory deployment.
- Promote access to information by enforcing transparency obligations for public institutions, digitising public records, and ensuring online access to government information in accessible formats and local languages.
- Adopt a dedicated child online protection law that criminalises online exploitation, abuse, and harmful content targeting children, complemented by regulatory mechanisms to ensure enforcement, platform accountability, and nationwide digital literacy programs for children, parents, and educators.

The Private Sector should:

- Publish regular transparency reports detailing content moderation actions, data requests, and network disruptions affecting users in Somalia.
- Expand network coverage beyond commercially viable urban centres by partnering with government and development actors through public–private partnerships.
- Support local innovation ecosystems by investing in skills development, research, and incubation programs, particularly in AI, digital services, and content creation.
- Engage constructively in policy dialogue and regulatory processes to ensure commercial innovation aligns with public interest and human rights obligations.

Civil Society Organisations should:

- Invest in research and storytelling that centres local realities and lived experiences, amplifying Somali voices in regional and global digital policy spaces.
- Advocate for inclusive implementation of national ICT and AI policies, ensuring affected communities are meaningfully involved in decision-making processes.
- Promote access to information initiatives, including open data advocacy, digital archiving, and public-interest technology projects.
- Build digital rights literacy among journalists, activists, women, and youth to strengthen safe, informed participation in online civic spaces.

The Media:

- Monitor, document, and publicly report violations of freedom of expression, including arrests for online speech, content takedowns, and platform restrictions.
- Strengthen investigative and independent reporting while adhering to ethical standards, ensuring transparency and accountability in news coverage.
- Engage in public awareness campaigns to educate citizens about their digital rights, access to information, and safe online practices.

The Score Index

Somalia, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	3	4	Somalia has not experienced government imposed nationwide internet shutdown in 2025 and 2024. Past connectivity challenges in the country were largely driven by political instability and fragile telecommunications infrastructure, rather than deliberate state mandated restrictions on internet access.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	2	3	Somalia has made progress by adopting legal and policy frameworks such as the Digital Inclusion Policy (2025), the Digital Transformation Strategy (2025–2030), these measures are still in early stages of implementation and enforcement remains limited
False News Criminalisation	P22(2)	2	2	False news criminalisation remains a concern due to legal provisions that criminalise expression under vaguely defined offences and are enforced through security driven practices. The absence of clear definitions and safeguards enables discretionary application, contributing to self-censorship among journalists and media actors.
Sedition Legislation	P22(2)	2	2	The Somali Penal Code contains specific provisions that criminalise sedition, which the report identifies as a significant restriction on freedom of expression. While these laws are intended to maintain public order, their wording is often “vague,” which frequently leads to misuse by authorities.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	2	2	Monitoring reports from Safe Reporters of Somalia (SRS) in 2025 documented multiple incidents of intimidation, detention, and obstruction by security agencies and local authorities. Security forces frequently targeted journalists through the confiscation of their electronic devices which were carried out without formal charges or judicial oversight.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Data Protection Legislation.	P42	4	4	Somalia enacted the Data Protection Act and established a dedicated Data Protection Authority (DPA) to safeguard individual privacy. In 2025 these foundational legal achievements are being integrated as core pillars of the country's 2025–2030 Digital Transformation and National AI strategies to ensure a rights based technological future.
Online Content Removal by Government	P38 and P39(4)	2	3	Somalia is refining its approach to digital governance, while the government has actively enforced content takedowns in politically sensitive situations, these actions are now being integrated into the broader Digital Transformation Strategy (2025–2030) and the National AI Strategy.
Invasion of Privacy of Communications	P41	2	2	The ongoing use of surveillance cameras without clear oversight mechanisms has impacted public trust and while the government aims for a rights based future, the current lack of specific, comprehensive surveillance laws means there are still no strong legal safeguards against unauthorised monitoring
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	3	3	Government disclosure remained limited in 2025 due to the continued absence of an operational access to information framework. Although the Official Information Bill was approved by the Council of Ministers in 2024, it remained pending before Parliament throughout 2025, leaving Article 32 of the Provisional Constitution unimplemented and restricting access to state held information, including on digital matters.
AI and Emerging Technologies national strategies	P39(6)	2	3	Somalia has taken important steps with the development of the National AI Strategy (2025–2030) and the establishment of the Somalia National AI Center (SNAIC) to coordinate AI research, innovation, and capacity building. While these frameworks mark progress toward a structured approach, the strategy is still in progress, gaps remain in implementation, ethical oversight, and sector specific adoption, meaning that the full potential of AI for economic growth, public service improvement, and societal benefit is still emerging.
Adoption of specific child laws, policies and measures promoting children's	P39(6)	1	1	Child online protection remains insufficiently addressed within Somalia's digital policy and regulatory landscape. Despite growing internet use among children, there is no comprehensive, child specific legal or policy framework to safeguard them online.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
digital safety and privacy online				Existing commitments have not been operationalised, and government led measures to address risks and exposure to harmful content remain limited. While civil society actors have played a role in raising awareness around child digital safety, these efforts have yet to translate into coordinated government action or a national child online protection framework.
Digital Inclusion	P37(3)	2	3	Somalia has made notable progress in digital inclusion, marked by the adoption of the Digital Inclusion Policy (2025), steps toward the Digital Transformation Strategy (2025–2030), establishment of the Somalia National AI Center (SNAIC) to coordinate research and innovation and targeted programs to expand connectivity, digital literacy, and access, reflecting a more systematic approach to equitable access. However, challenges remain in infrastructure, implementation, rural coverage, access for persons with disabilities and meaningful utilisation of digital services, highlighting areas for continued investment and implementation.
				50 major towns. Furthermore, the move challenged the longstanding duopoly of the state-owned Mobile Telecommunications Company (MTC) and Telecom Namibia, introducing new competitive dynamics that could benefit coverage expansion and service quality.
Total (out of 60):	2024: **27**		2025 **32**	

Somalia's total score for 2025 stands at 32 out of 60, reflecting measurable progress in the digital rights landscape compared to the previous year. The increase points to gradual improvements in policy direction and institutional developments. However, despite this upward trend, gaps remain, highlighting the need to build on current gains through stronger implementation and accountability.



South Africa

By Claire Dehosse, Phenyo Sekati and Sophie Smit from ALT Advisory

Executive Summary

2025 reflects a year of ambitious regulatory initiatives, including the publication of the Draft White Paper on Audio and Audiovisual Media Services and Online Safety, and strengthened institutional capacity and oversight by the Information Regulator in South Africa. However, there are persistent gaps in connectivity, digital literacy, online safety, and equitable access. This illustrates the continued need for sustained, multi-stakeholder collaboration with accountability measures enforced on government and tech platforms, alongside the implementation of safeguards to advance digital rights and inclusion. Key findings highlight progress in the expansion of mobile broadband and 4G coverage, the strengthening of the Information Regulator's mandate, and greater awareness around digital rights. Persistent challenges remain, including high data costs, unreliable infrastructure, low digital literacy, online gender-based violence, risks associated with emerging technologies such as AI and digital IDs, and the potential chilling effect of new regulatory frameworks.

This report was formulated through extensive desktop research, the findings of which were then compared to key indicators outlined in the African Commission on Human and People's Rights' Declaration of Principles on Freedom of Expression and Access to Information in Africa. The Score Index, set out below, was then used to assign South Africa a score for each key indicator. Each indicator score makes up the total score, which is reflective of the overall position of digital rights in South Africa. Based on these findings, South Africa has been allocated a score of 47 out of 60 on the Score Index – a 4-point increase from 2024.[1] This improvement is partly attributable to government efforts to expand digital inclusion and increase the dissemination of information through digital technologies in underserved areas, alongside incremental progress in policy development related to emerging technologies.

Key recommendations are proposed, based on the aforementioned developments and findings of the Score Index. Such recommendations include expanding affordable and equitable internet access and improving digital literacy initiatives. Stronger oversight of surveillance, data protection, and access-to-information systems is needed, alongside clearer protections for free expression and careful regulation of mis- and disinformation. Efforts to address online gender-based violence should be strengthened through awareness campaigns, reporting mechanisms, and accessible legal remedies. Additional priorities include improving journalist safety online, enhancing content-verification practices, investing in secure digital infrastructure, and promoting ongoing civic participation in policy and legislative processes to support inclusive, rights-respecting digital governance.

1. See below page 21.

Introduction

Since 2016, South Africa has established strong legal foundations for digital rights – such as enacting cybercrime and data protection laws, online gender-based violence protections, and progressive policy frameworks. Civil society engagements in the country are robust and have helped to deepen awareness and accountability within these spaces. South Africa continues to play an influential role in shaping digital rights across the continent.

However, persistent gaps have remained in the past decade. The digital divide endures with high data costs, unreliable electricity supply, and low digital literacy rates continuing to limit meaningful access to online spaces, especially for rural communities, women, and low-income households.[2] Several government initiatives aimed at increasing and monitoring regulation of online harms and digital spaces have been implemented in recent years, with some being criticised for potentially criminalising misinformation and imposing overly broad obligations on online platforms.[3] This highlights ongoing tensions between regulating online harms and safeguarding freedom of expression in South Africa. Emerging technologies such as Artificial Intelligence (AI), digital IDs, and deepfakes further complicate the landscape, presenting both opportunities for inclusion and risks of discrimination, surveillance, and exclusion.

Internet Access And Disruptions

By mid-2025, South Africa's population reached 63.1 million,[4] with internet penetration rising to 78.9% from 74.7% in 2024[5]. However, the digital divide remains significant.[6] Rural communities lack in-home internet access, and income disparities continue to restrict both device ownership and data accessibility.[7] Even where coverage is available, a persistent "usage gap" driven by affordability constraints and limited digital literacy prevents many from fully participating online.[8] Service quality is improving, but frequent power outages force operators to depend on costly backup systems, resulting in disruptions to access to services that disproportionately affect lower-income households and rural areas, reinforcing existing inequalities in meaningful internet access.[9]

The SA Connect flagship project, which was launched last year, has to date failed to meet its desired targets due to budgetary constraints.[10] However, the Department of Communications and Digital Technologies allocated ZAR 710 million, approximately USD 42.4 million, in 2025 to the programme for the 2025/2026 financial year.[11] In addition, in May 2025,

2. Gillwald and Mothobi 'The state of ICT in South Africa' (2018) https://researchictafrica.net/research/state-of-ict-in-south-africa/ (accessed 21 November 2025).
3. Nicole Fritz and Justine Limpitlaw 'OPINION | Balancing freedom and safety: Online regulation debate demands oversight' (2025) https://www.news24.com/opinions/columnists/opinion-balancing-freedom-and-safety-online-regulation-debate-demands-oversight-20251015-0901 (accessed 23 November 2025).
4. StatsSA 'Mid-year population estimates 2025' (2025) https://www.statssa.gov.za/publications/P0302/P03022025.pdf (accessed on 22 November 2025).
5. Data Reportal 'Digital 2025: South Africa' (2025) https://datareportal.com/reports/digital-2025-south-africa (accessed on 21 November 2025).
6. ICASA 'A step closer to achieving a connected South Africa where no one is left behind' (2023) https://www.icasa.org.za/news/2023/a-step-closer-to-achieving-a-connected-south-africa-where-no-one-is-left-behind (accessed 21 November 2025).
7. GSMA 'Driving Digital Transformation of the Economy in South Africa Opportunities, policy reforms and the role of mobile' (2024) https://www.gsma.com/about-us/regions/sub-saharan-africa/wp-content/uploads/2024/11/GSMA_South-Africa-Report_Nov-2024-FINAL-VERSION (accessed 21 November 2025).
8. Id.
9. Id.
10. Nicola Mawson 'SA Connect rebooted with private sector support' (2025) https://www.itweb.co.za/article/sa-connect-rebooted-with-private-sector-support/o1Jr5MxPOQmMKdWL (accessed 25 November 2025.)
11. Parliament 'Parliament Communications Minister Allocates R710 Million to SA Connect Programme in 2025/26 Budget' (2025) https://www.parliament.gov.za/news/communications-minister-allocates-r710-million-sa-connect-programme-2025-26-budget (accessed on 21 November 2025).

Operation Vulindlela Phase II was introduced by the Treasury to include new priority areas such as addressing spatial inequality, strengthening local government performance, and advancing digital transformation.[12] This could play a role in closing the usage gap, although its impact has not yet been demonstrated in practice.

Online Freedom of Expression and Access to Information

South Africa continues to have an enabling legislative environment that protects freedom of expression and access to information. In 2025, the government published a Draft White Paper on Audio and Audiovisual Media Services and Online Safety (White Paper), which, while intended to address digital harms, has been criticised for proposing an overly broad regulatory licensing framework for online platforms. If the White Paper is adopted in its current form, it could chill lawful expression and public discourse. Therefore, critics warn that this overregulation could criminalise misinformation, restrict free expression, and impose overburdensome obligations on platforms, potentially chilling public discourse.[13] In addition, the Cybercrimes Act 19 of 2020 continues to be criticised for vague definitions that do not sufficiently set out the required intention necessary for the downloading of illegal content, which may result in those with lower digital literacy levels facing punitive consequences, effectively creating indirect discrimination among marginalised users. Further, the Act has limited public interest safeguards which may chill journalistic activity and whistleblowing if misapplied.[14]

12. National Treasury 'Q2 Operation Vulindlela Progress Report' (October 2025) https://www.treasury.gov.za/Q2%20Operation%20Vulindlela%20Progress%20Report.pdf (accessed on 11 November 2024).
13. Nicole Fritz and Justine Limpitlaw 'OPINION | Balancing freedom and safety: Online regulation debate demands oversight' (2025) https://www.news24.com/opinions/columnists/opinion-balancing-freedom-and-safety-online-regulation-debate-demands-oversight-20251015-0901 (accessed 23 November 2025).
14. SANEF 'Media and the law: legislation that affects journalists' (2024) https://presscouncil.org.za/2024/08/28/laws-that-threaten-journalists (accessed 21 November 2025).

Access to information

The Promotion of Access to Information Act (PAIA) remains the main mechanism for public access to State and publicly held information, but compliance by public bodies is unreliable, and request processing is often slow.[15] PAIA mandates that a request for information should be complied with within 30 days. However, government bodies often request extensions on this timeframe and subsequently deny access to the requested information through misapplying the PAIA grounds of refusal.[16] The Information Regulator, which is empowered to monitor and investigate complaints made in terms of PAIA,[17] has noted a substantial increase in PAIA complaints in 2025, reflecting non-compliance by public bodies and weak enforcement of access-to-information obligations.[18] To this end, the Regulator has launched a new promotion of an access to information programme with a sub-programme to investigate PAIA complaints.[19]

Disruptions and the lingering Digital Divide

South Africa lacks a clear, publicly accountable statutory takedown regime that balances rights with platform obligations. With regards to the White Paper above, civil society has also expressed concern that combining both broadcasting and online safety under one Act, and thus framing online safety through a broadcasting lens, conflates media regulation with platform oversight, creating risks of

15. South African History Archive 'Failure to respond to PAIA requests' (2018) https://www.saha.org.za/news/2018/September/failure_to_respond_to_paia_requests.htm (accessed 21 November 2025).
16. Timothy Lloyd, 'The Just Energy Transition in South Africa: Approaches to accessing information and knowledge for transition-affected communities' (2024) https://climateresilience.africa/wp-content/uploads/2024/06/JET_in-south_africa_v8.pdf (accessed on 20 January 2026); Daily Maverick 'Transparency, democracy the losers with most public institutions shamelessly ignoring requests for information' (2024) https://www.dailymaverick.co.za/article/2024-10-01-transparency-democracy-the-losers-with-most-public-institutions-shamelessly-ignoring-requests-for-information/ (accessed 19 January 2026).
17. Information Regulator of South Africa 'About the Regulator' https://inforegulator.org.za/ (accessed on 28 October 2024).
18. Information Regulator 'Annual Report' (2025) https://inforegulator.org.za/wp-content/uploads/2025/11/Information-Regulator-Annual-Report-2025-210mm-x-260mm-1.pdf (accessed 23 November 2025).
19. Information Regulator 'Annual Report' (2025) https://inforegulator.org.za/wp-content/uploads/2025/11/Informa-

censorship rather than protecting rights.[20] In addition, the continuous surge of Online Gender Based Violence (OGBV) may be seen as a cause of self-censorship for women journalists due to the increased amount of harassment and threats that they receive online, compounding existing gender-based barriers to participation in public discourse and violating their constitutional rights to equality, dignity, freedom of expression, and the right to be free from all forms of violence.[21]

In July 2025, the Gauteng High Court ordered Meta to shut down certain Instagram accounts and WhatsApp channels that were distributing explicit Child Sexual Abuse Material (CSAM) and to provide identifying information of the offenders.[22] After the judgement, Meta confirmed that the accounts that it was able to identify were shut down and that the relevant reports were filed to the National Centre for Missing and Exploited Children.[23] This first of its kind litigation in South Africa established legal accountability for global platforms operating in the country while balancing content removal with due process.

Arrests and prosecutions

Detailed, consolidated national statistics on arrests linked specifically to online expression remain limited in public reporting. However, in January 2025, a social-media user was charged for statements made online under the Cybercrimes Act and common-law offences of crimen injuria and incitement, but the case was later struck off the roll for incomplete investigations, illustrating how arrests alone can produce chilling effects even in the absence of convictions.[24] In addition, vigilante group Operation Dudula were interdicted by the Johannesburg High Court from spreading hate speech and incitement online after the Court recognised that they routinely used online spaces to mobilise violence, and encourage unlawful acts against foreign nationals.[25]

Gendered disinformation

In South Africa, gendered disinformation disproportionately targets women, politicians, journalists, and human rights defenders, through online attacks.[26] A recent study of tweets targeting South African female journalists revealed how gendered and racialised insults are mobilised to undermine their credibility and push them out of public conversations.[27] These online attacks often spill over into real-world fear and self-censorship, and many women report withdrawing from social media, toning down their digital presence, or not voicing opinions to avoid abuse.[28] Despite the scale of abuse, platforms and authorities continue to provide little protection, highlighting accountability gaps in both platform governance and state enforcement of digital safety for women.[29]

tion-Regulator-Annual-Report-2025-210mm-x-260mm-1.pdf (accessed 23 November 2025).

20. Above at n 12.
21. Sisanda Nkoala 'Baloi, clever blacks and magogo: Language as symbolic action in online violence against South African female journalists on X' (2025) https://link.springer.com/article/10.1007/s43545-025-01069-x (accessed on 21 November 2025).
22. The Department of Communications and Digital Technologies 'DCDT Welcomes the Ruling Ordering Meta to Shut Down Certain Instagram Accounts and WhatsApp Channels Posting Sexual Content' (2025) https://www.dcdt.gov.za/media-statements-releases/604-dcdt-welcomes-the-ruling-ordering-meta-to-shut-down-certain-instagram-accounts-and-whatsapp-channels-posting-sexual-content.html (accessed 21 November 2025).
23. L Isaacs, 'After court order, Meta agrees to several steps to shut down child port distribution on Whatsapp, Instagram in SA' EWN (2025) https://www.ewn.co.za/2025/07/18/after-court-order-meta-agrees-to-several-steps-to-shut-down-child-porn-distribution-on-whatsapp-instagram-in-sa (accessed 16 February 2026).
24. SA News 'Social media personality appears in court' (2025) https://www.sanews.gov.za/south-africa/social-media-personality-appears-court. (assessed 21 November 2025).
25. Power Law Africa 'Kopanang Against Xenophobia & Others v Operation Dudula & Others' (2025) https://powerlaw.africa/2025/11/04/kopanang-against-xenophobia-others-v-operation-dudula-others/ (accessed on 21 November 2025).
26. David Maas 'In South Africa, women journalists are targeted online routinely and with impunity, new research finds' (2025) https://ijnet.org/en/story/south-africa-women-journalists-are-targeted-online-routinely-and-impunity-new-research-finds (accessed on 21 November 2025). .
27. Id
28. SAHRC 'Opinion: GBV at the click of a button: even online, misogyny is out of line' (2023) https://www.sahrc.org.za/index.php/sahrc-media/opinion-pieces/item/3499-opinion-gbv-at-the-click-of-a-button-even-online-misogyny-is-out-of-line (accessed 21 November 2025).
29. Id.

Data Protection and Cybersecurity (Indicator 6)

In 2025, the Information Regulator launched a new e-system to report any security compromises of personal information in an ongoing effort to improve the monitoring of security incidents affecting personal information.[30] A 40% increase in data breaches was reported in 2025.[31] A notable data breach in 2025 was of a leading real estate firm, which suffered an unauthorised breach to its client database, including names, ID numbers, physical addresses, and contact details.[32] Further, at the international level, South Africa has not yet ratified the African Union Convention on Cybersecurity and Personal Data Protection. This results in limited regional alignment on data-protection norms and weak cross-border co-operation and enforcement of cybersecurity.

Digital IDs

Despite indications from the Department of Home Affairs last year that the National Identification and Registration Bill would be submitted to Cabinet during the 2024/25 financial year, there has been no movement on this. However, South Africa has made notable strides in its journey towards introducing digital IDs through its Roadmap for the Digital Transformation of Government.[33] The Roadmap, which falls under the Operation Vulindlela Phase II mentioned above, seeks to create digital public infrastructure reform under four main workstreams: digital identity; data exchange; digital payments; and digital

30. Information Regulator 'Media Statement: Regulator launches online reporting platform for security compromises' (2025) https://inforegulator.org.za/wp-content/uploads/2025/04/MEDIA-STATEMENT-INVITATION-TO-REPORT-SECURITY-COMPROMISES-THROUGH-THE-eSERVICES-PORTAL-.pdf (accessed 23 November 2025).
31. Corbado '10 Biggest Data Breaches in South Africa [2025]' (2025) https://www.corbado.com/blog/data-breaches-south-africa (accessed 23 November 2025).
32. Id.
33. My Mzansi 'South Africa's Roadmap for the Digital Transformation of Government' (2025) https://www.gov.za/sites/default/files/gcis_document/202505/south-africas-roadmap-digital-transformation-government.pdf (accessed 25 November 2025).

services.[34] In 2025, the pilot phase of the data exchange workstream was launched through MzanziXchange, which is a national data exchange initiative that seeks to support effective planning, policymaking, reporting, and service delivery.[35]

Under this pilot phase, several task teams have been established, including a legal and governance task team which, amongst other things, is aimed at safeguarding the exchange of personal and sensitive information.[36] While this initiative aims to aid access to services, without stronger data and human rights protections, the move to digital ID and other digital public infrastructure may deepen inequality and amplify privacy risks.

Privacy and Surveillance (Indicators 7,8)

The General Intelligence Laws Amendment Bill (GILAB) was passed by the National Council of Provinces in early 2024 and was finally assented to by the President on 28 March 2025.[37] The Act seeks to amend several of South Africa's existing intelligence laws to modernise and strengthen the country's intelligence framework. Despite substantial amendments following the public consultation process, commentators remain concerned about numerous aspects of the Act, including oversight mechanisms, scope of inception powers, and safeguards for journalists and lawyers.[38] Furthermore, the Act is not yet in force due to the need to align current regulations and

34. Id at pages 4-5.
35. MzansiXchange, 'What is MzanziXchange?' (2025) https://mzansixchange.treasury.gov.za/about/ (accessed on 26 November 2025).
36. MzansiXchange, 'Task Teams Driving the Pilot' (2025) https://mzansixchange.treasury.gov.za/pilot/ (accessed on 21 January 2026).
37. President Ramaphosa Assents to General Intelligence Laws Amendment Bill (28 March 2025) https://www.thepresidency.gov.za/president-ramaphosa-assents-general-intelligence-laws-amendment-bill (accessed on 19 November 2025).
38. Press Council 'General Intelligence Law Amendment Act adopted; still 'deeply flawed'' (29 March 2025) https://presscouncil.org.za/2025/03/29/general-intelligence-law-amendment-act-adopted-still-deeply-flawed/ (accessed on 23 November 2025).

directives with the Act.[39] On July 25 2025, the Constitutional Court handed down judgment in President of the Republic of South Africa v Speaker of the National Assembly and Others.[40] Here the Court ordered that, pending new legislation, the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) must be deemed to include provisions requiring the appointment of designated judges by the Minister upon nomination by the Chief Justice, that surveillance applications involving journalists or lawyers must disclose their status and be subject to additional protections, and that post-surveillance notification requirements must be reinstated.[41]

Mass surveillance technologies and biometric surveillance

South Africa continues to grapple with the legal and ethical implications of expanding mass surveillance infrastructure. In February 2025, the City of Johannesburg adopted the Privately-Owned Closed-Circuit Television Surveillance Camera By-law, which sought to regulate the installation and operation of private CCTV systems.[42] The by-law required individuals and businesses to register their cameras with the metro police, pay annual fees, submit technical plans, and grant the city access to footage.[43] In July 2025, civil society organisations challenged the by-law on constitutional and administrative grounds.[44] They argued that it infringed on residents' rights to privacy, imposed unjustified financial burdens, and failed to enhance public safety. The by-law was ultimately repealed in September 2025.[45]

Oversight

The Constitution outlines that the Inspector-General of Intelligence provides independent oversight of the State Security Agency, SAPS Crime Intelligence, and Defence Intelligence, with appointments requiring nomination by the Joint Standing Committee on Intelligence and approval by two-thirds of Parliament.[46] Beyond these, the Auditor-General audits intelligence budgets, including secret expenditure, while the Public Protector may investigate maladministration linked to surveillance practices.[47]

Despite this sound legal structure, a Commission of Inquiry into alleged criminality, political interference, and corruption in the criminal justice system is currently underway in South Africa. This inquiry underscores the risk that surveillance powers may have been misused, applied without sufficient oversight, or influenced by political or institutional bias, which may have implications for the oversight of privacy and surveillance laws.[48] The Commission is expected to examine how intelligence and law-enforcement agencies operate, including their use of surveillance powers, and could recommend reforms to enhance accountability, transparency, and human-rights protections.[49]

39. Ministry in the Presidency 'Question for Oral Reply Question Number: 538' (2025) https://www.parliament.gov.za/storage/app/media/Docs/exe_rq_na/01pv5mf2e6kzxkbsq55bbivjny2sclj4qg.pdf (accessed 25 November 2025).
40. [2025] ZACC 12; 2025 (9) BCLR 994 (CC) (President v Speaker of the National Assembly) https://www.saflii.org/za/cases/ZACC/2025/12.html (accessed on 20 November 2025).
41. President v Speaker of the National Assembly above n 41 at para 21.
42. See the draft bill here: https://joburg.org.za/documents_/Documents/By-Laws/2024/CCTV%20By-Law%20(ITEM%2069%20ANNEXURE).pdf.
43. OUTA 'Police the City of Joburg, not our CCTV cameras' (7 July 2025) https://www.outa.co.za/blog/newsroom-1/police-the-city-of-joburg-not-our-cctv-cameras-1428 (accessed on 21 November 2025).
44. OUTA 'Lights, camera, repeal: Joburg ditches CCTV by-law' (4 September 2025) https://www.outa.co.za/blog/newsroom-1/lights-camera-repeal-joburg-ditches-cctv-by-law-1443 (accessed on 21 November 2025).
45. Id.
46. Office of the Inspector-General of Intelligence https://www.oigi.gov.za/ (accessed 21 November 2025).
47. Auditor-General South Africa https://www.agsa.co.za/AboutUs.aspx (accessed 21 November 2025); Public Protector South Africa https://www.pprotect.org/?q=content/our-mandate (accessed 21 November 2025).
48. Commission of Inquiry 'The Judicial Commission of Inquiry into Alleged Criminality, Political Interference and Corruption in the Criminal Justice System' (2025) https://criminaljusticecommission.org.za/ (accessed 25 November 2025).
49. Id.

Developments in ICT and Emerging Technologies (Indicator 10)

AI Policy development

The enactment of the National Artificial Intelligence Policy Framework is still underway following its introduction in August 2024.[50] In October 2025, the Minister of Communications and Digital Technologies confirmed, in an interview, that the policy development process had been finalised and that stakeholder feedback had been incorporated into the Framework.[51] According to the Minister, the Framework is now ready to be presented to Cabinet for approval, after which it will proceed to Parliament for formal processing as a Bill.[52]

AI and the media

In November 2025, the Competition Commission published its final report in its Media and Digital Platforms Market Inquiry (MDPMI), the first of its kind in South Africa to examine the impact of digital platforms and AI on news media sustainability through a competition law framework.[53] The Competition Commission's final report found that AI chatbots significantly affect South Africa's news media as they rely on local journalism for training, but provide very little traffic or value back to the publishers who produced it.[54] The report also found that larger outlets are beginning to opt out of AI web crawlers, but most smaller media remain vulnerable due to a lack of resources. This creates bargaining imbalances that favour global publishers with content deals and marginalise South African outlets.[55] To address these issues, the Commission proposes empowering local publishers with clearer opt-out mechanisms, periodic training, and technical support, while encouraging AI companies to extend emerging compensation models to South African media.[56] If platforms fail to comply with these recommendations, the Competition Commission may refer the matter to the Competition Tribunal for enforcement.[57]

Other Emerging Technologies

Other innovations include the development of South Africa's first AI-powered teaching robot (IRIS), which was designed to master all subjects from Grade R to tertiary level in 11 official languages.[58] IRIS was developed by a private innovator, who undertook to introduce IRIS into classrooms by October 2025.[59] While this has not been achieved, the Minister of Science, Technology and Innovation praised the development of IRIS, highlighting its ability to "enhance education in the country by enabling learners to reach their full potential". [60]

Digital Inclusion

Persons with disabilities

In August 2025, the Deputy Minister of Science, Technology and Innovation launched a suite of locally developed assistive technologies to enhance accessibility and inclusion for people with disabilities, including learners from special

50. Department of Communications and Digital Technologies, 'South Africa National Artificial Intelligence Policy Framework' (2024) https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html (accessed on 23 November 2025).
51. Mzekandaba 'ITWeb TV: Malatsi vows to finalise SA's AI policy' (24 October 2025) https://www.itweb.co.za/article/itweb-tv-malatsi-vows-to-finalise-sas-ai-policy/KPNG878NDgWq4mwD (accessed on 23 November 2025).
52. Id.
53. Competition Commission 'Media Statement: Media and Digital Platforms Market Inquiry Releases Final Report' (13 November 2025) https://www.compcom.co.za/wp-content/uploads/2025/11/MDPMI-Releases-Final-Report-13-November-2025-2.pdf (accessed 23 November 2025).
54. Competition Commission 'Media and Digital Platforms Market Inquiry' (2025) https://www.compcom.co.za/wp-content/uploads/2025/11/CC_MDPMI-Final-Report_Non-Confidential-1.pdf at page 95.
55. Id.
56. Competition Commission 'Media and Digital Platforms Market Inquiry' (2025) https://www.compcom.co.za/wp-content/uploads/2025/11/CC_MDPMI-Final-Report_Non-Confidential-1.pdf at page 96.
57. The Competition Act 89 of 1998 at section 50.
58. Department of Science, Technology and Innovation 'Deputy Minister Gina launches South Africa's first AI teaching robot' (20 August 2025) https://www.dsti.gov.za/index.php/media-room/latest-news/4747-deputy-minister-gina-launches-south-africa-s-first-ai-teaching-robot (accessed on 23 November 2025).
59. Id.
60. Id.

needs schools.[61] Some of these assistive technologies include video remote interpreting, sign language translation, audio description, and wearable smartphone interfaces.

Adoption of child online-specific laws

While South Africa does not have any laws that specifically address the online safety of children, the White Paper on Audio and Audiovisual Media Services and Online Safety discussed above proposes a framework to address this gap. The White Paper sets out regulatory obligations for online platforms and streaming services, including measures to protect children from harmful content, enforce age-appropriate safeguards, and implement reporting mechanisms. Regardless of other concerns, civil society has welcomed the White Paper's focus on child safety.[62]

The Universal Service and Access Fund

The Universal Service and Access Agency of South Africa (USAASA) was allocated ZAR 268 million, approximately USD 16 million, for its operations, and the Universal Services and Access Fund (USAF) was allocated ZAR 173 million, approximately USD 10.3 million, for the 2025/26 financial year.[63] While these allocations reflect ongoing policy commitment, their scale remains insufficient to meaningfully close South Africa's digital divide, particularly in rural and underserved areas. According to its 2025-2026 Annual Performance Plan, the USAF will direct its funds toward expanding broadband connectivity in rural schools, clinics, and community centres, alongside localised Wi-Fi initiatives in underserved provinces.[64]

In parliamentary discussions, the Minister of Communications and Digital Technologies stated that governance failures and financial mismanagement persist at these entities, and as a result, an investigation into governance irregularities at USAASA was conducted in 2025. This resulted in the recent appointment of a new interim board to strengthen the institution and re-establish credibility.[65] These persistent governance and financial challenges have further delayed implementation and weakened institutional capacity, undermining the State's obligations under Principle 37 of the ACHPR Declaration..[66] These constraints disproportionately affect marginalised communities, including rural learners and low-income households, limiting progress towards equitable digital inclusion.

Conclusion

While 2025 saw an increase in South Africa's overall score index to 47 from 43 in 2024 due to notable advances for digital rights and inclusion in South Africa, major gaps persist. Addressing these challenges requires sustained collaboration between government, industry, civil society, and the media. A coordinated, rights-based approach is essential to close the digital divide and ensure meaningful digital inclusion. Further, financial mismanagement and potential oversight bodies threaten the effectiveness of institutions mandated to uphold and promote digital rights. The recommendations below outline priority actions.

61. South African Government 'Deputy Minister Nomalungelo Gina on innovations to assist people with disabilities in South Africa' (5 August 2025) https://www.gov.za/news/media-statements/deputy-minister-nomalungelo-gina-innovations-assist-people-disabilities-south (accessed on 23 November 2025).
62. Above at n 3.
63. South African Government, 'Minister Solly Malatsi: Communications and Digital Technologies Dept Budget Vote 2025/25' (2025) https://www.gov.za/news/speeches/minister-solly-malatsi-communications-and-digital-technologies-dept-budget-vote (accessed on 26 November 2025).
64. USAF 'Universal Service and Access Fund Annual Performance Plan: 2025/26' https://static.pmg.org.za/USAF_APP_31_Jan_2025__5.pdf.SIGNED.pdf at page 13 (accessed 23 November 2025).
65. Parliamentary Monitoring Group 'DCDT fiscal environment and an update on its entities' (19 November 2025) https://pmg.org.za/committee-meeting/42084/ (accessed on 26 November 2025).
66. IT Web 'USAASA board shrinks as four members resign' (2025) https://www.itweb.co.za/article/usaasa-board-shrinks-as-four-members-resign/VgZeyqJlODP7djX9 (accessed 19 January 2026).

Recommendations

The Government should:

- Expand equitable and affordable internet access and strengthen digital inclusion by prioritising communities with limited connectivity and investing in national digital literacy programmes.
- To ensure universal access to ICT services and access to information for marginalised communities, the Universal Service and Access Agency should ensure transparent reporting on its mandate, funding, and performance.
- The Universal Service and Access Agency should further align its role with broader 2025 digital inclusion initiatives such as South Africa Connect, the National AI Policy, and the B20 Digital Transformation Task Force recommendations on connectivity, literacy, and digital public infrastructure.
-
- Strengthen protections for free expression, privacy, and access to information by ensuring laws such as POPIA and PAIA are effectively implemented and enforced. In particular, there should be stronger administrative and financial consequences for unjustified delays or refusals to respond to PAIA requests. In addition, oversight of surveillance practices should be improved, and the Information Regulator's financial and human resources should be increased to support robust enforcement and timely responses to data breaches.
-
- Address OGBV and strengthen justice-sector capacity through public-awareness campaigns, improved reporting mechanisms, and strengthened legal remedies to ensure that social media companies are held accountable through clear regulatory guidance, co-regulatory mechanisms, and effective judicial oversight for the harms perpetuated on their platforms.

The Media should:

- Protect journalists online by implementing policies and training to safeguard staff, especially women and human-rights reporters, from online harassment.
- Establish standards for verifying content, countering mis- and disinformation, and monitoring online abuse without infringing privacy.
- Strengthen access to information and support journalists in using PAIA for reporting purposes, particularly against state institutions that do not comply with timelines mandated in PAIA for accurate and timely public interest reporting.

The Private Sector should:

- Invest in public–private partnerships in order to strengthen infrastructure and enable government initiatives to address the digital divide by offering affordable data plans that will serve to address access to the internet disparities.
- Protect individual data rights by complying with POPIA, PAIA, and by investing in cybersecurity prevention measures.

Civil Society Organisations should:

- Continue to hold the government accountable to its stated commitments and deliverables, while finding suitable ways to collaborate with government and other stakeholders to promote digital literacy and access to the internet for all.
- Continue to participate robustly in legislative and other government processes.

The Score Index

Nigeria, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	5	5	South Africa experienced no deliberate internet shutdowns in 2025.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	3	3	Although laws and policies exist to promote internet access, significant inequalities persist. The government has taken steps to address this, but progress has been slow.
False News Criminalisation	P22(2)	4	4	There are risks that regulatory bodies will attempt to criminalise mis- and disinformation in an overly broad manner that would unduly chill freedom of expression, particularly if the draft White Paper on Audio and Audiovisual Media Services and Online Safety is adopted as it currently stands.
Sedition Legislation	P22(2)	5	5	There are no sedition laws in South Africa, and the government has taken no action against such acts.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	3	3	There continues to be a growing trend of online harassment against journalists and human rights defenders, especially women.
Data Protection Legislation.	P42	4	5	There is strong data protection legislation in place, and progress has been made in its enforcement.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	5	5	There is no indication of unwarranted state interference with internet intermediaries.
Invasion of Privacy of Communications	P41	3	3	Recent surveillance legislation in South Africa has yet to take effect, with ongoing concerns over its scope, enforcement, and impact on privacy.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	3	4	Government efforts to expand the dissemination of information through digital technologies in rural areas have increased.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
AI and Emerging Technologies national strategies	P39(6)	2	3	There have been positive, although slow, advances in policy development in 2025.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P39(6)	3	3	There have been positive developments from government in working towards laws which deal with children's digital safety.
Digital Inclusion	P37(3)	3	4	Government has made positive strides towards digital inclusion.
Total (out of 60):	2024: **43**	2025 **47**		



Sudan

Jonette-Ann Matilda O. Greene

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 privacy, 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 Starlink 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 situation 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 2018[8]. 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 Starlink 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 internet[11]. 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 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

8. TPRA, Laws, https://tpra.gov.sd/wp-content/uploads/2025/02/THE-TELECOMMUNICATION-AND-POST-ORGANIATION-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 ini 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://advox.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)
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, "[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, "[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)

Crimes Against the State Court issued a ruling against a medical director who was sentenced to four years in prison, and his phones were confiscated on charges of insulting and cursing leaders of the armed forces.[20] He was charged under Article 24 of the Cybercrimes law, which criminalises defamation.

In addition, after the RSF takeover of Al Fasher, the Sudanese journalists' syndicate reported on November 6 2025 that they lost communication with seven journalists there, and another four journalists were in RSF custody before entering Al Fasher.[21]

In 2025, no cases of website blockage were recorded. However, arrests related to online freedom of expression were noted during the year. On June 28, the 'security cell', a joint force of several security agencies, arrested the journalist Onor Hamad, following his post criticising the General Intelligence Service (GIS) because of confiscating his passport.[22] Also, on October 26, the journalist Rashan Oshi posted on Facebook saying that she was released after an arrest by a "security entity that I will not mention".[23] Moreover, the RSF arrested Al Jazeera's correspondent Moamer Ibrahim following their takeover of Al Fasher city.[24]

Moreover, regarding access to information, Sudan has the Right to Access Information Act, 2015,[25] which is concerningly restrictive of access to information instead of facilitating access as it listed 12 types of classified information that are restricted to access, including information related to 'national security' and 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.

20. Al Sudani, "السجن ٤ سنوات لمدان تمت ادانته بسب وقياديات الدولة [A man was sentenced to four years in prison for insulting and verbally abusing state leaders.]", https://alsudaninews.com/?p=190682, (accessed on 19 November 2025)
21. Alttahrir, "تجمع الصحفيين يكشف عن أوضاع الصحفيين في الفاشر بعد المواجهات الأخيرة [The Journalists' Syndicate reveals the situation of journalists in El Fasher after the recent clashes.]", https://www.alttahrer.com/archives/107029, (accessed on 20 November 2025)
22. Facebook, Azza Aira, https://www.facebook.com/100002844124678/posts/9544067919031251/?rdid=2oW8cI-C7amM7L6Cb#, (accessed on 29 November 2025)
23. Al Raya News, " راشان أوشي ترسل تفاصيل اعتقالها [Rashan Oshi recounts the details of her arrest]", https://alrayanews.net/85337, (accessed on 29 November 2025)
24. Al Jazeera, "تنديد محلي ودولي واسع الذع للاعتقال السريع للصحفي معمر إبراهيم [Local and international condemnation of the Rapid Support Forces' arrest of journalist Muammar Ibrahim]", https://www.ajnet.me/media/2025/10/28/%D8%AA%D9%86%D8%AF%D9%8A%D8%AF-%D9%85%D8%AD%D9%84%D9%8A-%D9%88%D8%AF%D9%88%D9%84%D9%8A-%D8%A8%D8%A7%D8%B9%D8%AA%D9%82%D8%A7%D9%84-%D8%A7%D9%84%D8%AF%D8%B9%D9%85-%D8%A7%D9%84%D8%B3%D8%B1%D9%8A%D8%B9, (accessed on 29 November 2025)
25. Ministry of Justice, "The Right to Access information act for the year 2015", https://moj.gov.sd/sudanlaws/#/reader/chapter/362, (accessed on 6 November 2025)

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://advox.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, "روفراد بونجب الاياين في نيينمدلا فتاوملا شيتفت حلم [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, " عيرسلا معدلا تاباسح تاصنم فاقيإ دعب نادوسلا في 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=pfbid02Vz6Amw3R8JUcAv9f5hVXeu81XRE56zyxf6v9vHM5sYw6mTnvokbuRnLCXXBSsjMDl&id=100069487239242&__cft__[0]=AZXHAkmhXosehZGKgfIr56QuHT31qD7OXPSXHOU4Ag5u9XG7rYa6EStZ4hQElZvdD9mGXoyG4TvqJASuoWfFPBtOAsOKmkBpLxV6c7C0swo8Pi_WhzzTqV5TJq3KimVvQv8fnWLLJk8uFxAiHwWEdXCRQwaYLVQ-PcwavaBjNl4NbFzt_u6OQPCku2MDMGptGFw&__tn__=%2CO%2CP-R, (accessed on 29 November 2025)

Moreover, the Meta transparency center highlighted[36] 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, "ءاكذلا ءاطصنالا زكرم في ربابلا ربتعي يذلا يسوسنملا ملعلا ةرسل ظاملا ةبتكلا" [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 institutions, 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 stealing citizens' phones and other electronic devices.

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)

Civil Society Organisations should:

- Actively monitor and document cases where the amended cybercrimes 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	2	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)	2	2	The Cybercrimes law criminalised Sedition.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	Several arrests and media harassment cases by the authorities and RSF have been reported.
Data Protection Legislation.	P42	2	2	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)	2	2	While there is no information for this year, last year witnessed numerous cases of governmental interference.
Invasion of Privacy of	P41	1	1	The RSF areas witnessed phone inspections.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	2	1	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)	1	1	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)	2	2	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**	



Tanzania

By Anonymous

Executive Summary

This report covers the state of digital rights and inclusion in Tanzania for the year 2025. Throughout the years, Tanzania has made numerous efforts to bridge the digital gap. Furthermore, the nation has adopted Information Communication Technology (ICT) policies and supportive legal frameworks to build a robust digital ecosystem. Despite the efforts made through the various pieces of legislation, including the Constitution of the United Republic of Tanzania, there are still areas of grave concern that impact disproportionately on different demographics of the country.[1] The report employed a combination of qualitative research methods including literature review, policy and legal analysis, monitoring and observations of digital rights trends throughout the year. The report also gained insights

1. CIPESA,State of Internet Freedom in Africa 2024 Africa's Electoral democracy and technology:pitfalls and promises(accessed on 6 November 2025) https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_Report_2024.pdf

from The Score Index, developed by Paradigm Initiative, to assess compliance with the African Charter on Human and Peoples' Rights (ACHPR) Declaration, evaluating the state of digital rights. This report gained insights from desktop research on existing laws, policies, policy briefs, news, other reports and commentaries from different stakeholders. Tanzania is moderately compliant as there are areas of improvement, such as revision and development of specific laws, the Personal Data Protection Commission (PDPC) issued its first-ever ruling regarding child data protection in August 2025, highlighting its proactive enforcement stance[2]. This report aims to shed light on what currently exists, identify the gaps and make recommendations to help Tanzania's digital space thrive.



2. Fin and Law. (2025, August 20). The Tanzania Personal Data Protection Commission issues its decision on protection of child's data.https://finandlaw.co.tz/2025/08/20/the-tanzania-personal-data-protection-commission-issues-its-decision-on-protection-of-childs-data/

Introduction

In 2016, Tanzania's digital ecosystem was still at a relatively early stage. Internet access was limited, particularly in rural areas where the majority of the population resides. Mobile connectivity was expanding, but broadband infrastructure remained uneven, and internet use was largely confined to urban centres. During this period, the regulatory environment increasingly relied on restrictive laws such as the Media Services Act (2016), which laid the foundation for criminalisation of online expression and the control of digital spaces[3].

By 2017–2019, Tanzania experienced gradual growth in mobile and internet subscriptions, alongside rising concerns around surveillance and misuse of personal data. Allegations by opposition figures and journalists including claims that telecommunications companies had shared user data with the government highlighted early warning signs of weak data protection safeguards. At the same time, civil society and independent media began reporting increased pressure, arrests, and censorship linked to online activity, reflecting a tightening digital civic space.

In 2020, these challenges became more visible during the general elections, when the government imposed partial internet disruptions and social media restrictions.[4] These actions demonstrated the state's growing willingness to interfere with internet access during periods of political activity, reinforcing concerns raised in earlier Londa reports about internet shutdowns, freedom of expression, and access to information.

Between 2021 and 2023, internet usage continued to expand, driven primarily by mobile broadband. However, this growth was accompanied by persistent regulatory gaps. Laws on cybercrime, electronic transactions, and online content moderation were actively enforced, often in ways that disproportionately restricted speech

3. Media Services Act, 2016 (United Republic of Tanzania) (accessed on 6 November 2025), https://www.parliament.go.tz/uploads/bills/1454936437-The%20Media%20Services%20Act,%202016.pdf
4. NetBlocks, Internet disrupted in Tanzania on eve of presidential elections 2020 (accessed on 6 November 2025), https://netblocks.org/reports/internet-disrupted-in-tanzania-on-eve-of-presidential-elections-oy9abny3

and access to information. Although the Personal Data Protection Act was enacted in 2022, it was criticised for vague provisions, including the absence of clear timelines for registration and notification of data controllers and processors[5]. As a result, Tanzania's compliance with regional digital rights standards remained moderate at best.

By 2024, Tanzania made notable institutional progress. The government inaugurated a Data Protection Authority on April 3 2024[6], signalling an intention to strengthen data governance. The launch of the Tanzania Digital Economy Strategy 2024–2034 further reflected efforts to position the country as a regional digital hub in East Africa[7]. The strategy's six pillars, namely digital infrastructure, governance, skills, innovation, inclusion, and digital financial services outlined an ambitious vision for leveraging digital technologies for economic growth and social development. However, these policy gains were accompanied by persistent regulatory and rights-based concerns. The penalties imposed on information holders for releasing information under the Access to Information Act remained disproportionately severe, creating a chilling effect on transparency. Government actions continued to undermine access to information through deliberate internet throttling and platform restrictions. In May 2025, authorities restricted access to X (formerly Twitter), limiting online civic discourse[8]. In addition, the introduction of Tanzania's Virtual Private Network (VPN) policy in 2024 exposed vulnerable communities to heightened risks[9]. Where VPNs had previously enabled safer anonymous expression, users were now required to obtain government authorisation, effectively removing a critical layer of privacy and digital security for those most in need.

5. Personal Data Protection Act, No. 11 of 2022 (United Republic of Tanzania) (accessed on 6 November 2025), https://tanzlii.org/akn/tz/act/gn/2023/395b-1/eng%402023-06-13
6. Tanzania launches Personal Data Protection Commission (PDPC) on 3 April 2024 (accessed on 6 November 2025), https://www.thecitizen.co.tz/tanzania/news/national/tanzania-launches-commission-to-oversee-personal-data-protection-4577912
7. Ministry of Information,communication and information technology "Tanzania Digital Economy Strategy 2024-2034' (2024)https://www.ictc.go.tz/public/documents/tanzania_digital_economy_strategy.pdf (accessed on 10 November 2025)
8. Minority Africa 'My privacy matters": Tanzania's new VPN policy leaves LGBTQ+ individuals exposed'(2024) https://minorityafrica.org/my-privacy-matters-tanzanias-new-vpn-policy-leaves-lgbtq-individuals-exposed/(accessed on November 2025)
9. 3 Daily News "Digital growth spurs youth inclusion, connectivity" (2025) https://dailynews.co.tz/digital-growth-spurs-youth-inclusion-connectivity/ (accessed on 5 January,2026).

In 2025, Tanzania's digital landscape presents a complex mix of progress and persistent challenges. According to the 2022 national census, the population stands at approximately 61 million, with a majority living in rural areas[10]. By September 2025, the country recorded 56.3 million active internet subscriptions, translating to an estimated 82.6–87% connectivity rate[11].

Mobile devices dominate internet use, with over 99% of users accessing the internet via smartphones, supporting growth in mobile money, e-commerce, and online services. Yet, regulatory practices continue to undermine digital rights. On October 29 2025, during Tanzania's general election, the government imposed a nationwide total internet shutdown lasting five days and six hours[12] marking a significant escalation from the partial shutdowns observed in 2020. The government did not only mandate a shutdown but also instituted a curfew in the major city of Dar-es-Salaam, deployed military in major cities and closed down economic activities, including schools, for the whole duration. A report by Cable News Network (CNN) verified by forensic video content of police brutality recorded by citizens during the shutdown.[13]

Unlike 2016, when Tanzania's primary challenge was limited connectivity, 2025 is characterised by widespread infrastructure expansion but shrinking civic space online. While the country has transitioned from low internet access to near-universal connectivity in technical terms, meaningful access, digital inclusion, and the protection of digital rights have not progressed at the same pace. Regulatory responses to political dissent such as shutdowns, surveillance, and platform restrictions continue to offset gains made through policy reforms and infrastructure investment.

This report aims to shed light on what currently exists, identify the gaps, and make

10. National Sensas "National Sensas 2022" (2022) https://sensa.nbs.go.tz/ (accessed on 14 December 2025).
11. Tanzania Communications Regulatory Authority "Communication Statistics Report for the Quarter Ending September 2025" (2025)https://www.tcra.go.tz/uploads/text-editor/files/Communication%20statistics%20report%20for%20quarter%20one%20ending%20September%202025_1760792820.pdf (accessed on 14 December 2025).
12. Paradigm Initiative 'Press statement: Tanzania's Internet Blackout and Ongoing X Suspension Cost Over US $238 Million, Paradigm Initiative Warns' (2025) https://paradigmhq.org/tanzanias-internet-blackout-cost-over-us-238-million/ (accessed on 6 January 2026). Paradigm Initiative
13. CNN "'Oh My God, This Is Our Tanzania': Tanzania Police Shooting Protesters & Possible Mass Graves" (2025) https://edition.cnn.com/2025/11/21/africa/tanzania-police-shooting-protesters-deadly-election-intl-invs (accessed on 21 November 2025)

recommendations to help Tanzania's digital space thrive. This report gained insights from desktop research on existing laws, policies, policy briefs, news, other reports and commentaries from different stakeholders.

Internet Access and Disruptions

Mobile network availability (signal presence) is high nationally, with most of the population within range of 2G/3G/4G networks due to extensive infrastructure expansion. 2G covers nearly all areas, while 3G and 4G have reached roughly 93–94% of the population. 5G coverage is emerging, now reaching around 26–29% of the population.[14] Internet subscriptions have grown significantly: by September 2025 there were over 56 million active internet subscriptions, driving overall penetration toward around 80–83% of the population; however DataReportal states that internet penetration stood at 29.1% of the total population in Tanzania at the end of 2025.[15] Mobile broadband accounts for virtually all internet use (over 99%), as most subscribers connect via smartphones or mobile devices rather than fixed broadband. While national infrastructure statistics show widespread coverage, there remains a clear digital divide between urban and rural areas, especially in terms of actual usage and effective access. Network signals e.g., 3G/4G tends to be more reliably available in urban centers where population density and commercial profit justify investment, while rural areas often have coverage gaps or lower-quality connections. Independent telecom market analysis indicates that providers and policy initiatives are working to extend rural coverage, but gaps persist due to cost and lower demand in sparsely populated regions. Urban areas have significantly higher rates of internet use and ICT ownership compared with rural zones. Based on the 2022 census and ICT data (the most recent demographic breakdown available), approximately 27.3% of urban residents used the internet, compared with only about 7.7% of rural residents.[16]

During Tanzania's October 29 2025 general election, authorities imposed a nationwide internet restriction, severely disrupting mobile data and access to social media platforms such as Facebook and WhatsApp.[17] The shutdown began as polling booths opened and coincided with protests and reports of violence, raising serious concerns about censorship and suppression of information in a critical democratic moment.[18]

Despite widespread mobile network coverage in Tanzania, internet access in 2025 remains constrained by affordability and quality challenges. Mobile data and internet-capable devices remain costly relative to average incomes particularly for rural and low-income households while connection quality is uneven, with urban areas benefiting from faster and more stable services compared to rural regions that experience slower speeds, congestion, and frequent outages. This disparity between nominal coverage and meaningful connectivity continues to reinforce the urban–rural digital divide.[19]

Online Freedom of Expression and Access to Information

In 2025, Tanzania's legal framework governing online expression remained heavily weighted toward restriction rather than protection, despite constitutional guarantees of freedom of expression. Laws such as the Cybercrimes Act (2015)[20], the Electronic and Postal Communications (Online Content) Regulations (2020)[21], the Media Services Act (2016), and Penal Code provisions on sedition and false

14. Extensia.Tech "Tanzania: Telecoms services adoption to increase in the first quarter of 2025/2026" (2025) https://extensia.tech/tanzania-telecoms-services-adoption-to-increase-in-the-first-quarter-of-2025-2026/ (accessed on 5 January 2026).
15. DataReportal "Digital 2026: Tanzania" (2025) https://datareportal.com/reports/digital-2026-tanzania (accessed on 5 January 2026).
16. National Bureau of Statistics and Office of the Chief Government Statistician (OCGS) "Information and Communication Technology Analysis in Tanzania" (2025) https://www.nbs.go.tz/uploads/statistics/documents/en-1764330874-Information%20and%20Communication%20Technology%20%20Analysis%20%20in%20Tanzania.pdf? (accessed on 5 January 2026).
17. TechCabal "Tanzania restricts internet as citizens vote in general election" (2025) https://techcabal.com/2025/10/29/tanzania-restricts-internet-as-citizens-vote-in-general-election/ (accessed on 5 January 2026).
18. The Condia "The internet goes slow in Tanzania on election day" (2025) https://thecondia.com/tanzania-internet-shutdown-election-2025/ (accessed on 5 January 2026).
19. World Bank "Tanzania Digital Economy Diagnostic" (2022) https://www.worldbank.org (accessed on 14 December 2025).
20. The Cybercrimes Act, Act No. 14 of 2015 (the Cybercrimes Act).
21. The Electronic and Postal Communications (Online Content) Regulations, 2020 (the Online Content Regulations).

information continue to be used to stifle online speech. These laws contain vague and overly broad provisions particularly those criminalising false, misleading, or offensive information which have been used against journalists, activists and opposition figures for online expression.[22] From an international human rights law perspective, these restrictions fail to meet the requirements of legality, necessity, and proportionality under Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[23] and Article 9 of the African Charter on Human and Peoples' Rights.

Legal protections for access to information remain weakly implemented in practice. Although Tanzania's Access to Information Act formally guarantees the public's right to seek and receive information held by public bodies, its effectiveness in 2025 was limited.[24] The lack of a fully independent and operational Information Commission continues to undermine enforcement, leaving citizens without effective remedies when access requests are denied. Civil society organisations report that public authorities frequently rely on broad exemptions related to national security or public order, resulting in limited transparency and inconsistent disclosure practices.[25] These shortcomings fall short of international standards requiring independent oversight, proactive disclosure and effective appeal mechanisms.

Censorship and content removal intensified in 2025, particularly during elections and periods of political tension. Authorities ordered internet shutdowns, platform suspensions and content restrictions affecting social media and online discussion spaces. The Tanzania Communications Regulatory Authority (TCRA) also suspended the online platform JamiiForums for 90 days in September 2025, accusing it of publishing content that "misleads the public" and threatens national unity.[26]

Following the blackout, mobile users received messages warning that sharing images or videos deemed inflammatory could lead to treason charges.[27] Rights groups and civil society organisations strongly condemned these measures, arguing that the internet restrictions undermined freedom of expression, restricted media reporting, and violated citizens' rights during a key moment for political participation.[28]

Regulatory directives were issued to major platforms such as Meta, to restrict or remove content deemed unlawful under domestic legislation. Renown activist Mange Kimambi[29] Maria Sarungi Tsehai's Meta accounts faced restrictions. Kimambi's Instagram accounts were removed, citing "recidivism" and repeated violations of its community standards, while Maria Sarungi Tsehai's Instagram page was geo-restricted inside Tanzania after what Meta described as a "legal order from Tanzanian regulators."[30]

Several key Tanzania figures were arrested pre- and post-election for content shared on digital platforms. On April 9 2025, prominent opposition leader Tundu Lissu, chairman of the main opposition party, Chama cha Demokrasia na Maendeleo (CHADEMA), which translates from Swahili to "the Party for Democracy and Progress", was arrested and charged with treason and related offences, including for public statements and actions calling for electoral reform that were widely disseminated online and offline.[31]

Businesswoman and social media influencer Jennifer Bilikwija Jovin, popularly known as Niffer, was arrested in late October 2025 and charged with treason in connection with protests surrounding the October 29 2025 general election. Prosecutors alleged she and 239 other people were involved in actions linked to election-day unrest and in a related treason case she faced distinct charges alleged-

22. ARTICLE 19 "Tanzania: Laws restricting freedom of expression" (2025.) https://www.article19.org/region/tanzania/ (accessed on 17 February 2026).
23. International Covenant on Civil and Political Rights (ICCPR) https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights(accessed on 4 January 2026).
24. The Access to Information Act, Act No. 6 of 2016 (the Access to Information Act).
25. Twaweza "Analysis of the Access to Information Act No. 6 of 2016" (2017) https://twaweza.org/wp-content/uploads/2021/05/Twaweza-ATI-Act-Analysis-BT130217.pdf (accessed on17 February 2026).
26. Human Rights Watch "Tanzania: Deepening Repression Threatens Elections" (2025) https://www.hrw.org/news/2025/09/29/tanzania-deepening-repression-threatens-elections (accessed on 14 December 2025)
27. Africanews "Tanzania partially restores internet access, warns against image sharing" (2025) https://www.africanews.com/2025/11/04/tanzania-partially-restores-internet-access-warns-against-image-sharing/(accessed on 14 December 2025)
28. CADE Project "Digital rights groups urge Tanzania to guarantee online freedoms ahead of general election" (2025) https://cadeproject.org/updates/digital-rights-groups-urge-tanzania-to-guarantee-online-freedoms-ahead-of-general-election/ (accessed on 14 December 2025).
29. BBC News "Meta restricts Tanzanian activist accounts after government request" (2025) https://www.bbc.com/news/articles/cwyv7ggqpjpo (accessed on 10 December 2025).
30. The Africa Report "Tanzania crackdown goes digital: Meta blocks two leading activists" (2025) https://www.theafricareport.com/401302/tanzania-crackdown-goes-digital-meta-blocks-two-leading-activists/(accessed on 14 December 2025).
31. BBC News "Tanzania's opposition leader charged with treason" (2025) https://www.bbc.com/news/articles/c98gg7172ymo (accessed on 10 November 2025).

ly tied to her conduct prior to the elections.[32] Amani Golugwa, the deputy secretary-general of CHADEMA, was arrested in early November 2025 as part of a wider crackdown and charged, along with hundreds of others, for alleged involvement in protests that followed the disputed election. Authorities framed these in part as treason cases linked to incitement and coordination.[33] By November 26 2025, the Director of Public Prosecutions had withdrawn treason charges against 220 youths arrested after the general election unrest, although treason prosecutions continued for Jenifer "Niffer" Jovin and another suspect.[34] This arrest over youth's right to protest unfair elections and share on digital platforms, what happened on October 29 2025, shows a declining rate of freedom of speech and that citizens get punished for it.

Gendered Disinformation

In Tanzania, women and girls in public life including women politicians, journalists and human rights defenders (HRDs) are disproportionately affected by gendered disinformation and technology-facilitated gender-based violence (TFGBV). Online threats, misinformation and hate campaigns target women on the basis of gender and political identity, undermining their credibility, deterring participation, and amplifying stigma. TFGBV has been recognised as a growing digital threat in Tanzania, with abuses such as hate speech, threats and coordinated disinformation campaigns often aimed at silencing and discrediting women in political and civic roles, particularly during election cycles and periods of heightened political tension.[35] Gendered online abuse in Tanzania includes hate speech, cyberstalking, coordinated trolling, non-consensual sharing of intimate content, and deepfake pornography, all aimed at intimidating, shaming, or discrediting female public figures and HRDs. Despite the growing recognition of TFGBV in Tanzania, including through national dialogues on technology-facilitated violence and GBV during elections, policy responses remain nascent and uneven.[13] Initiatives such as integrating digital safety and GBV prevention into the National Plan of Action for the Prevention of Violence Against Women and Children (2025–2029) was officially launched in May 2024 and represent important steps toward addressing online gendered violence and strengthening coordination across media, tech, and legal stakeholders.[36] Tanzanian activist and media figure Maria Sarungi Tsehai has been a vocal advocate for social change and media freedom. In January 2025, she was reportedly abducted by armed men in Nairobi, Kenya, an incident linked in local reporting to her activism. This episode reflects risks faced by outspoken activists in the region and contributes to an atmosphere where threats against HRDs and online critics are taken seriously.[37]

Data Protection and Cybersecurity

In 2025, Tanzania saw significant developments in data privacy and protection, particularly through the enforcement actions of its Personal Data Protection Commission (PDPC) under the Personal Data Protection Act (PDPA), Act No. 11 of 2022. One major event was the extension of the registration deadline for all public and private data-handling institutions to April 30 2025, after which non-compliant organisations risked legal penalties. PDPC Director General Mkilia stated that enforcement would begin from May 2025.[38]

In 2025, the PDPC began building institutional capacity. In July 2025, it held a three-day training for Data Protection Officers (DPOs), covering key topics such

32. The Citizen "Niffer, 21 others charged with treason and related offences" (2025) https://www.thecitizen.co.tz/tanzania/news/national/niffer-21-others-charged-with-treason-and-related-offenses-5256794 (accessed on 14 December 2025).
33. France 24 "Tanzania arrests senior opposition figure as hundreds face treason charges" (2025) https://www.france24.com/en/africa/20251108-tanzanian-police-arrest-top-opposition-official-hundreds-charged-with-treason (accessed on 14 December 2025)
34. The Chanzo. (2025, November 26). DPP withdraws treason cases against another 220 linked to election unrest. https://thechanzo.com/2025/11/26/dpp-withdraws-treason-cases-against-another-220-linked-to-election-unrest/
35. Zaina Foundation. (2025). TFGBV: Technology-facilitated gender-based violence in Tanzania — a growing digital threat.https://zainafoundationtz.org/tfgbv-technology-facilitated-gender-based-violence-in-tanzania-a-growing-digital-threat/
36. National Dialogue on Technology Facilitated Violence. (2025). Concept Note 2025. Women in Law and Development in Africa Tanzania. https://wildaftanzania.or.tz/wp-content/uploads/2025/10/National-Dialogue-Concept-Note-2025.pdf
37. Maria Sarungi Tsehai (n.d.) In Wikipedia https://en.wikipedia.org/wiki/Maria_Sarungi_Tsehai (accessed on 5 January,2026).
38. Africa-Press "PDPC extends registration deadline" (2025) https://www.africa-press.net/tanzania/all-news/pdpc-extends-registration-deadline (accessed on 15 December 2025).

as Data Protection Impact Assessments (DPIAs), cross-border data flow permits and compliance report preparation.[39] Later, in August 2025 the PDPC convened another DPO training session to further strengthen data protection capacity across institutions. 29 A landmark ruling also marked Tanzania's data privacy landscape, when in August 2025, the PDPC issued its first-ever decision on a complaint involving a child's image. The commission found that posting a newborn's photo on Instagram without parental consent constituted unlawful processing of sensitive personal data. It fined the data controller, ordered deletion of the image and awarded compensation of TZS 20,000,000 (approximately US$7800) to the complainant.[40]

Beyond enforcement, Tanzania's privacy system received international recognition. In June 2025, analysts and technology leaders noted that Tanzania was making "better and stable systems for personal information protection and internet protection" a sign that data protection was moving from policy into practice.[41] Additionally, legal experts raised concerns over the unlawful repurposing of personal data. According to Clyde & Co (2025), under Section 25 of the PDPA, repurposing data requires new consent unless the use is authorised by law or the data is anonymised. Some data controllers risk heavy fines or even imprisonment if they process personal data beyond its original intended purpose.[42]

Privacy and Surveillance

Tanzania's surveillance powers are primarily grounded in the Cybercrimes Act (2015), the Electronic and Postal Communications (Online Content) Regulations Act (2020), which allow authorities to access communications data and order monitoring or takedowns on broad grounds such as national security or public order. The laws authorising surveillance lack clear thresholds for necessity and proportionality and do not consistently require prior judicial authorisation. As a result, surveillance powers are broad, discretionary and insufficiently constrained by human rights safeguards.

Although the government has not publicly confirmed procurement of advanced mass surveillance tools, there are persistent concerns that authorities monitor digital communications, particularly during elections and protests[43]. In 2025, nationwide internet restrictions and platform blocking during the general election indicated extensive state capacity to control and observe online activity. Civil society groups reported monitoring of WhatsApp groups and social media platforms used for mobilisation, leading to arrests[44].

Tanzania continues to rely on biometric systems, including biometric national identification (IDs), Subscriber Identity Module (SIM) card registration and biometric voter registration, all of which collect fingerprints and other sensitive personal data. While these systems are justified for administrative and electoral purposes, safeguards on data retention, sharing and secondary use remain unclear. There is no public confirmation of live facial recognition technology in public spaces as of 2025, but the lack of explicit legal limits on biometric expansion raises concerns. Weak enforcement of data protection laws heightens risks to privacy and non-discrimination.

In 2025, the Tanzania Communications Regulatory Authority (TCRA) ordered content restrictions and platform suspensions during the election period, including blocking access to X (formerly Twitter).[45] Meta's transparency reports for 2025 notes that by June 2025 The Tanzanian Government had requested an emergency disclosure of an account indicating there

39. Personal Data Protection Commission "Invitation letter: Special training for Data Protection Officers (DPOS) Fourth Batch" (2025)https://www.pdpc.go.tz/media/filer_public/c8/d6/c8d6f071-f7c4-40e2-a9b5c4dedbceb5f5/invitation_letter_special_training_dpos_fourth_batch.pdf (accessed on 14 December 2025).
40. Fin & Law "The Tanzania Personal Data Protection Commission issues its decision on protection of child's data" (2025) https://finandlaw.co.tz/2025/08/20/the-tanzania-personal-data-protection-commission-issues-its-decision-on-protection-of-childs-data/ (accessed on 10 December 2025).
41. IPP Media/ The Guardian "Tanzania recognized for advancing personal data and internet protection systems" (2025) https://www.africa-press.net/tanzania/all-news/pdpc-extends-registration-deadline (accessed on 10 December 2025).
42. Clyde & Co LLP "Protection of Personal Data in Tanzania: Addressing the Unlawful Repurposing of Personal Data" (2025) https://www.clydeco.com/en/insights/2025/11/protection-of-personal-data-in-tanzania-addressing (accessed on 14 December 2025).
43. CIPESA, State of Internet Freedom in Africa 2024: Africa's Electoral Democracy and Technology – Pitfalls and Promises (accessed on 6 November 2025), https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_Report_2024.pdf
44. Human Rights Watch, Tanzania: Repressive Cybercrime Law Used to Silence Critics (accessed on 6 November 2025), https://www.hrw.org/news/2023/03/30/tanzania-repressive-cybercrime-law-used-silence-critics
45. BBC News "Tanzania blocks access to X after government says hackers targeted accounts" (2025) https://www.bbc.com/news/articles/cgmjjdrlkz1o (accessed on 5 January 2026).

need to surveil content and the creators.[46] The exact number of takedown requests is not publicly disclosed by authorities, limiting accountability. These actions are typically carried out without judicial oversight or public explanation, falling short of rights-respecting standards. Oversight of surveillance in Tanzania remains weak in 2025. While the Personal Data Protection Commission exists in law, it lacks full independence and operational capacity. Surveillance and content-restriction decisions are largely executed by executive and regulatory bodies without mandatory judicial review. Parliamentary oversight of intelligence and surveillance activities is minimal, and affected individuals have limited access to remedies or appeals, resulting in low transparency and accountability.

Developments in ICT and Emerging Technologies

In 2025, Tanzania made several significant advances in artificial intelligence and emerging technologies, underpinned by policy, innovation and stakeholder engagement. First, the United Nations Educational, Scientific and Cultural Organization (UNESCO) supported a national AI Readiness Assessment through multi-stakeholder consultations in Dar es Salaam and Zanzibar, culminating in a report presented at the Africa Internet Governance Forum in May.[47] This laid the foundation for Tanzania's emerging national AI strategy. By September, the government unveiled draft national AI guidelines and announced plans to establish a National Institute for Digital and AI Technologies in Dodoma, aimed at building capacity in machine learning, deep learning and responsible AI.[48]

In the media, the AI for Media Development (AI4MD) initiative organised by Tech and Media Convergence and supported by UNESCO, released a report documenting growing AI adoption in journalism.[49] The report highlights how journalists are increasingly using AI tools for writing, fact-checking, translation and trend monitoring, but also warns of low overall awareness and the need for capacity building. Tanzania is also integrating AI into its healthcare system, for example, the Muhimbili Orthopaedic Institute announced that it is deploying AI-powered medical equipment to improve diagnostic capacity and patient flow, making services more efficient and responsive.[50] Finally, on the regulatory front, Tanzania's Ministry of Communication and Information Technology published Ethical Guidelines for AI use, reflecting a commitment to align AI development with national values, data governance, and human rights.[51]

Digital Inclusion

In 2025, Tanzania made significant strides in digital inclusion, driven by both infrastructure development and capacity building. Internet subscriptions surged to 56.3 million by September 2025, raising internet penetration to 82.6%, largely due to expanded mobile broadband coverage with 4G and emerging 5G networks.[52] DataReportal estimates that internet penetration in Tanzania stood at 29.1% of the total population at the end of 2025, reflecting the proportion of individuals who actually use the internet[53]. In contrast, figures cited by the Tanzania Communications Regulatory Authority (TCRA), which are based on active internet subscriptions linked to SIM card registrations rather than unique users, report penetration rates of approximately 82.6%[54], illustrating how subscription-based measurements can

46. Meta Transparency "Government Data Requests: Tanzania" (2025 https://transparency.meta.com/reports/government-data-requests/country/TZ/ (accessed on 17 february 2026).
47. The Citizen "Tanzania to host inaugural AI forum to drive inclusive innovation" (2025) https://www.thecitizen.co.tz/tanzania/news/national/tanzania-to-host-inaugural-ai-forum-to-drive-inclusive-innovation-5089014 (accessed on 14 December 2025)
48. Tech & Media Convergency / UNESCO IPDC "Launch of the UNESCO IPDC Supported Tanzania Media and AI Report" (2025) https://www.unesco.org/en/articles/launch-unesco-ipdc-supported-tanzania-media-and-ai-report(accessed on 10 December 2025)
49. UNESCO "AI ready and responsible: Tanzania unveils national assessment at Africa Internet Governance Forum" (2025) https://www.unesco.org/en/articles/ai-ready-and-responsible-tanzania-unveils-national-assessment-africa-internet-governance-forum (accessed on 10 December 2025).
50. The Respondent Online "Tanzania turns to artificial intelligence to improve healthcare delivery" (2025) https://www.therespondents.co.tz/2025/09/tanzania-turns-to-artificial.html (accessed on 14 December 2025).
51. Ministry of Communication and Information Technology (MICIT) "Guidelines for the Secure and Ethical Use of Artificial Intelligence in Tanzania" (2024)https://www.mawasiliano.go.tz/uploads/documents/sw-1749982790-Guidelines%20for%20AI%20ethical%20USE%20Guideline%20MICIT%202025ver.pdf (accessed on 5 January 2026).
52. Business Insider Tanzania "Tanzania's digital boom: Internet and mobile services soar" (2025) https://businessinsider.co.tz/tanzanias-digital-boom-internet-and-mobile-services-soar/ (accessed on 14 December 2025).
53. DataReportal "Digital 2026: Tanzania" (2025) https://datareportal.com/reports/digital-2026-tanzania (accessed on 5 January 2026).
54. Tanzania Communications Regulatory Authority "Communication Statistics Report for the Quarter Ending September 2025" (2025)https://www.tcra.go.tz/uploads/text-editor/files/Communication%20statistics%20report%20for%20quarter%20one%20ending%20September%202025_1760792820.pdf (accessed on 14 December 2025).

significantly overstate individual internet access. At the same time, the cost of internet access became more affordable, a change credited to government investments and regulatory efforts, which particularly benefited women and rural populations.[55]

On the governance side, Tanzania hosted the 14th Africa Internet Governance Forum (AfIGF) in May 2025, bringing together over 1,000 delegates from across Africa to shape inclusive digital policy and push for equitable, community-led internet governance.[56] In parallel, the National AI Readiness Assessment, conducted in collaboration with UNESCO, outlined a path toward an ethical and inclusive AI strategy aligned with development goals.[57]

Tanzania has adopted several legal and policy measures relevant to children's online safety, primarily through the Cybercrimes Act (2015)[58], the Electronic and Postal Communications (Online Content) Regulations (2020), and the Law of the Child Act[59], which collectively criminalise online child sexual abuse material (CSAM), exploitation, and harmful online content.[123] These laws provide a general framework for protecting children online, including obligations on service providers to restrict prohibited content and cooperate with authorities. However, Tanzania lacks a comprehensive, child-specific digital safety law addressing emerging online risks such as cyberbullying, online grooming, algorithmic harms and data protection for children.[4] In practice, enforcement focuses more on criminal punishment than on prevention, digital literacy or child-centred remedies, limiting alignment with international standards such as the UN Convention on the Rights of the Child and General Comment No. 25 on children's rights in the digital environment.[5]

In 2025, persons with disabilities in Tanzania continue to face significant barriers to meaningful digital access despite existing legal protections. The Persons with Disabilities Act (2010) and the National ICT Policy recognize the rights of PWDs to access information and communication technologies, but implementation remains uneven, with limited enforcement of accessibility standards for websites, mobile applications, and digital public services.[60] Low levels of targeted digital literacy programs for PWDs further exacerbate exclusion, undermining compliance with the UN Convention on the Rights of Persons with Disabilities (CRPD), particularly Articles 9 and 21 on accessibility and access to information.[61]

Universal Service Fund (USF)

Based on the Universal Communications Service Access Fund, UCSAF's official 2025 project reports, Tanzania's Universal Communications Service Access Fund has supported a large-scale expansion of telecommunications infrastructure during the year. By early 2025, UCSAF had contracted the construction of 2,143 communication towers nationwide, targeting 1,974 wards and more than 5,100 villages, with the aim of extending services to over 23 million people. Of these, approximately 1,754 towers were already completed and operational by January 2025, while the remainder were under construction. A major component of this rollout is the 758-tower project under the Digital Tanzania Project, which by mid-2025 was reported to be over 90 percent complete, with more than 680 towers finished across multiple regions, mainly in rural and previously unserved areas.[62] In addition, UCSAF initiated new deployment phases in late 2025, including plans for around 280 additional towers in strategic and border areas, indicating continued expansion beyond the main rollout.[63] This is great progress in connecting more communities that are often marginalised and shows growth in terms of coverage and a significant growth compared to previous years.

55. IPP Media / The Guardian "Tanzania among leading countries with affordable internet access" (2025) https://ippmedia.co.tz/the-guardian/business/read/tanzania-among-leading-countries-with-affordable-internet-access-2025-05-09-124946/ (accessed on 14 December 2025).
56. United Nations Economic Commission for Africa "Tanzania hosts continental push for inclusive internet governance" (2025) https://uneca.org/stories/tanzania-hosts-continental-push-for-inclusive-internet-governance (accessed on 14 December 2025)
57. UNESCO "AI Ready and Responsible: Tanzania unveils national assessment at Africa Internet Governance Forum" (2025) https://www.unesco.org/en/articles/ai-ready-and-responsible-tanzania-unveils-national-assessment-africa-internet-governance-forum (accessed on 14 December 2025).
58. The Cybercrimes Act, Act No. 14 of 2015 (the Cybercrimes Act).
59. The Law of the Child Act, Act No. 21 of 2009 (the Law of the Child Act).
60. The National Information and Communications Technology Policy of 2016 (the National ICT Policy).
61. Convention on the Rights of Persons with Disabilities (CRPD) https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities (accessed on 5 January 2026).
62. IPP Media / The Guardian "UCSAF: 90 pc of 758 recent telecom towers completed" (2025) https://www.ippmedia.com/the-guardian/news/local-news/read/ucsaf-90pc-of-758-recent-telecom-towers-completed-2025-05-27-110231/ (accessed on 5 January 2026).
63. Universal Communications Service Access Fund (UCSAF) "Taarifa ya Miradi ya UCSAF" (2025) http://ucsaf.go.tz/uploads/documents/sw-1755174497-TAARIFA%20YA%20MIRADI%20YA%20UCSAF.pdf(accessed on 5 January 2026).

Conclusion

The 2025 internet shutdown and the repression of digital rights in Tanzania represent a serious erosion of democratic norms, transparency in governance and fundamental freedoms. The national blackout, which lasted for several days during the contested general election, significantly undermined electoral integrity, access to information and civic participation[64]. Civil society organisations documented widespread human rights abuses, including arbitrary arrests, media suppression, and violence against civilians and journalists during and after the elections (LHRC et al., 2025; HRW, 2025). The shutdown not only disrupted communication but also blocked civil society and citizens from reporting and verifying human rights violations[65]. Regrettably, the government's robust deployment of regulatory power also involved amending online-content rules (TCRA, 2025), raising concerns about entrenched censorship and centralised control over digital platforms. Below are some recommendations made for the government, private sector and civil society.

64. Paradigm Initiative 'Press statement: Tanzania's Internet Blackout and Ongoing X Suspension Cost Over US $238 Million, Paradigm Initiative Warns' (2025) https://paradigmhq.org/tanzanias-internet-blackout-cost-over-us-238-million/ (accessed on 6 January 2026). Paradigm Initiative
65. CIPESA, Tanzania's Internet Disruption Undermines Electoral Integrity and Imperils Livelihoods (accessed on 6 November 2025), https://cipesa.org/2025/10/tanzanias-internet-disruption-undermines-electoral-integrity-and-imperils-livelihoods/

Recommendations

The Government should:

- Fully operationalise and enforce a comprehensive data protection framework, including independent oversight and clear safeguards on surveillance, in line with international human rights standards.
- Review, amend, or repeal laws that unduly restrict online expression, including provisions on false information, sedition and cybercrime and ensure judicial oversight of content takedowns and internet restrictions.
- Ensure Universal Communications Service Access Fund (UCSAF) resources are used transparently to bridge the digital divide, with greater focus on affordability, accessibility for persons with disabilities, gender inclusion and digital literacy.
- Strengthen access to information through an independent and effective Information Commission and proactive disclosure of public-interest data, including surveillance practices and USF expenditures.

The Media should:

- Raise public awareness on digital rights, including privacy, freedom of expression, online safety and protection from disinformation.
- Strengthen investigative and public-interest reporting on digital governance, elections, surveillance and internet shutdowns.
- Promote gender-sensitive, disability-inclusive and ethical reporting practices, particularly when covering online abuse and political discourse.

Civil Society Organisations should:

- Monitor and document digital rights violations, including censorship, surveillance, gendered disinformation and election-related restrictions.
- Conduct capacity-building training with the judiciary, law enforcement and security agencies to strengthen understanding of digital rights and international human rights standards.
- Expand digital literacy, online safety and rights awareness programmes targeting women, youth, persons with disabilities and rural communities.
- Pursue strategic litigation and policy advocacy to advance rights-respecting digital governance and accountability.

The private sector should:

- Strengthen data protection and cybersecurity safeguards, ensuring robust protection of users' personal data, particularly for vulnerable groups such as women.
- Invest in digital inclusion initiatives such as affordable access, accessible technologies for persons with disabilities, and programmes that expand meaningful connectivity in rural and underserved communities.
- Adopt and implement human rights–based policies and due diligence frameworks in line with the UN Guiding Principles on Business and Human Rights, ensuring that products and services do not facilitate censorship, unlawful surveillance, or discrimination.
- Increase transparency in content moderation, data requests, and service disruptions, including publishing regular transparency reports detailing government requests and company responses.

The Score Index

Tanzania, 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	X was restricted,internet was shut down during the election and after
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	2	3	There are some parts in existing laws that push for equity and affordable internet such as the Access to Information Act and also the Tanzania Digital Economy Strategy 2024–2034, the Electronic and postal communications act(2010) that promotes expansion of communication services by establishing UCSAF. However given 2025 complete internet shutdown during election,this in essence doesn't translate to practice.
False News Criminalisation	P22(2)	1	1	Although not labeled as false news arrests were made in connection with political expression and online communications

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Sedition Legislation	P22(2)	1	1	The Media Service Act and the Cybercrime Act criminalise “sedition” and in 2025 major opposition and critics were charged for treason.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	Over 1,700 arrests, while at least 10 protest-related deaths were confirmed by the UN, with civil society and opposition groups alleging significantly higher but unverified fatality figures amid the internet shutdown.
Data Protection Legislation.	P42	3	4	Progress was made including the commencement of registration of data controllers and processors, and the rollout of capacity-building and training programmes for public and private sector stakeholders.Still more work needed since law needs reviewing
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	2	2	Media houses have been banned arbitrarily for content they share. Government made requests to some notable Social media including meta to block/ limit the visibility of activist accounts
Invasion of Privacy of	P41	2	2	Laws such as PDPA exist but there is limited compliance, although the commission has done some capacity building to key stakeholders in 2025.Other laws such as Cybercrime act allow for invasion of privacy for national security concerns or investigations.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	4	3	The government uses online media to communicate with citizens such as social media and websites which are often updated in both languages. The UCSAF website shares regular updates as well as TCRA quarterly updates available in Kiswahili language making it more accessible to the public.
AI and Emerging Technologies national strategies	P39(6)	2	2	A Strategy for the Responsible Use of Artificial Intelligence in Tanzania has been drafted, stakeholders have inputted
Children rights online		3	3	The Law of the Child Act enforces general protection of children, while the Cybercrime Act, the electronics and postal communication Act address areas around child pornography and cyberbullying. In its August 2025 decision, the Tanzania Personal Data Protection Commission ruled that a child’s photograph constitutes sensitive personal data and that using or sharing it for commercial purposes without parental consent is unlawful under the Personal Data Protection Act.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Digital Inclusion	P37(3)	4	3	UCSAF ongoing efforts for connectivity including the additional towers it has built in 2025
Total (out of 60):	2024: **27**		**2025 26**	



Togo

By Emmanuel Elolo Agbenonwossi, Fronts Numériques, Togo

Executive Summary

Togo's 2025 digital rights landscape sits at a crossroads between accelerated state modernisation and a sharp contraction of civic space. Since 2016, the country has invested in submarine cables, backbone networks, digital identity, data protection, and cybersecurity institutions, as well as in artificial intelligence strategies and global initiatives, such as the Giga for school connectivity by the International Telecommunications Union (ITU) and United Nations Educational, Scientific and Cultural Organization (UNESCO). This positioning has enabled it to become an ambitious digital reformer in West Africa. In 2025, this ambition was reinforced by the elevation of the Ministry of Public Service Efficiency and Digital Transformation, and the operationalisation of the data protection authority, new oversight for video surveillance and a more active national cyber defence through Cyber Defense Africa and CERT.tg.

At the same time, the year was marked by massive protests against the 2024 constitutional reform and socio-economic pressures, met by lethal force. There were

more than 100 arrests for online expression, disruptions[1] of major platforms, the suspension of France 24 and Radio France Internationale, and a climate of fear shaped by the unresolved Pegasus scandal[2] and the expanded use of cybercrime provisions to police digital speech.

Connectivity improved but remained unequal, with high costs and rural gaps only partially offset by initiatives such as the first community network in Atti Akakpé. People with disabilities, women and low-income groups continued to face structural barriers and digital literacy gaps. Access to information stayed constrained by the non-implementation of the 2016 law and weak proactive disclosure, limiting the ability of media, lawyers and civil society to scrutinise State action.

Against this backdrop, the report finds that Togo's overall compliance with the African Commission's Declaration of Principles on Freedom of Expression and Access to Information in Africa declined compared to 2024, despite progress on data protection, digital inclusion and emerging technologies. The report recommends that the government prioritises legal reform of the cybercrime law, full operationalisation of the access to information framework, stronger guarantees for internet openness, independent oversight of surveillance and data systems, and targeted investments in inclusive connectivity and digital literacy. The report further highlights the need for media, civil society and the private sector to deepen their roles in monitoring rights, expanding digital skills and embedding privacy and accessibility in digital services.

1. Open Observatory of Network Interference (OONI). (2025). Togo: Network disruptions measurement data, June–July 2025., (Accessed 5 February 2026)https://ooni.org
2. Reporters Without Borders (RSF). (2024). Togo: Pegasus spyware used against journalists.https://rsf.org/en/togo, (Accessed 5 February 2026)

Introduction

Since 2016, Togo has pursued an ambitious digital transformation agenda aimed at strengthening state capacity, improving public service delivery and positioning the country as a digital reformer in West Africa. This period saw sustained investment in connectivity infrastructure, including submarine cables and fibre backbone expansion, alongside the rollout of digital public platforms. The adoption of a data protection law in 2019 and the creation of cybersecurity and digital regulatory institutions provided an initial legal and institutional framework for digital governance. The subsequent deployment of a biometric digital identity system marked a decisive shift, embedding digital technologies at the core of public administration and state authority.

Parallel to these reforms, persistent concerns emerged regarding civic space, freedom of expression and privacy in the digital sphere. The 2017 internet shutdown during political protests signalled early on that digital infrastructure could be constrained in moments of political tension, a practice later deemed incompatible with regional human rights standards by the ECOWAS Court[3]. In the years that followed, criminal law and cybercrime provisions were increasingly used to police online expression, including criticism of public officials and governance practices. Independent media and journalists operated under growing pressure, shaped by judicial harassment, economic vulnerability and surveillance risks, gradually narrowing the space for critical digital discourse.

These structural tensions culminated between 2024 and 2025, when constitutional reform heightened political uncertainty and digital platforms became central arenas for civic mobilisation, particularly among youth, artists, influencers and diaspora networks. Social media evolved into a primary space for political organisation and public debate, prompting a restrictive State response marked by arrests, platform disruptions and the

3. Amnesty International Togo, & 7 Ors v. The Togolese Republic, ECOWAS Community Court of Justice, Suit No. ECW/CCJ/APP/61/18, Judgment No. ECW/CCJ/JUD/09/20 (25 June 2020), (Accessed 5 February 2026)

suspension of international broadcasters. At the same time, the government continued advancing its digital agenda, including biometric identity expansion and AI policy development, underscoring a core paradox. While digital systems are promoted as tools for modernisation and efficiency, their deployment within fragile governance contexts has intensified concerns over accountability, concentration of power and the long term sustainability of rights based digital transformation.

Internet Access and Disruptions

Togo's connectivity profile in 2025 illustrates a country that has advanced considerably in building its digital infrastructure but still grapples with the deeper governance questions that accompany the expansion of the digital sphere. Over recent years, the arrival of new submarine cable capacity, the reinforcement of national fibre links, and the rise in mobile broadband adoption have helped strengthen the country's digital foundations. In major urban centres, connectivity is increasingly reliable and digital services are gaining prominence in administrative, commercial and educational settings. Yet these gains remain uneven. Rural communities continue to face lower quality coverage, higher effective costs in relation to household income, and persistent constraints linked to limited electrification. As a result, the distribution of digital opportunity in the country remains structurally imbalanced.

The events of mid-2025 demonstrated how quickly these technical gains can become vulnerable when political tensions rise. As youth-led demonstrations expanded across Lomé and other urban centres, several independent monitoring organisations recorded consistent disruptions affecting the platforms most widely used for communication and information sharing. Measurements conducted by the Open Observatory of Network Interference, corroborated by Internet Society monitoring tools, revealed repeated connection failures on WhatsApp, Facebook, Signal, Telegram, YouTube, and other high-traffic services beginning on June 26. These disturbances were documented across multiple operators, including Moov Africa, Togo Cellulaire, CanalBox and YAS Telecom, and their timing coincided with the most visible episodes of civic mobilisation in the country.

National observers confirmed the pattern. Internet Society Togo reported unusual service degradation that disproportionately affected platforms central to civic communication. Journalists and civil society organisations described significant difficulty in uploading videos, verifying incidents on the ground, or coordinating support for families seeking information about detained or injured relatives. Human rights defenders noted that the disruptions delayed the documentation of allegations of ill treatment and complicated emergency coordination with legal counsellors and partner organisations outside Togo.

The broader economic and social ramifications extended well beyond the immediate political context. Small businesses that rely on messaging applications to maintain customer engagement experienced rapid declines in activity. Students preparing for examinations found that collaborative study channels and online learning tools were intermittently inaccessible. Drivers, delivery workers and other service providers who depend on platform-based communication saw their daily operations disrupted. These consequences underscore the extent to which digital connectivity has become essential to economic participation and social coordination and how even targeted restrictions can generate cascading effects across multiple sectors of society.

The interruptions also had implications for public trust in the digital environment. The restrictions echoed earlier concerns raised across the region about the use of network management tools during periods of political sensitivity. Domestic organisations, including the Internet Society Togo chapter and Association Togolaise des Consommateurs (a consumer rights association), called for the restoration of full access and emphasised the importance of maintaining open communication channels during times of national uncertainty. Regional actors referenced the 2020 judgment of the ECOWAS Court of Justice, which affirmed that restrictions on internet access must comply with principles of legality, necessity and proportionality. These interventions reflected a growing regional consensus that reliable connectivity is a matter of public interest and not merely a technical service.

Although the disruptions in 2025 did not take the form of a complete nationwide outage, their targeted nature raises important policy questions. They point to the need for transparent decision-making processes governing the management of digital networks and stronger institutional safeguards to ensure that measures affecting access do not inadvertently restrict fundamental freedoms. The experi

ence of 2025 suggests that the credibility of Togo's digital transformation will depend not only on the expansion of infrastructure but also on the establishment of governance practices that protect the resilience of the digital ecosystem in periods of political stress.

Access to Information

In 2025, access to information and freedom of expression in Togo continued to be constrained by longstanding structural deficiencies that have been documented by national and international observers over several years. While a legal framework governing access to public information formally exists, its implementation remains weak, limiting transparency and directly affecting the ability of journalists, civil society organisations and citizens to exercise freedom of expression on the basis of verified and authoritative information.

The legal basis for access to information is provided by the 2016 law on access to public information[4] and its 2017 implementing decree, which establishes procedures for submitting requests, designates information officers within public institutions, and provides for recourse through the Office of the Mediator of the Republic. However, assessments by civil society organisations and governance experts, including findings referenced in parallel reporting to international anti-corruption mechanisms, indicate that these provisions are rarely operational in practice. Requests for information are often unanswered, response timelines are not respected, and refusals are generally not formalised or justified in writing. As a result, the access to information framework remains largely ineffective as a practical tool for transparency and accountability.

This limited access to official information has direct implications for freedom of expression. Journalists interviewed for recent monitoring exercises have consistently reported difficulties obtaining official documents, budgetary data and regulatory decisions, particularly in areas related to public finance, procurement, security and governance. These constraints weaken investigative journalism and reduce the capacity of media outlets to provide evidence based reporting. Civil society organisations engaged in public policy analysis similarly report[5] relying on informal networks rather than institutional disclosure mechanisms, which increases vulnerability to pressure and undermines the quality of public debate.

Developments during 2025 further highlighted the interdependence between access to information and freedom of expression. During civic mobilisations between May and July, public demand for timely and accurate information increased sharply, particularly regarding demonstrations, arrests, injuries and government responses[6]. At the same time, the space for independent information narrowed. On June 16 2025, the High Authority for Audiovisual and Communication suspended[7] the broadcasting of France 24 and Radio France Internationale for a period of three months, a decision reported by international media outlets and widely criticised by press freedom organisations. This measure significantly reduced access to international independent reporting at a moment of heightened political sensitivity.

Domestic media outlets attempted to compensate for this loss of external sources, but continued to face structural challenges documented by press freedom organisations, including limited access to official sources, financial fragility and increased risks of administrative or judicial pressure. Reports by international journalist protection bodies indicate that these conditions contributed to heightened self censorship and reduced on the ground coverage of sensitive events.

The digital information environment was also affected during this period. According to monitoring by regional media freedom organisations, disruptions to internet connectivity and online services were reported in late June 2025, coinciding with protest related events[8]. These dis

4. République togolaise. 2017. Décret n° 2017 104 PR du 10 août 2017 portant application de la loi sur l'accès à l'information publique. Gouvernement du Togo. https://communication.gouv.tg/wp-content/uploads/2020/11/decret-n%C2%B02017-104.pdf, (Accessed 5 February 2026)
5. UNCAC Coalition. 2023. Parallel report on Togo. United Nations Convention against Corruption Coalition. https://uncaccoalition.org/wp-content/uploads/FINAL_Parallel-Report-TOGO-UNCAC_EN.pdf, (Accessed 5 February 2026)
6. Amnesty International. 2025. Togo. Protesters tortured as authorities crack down on dissent. Amnesty International. https://www.amnesty.org/en/latest/news/2025/06/togo-protesters-tortured/ (Accessed 5 February 2026)
7. Reuters. 2025. Togo suspends RFI and France 24 for three months, communications authority says. Reuters. https://www.reuters.com/business/media-telecom/togo-suspends-rfi-france-24-three-months-communications-authority-says-2025-06-16/, (Accessed 5 February 2026)
8. Media Foundation for West Africa. 2025. Internet disruptions amid post protest repression in Togo. Media Foundation for West Africa. https://mfwa.org/country-highlights/togo-internet-disruptions-amid-post-protest-repression/, (Accessed 5 February 2026)

ruptions limited the ability of journalists and citizens to communicate, document events in real time and access independent sources of information. As a consequence, public discourse increasingly relied on fragmented and unverified information circulating through social media platforms rather than on transparent institutional communication.

Arbitrary arrests linked to the exercise of freedom of expression were documented by multiple credible sources throughout 2025[9]. International media reported approximately 80 arrests during protest related events in June alone. Human rights organisations documented a broader pattern extending beyond the immediate protest period, reporting that at least 133 young activists were arbitrarily arrested between June and October 2025 in connection with protest participation, online expression or public criticism of authorities[10]. In several cases, detainees were reportedly held without prompt access to legal counsel, raising concerns among legal practitioners regarding due process guarantees.

Several emblematic cases illustrate the broader pattern observed. In May 2025, a prominent musician was arrested following critical public statements and online publications[11]. His subsequent appearance in a video apology circulated on social media was described by media freedom organisations as indicative of coercion. In early June 2025, a journalist working for an international broadcaster was detained while covering demonstrations and reportedly forced by security forces to delete recorded footage, an incident documented by international journalist protection organisations[12]. These cases, combined with the suspension of international broadcasters, contributed to a climate of intimidation and had a chilling effect on journalistic activity and public expression.

9. Associated Press. 2025. Togo arrests dozens after protests over constitution change. Associated Press. https://apnews.com/article/e61f8334f1dc4483d446770b35aa9549, (Accessed 5 February 2026)
10. Front Line Defenders. 2025. Repression of Gen Z in Togo. 48 activists must be urgently released. Front Line Defenders. https://www.frontlinedefenders.org/en/statement-report/repression-gen-z-togo-48-activists-must-be-urgently-released, (Accessed 5 February 2026)
11. Media Foundation for West Africa. 2025. Arrested rapper reappears in viral apology video on social media. Media Foundation for West Africa. https://mfwa.org/country-highlights/togo-arrested-rapper-reappears-in-viral-apology-video-on-social-media/, (Accessed 5 February 2026)
12. Committee to Protect Journalists. 2025. Togo detains TV5 Monde journalist, forces deletion of protest videos. Committee to Protect Journalists. https://cpj.org/2025/06/togo-detains-tv5-monde-journalist-forces-deletion-of-protest-videos/(Accessed 5 February 2026)

The continued digitalisation of public administration did not offset these constraints. While online platforms expanded access to administrative services, independent assessments indicate that proactive disclosure of public information remained limited. Data on budget execution, infrastructure projects, regulatory decisions and policy implementation were not published systematically. As already observed in earlier research cycles, digital transformation improved administrative efficiency without strengthening transparency, public oversight or the right to information.

Overall, developments in 2025 confirmed and, in some respects, intensified concerns identified in previous reporting. The absence of an effective access to information regime, combined with restrictions on media freedom, digital disruptions and arrests linked to public expression, continued to limit access to verified information and weaken the conditions for free, informed and pluralistic public debate. In the absence of sustained institutional reforms and stronger protections for freedom of expression, administrative modernisation has not translated into greater transparency or increased public trust in state institutions.

Data Protection And Cybersecurity

Togo's data governance framework entered a more active phase in 2025 with the gradual operationalisation of the Instance de Protection des Données à Caractère Personnel[13]. The authority, established under the 2019 personal data protection law, began to transition beyond its foundational phase and assumed a more pronounced regulatory presence within the national digital ecosystem. Its activation came at a time when government services, financial institutions and private companies increasingly rely on the collection and processing of personal information. The biometric identity programme expanded its coverage, digital administrative services became more widely used, and a broader part of citizens' daily interactions with the state moved onto digital platforms. These de

13. Togo First. (2025, April 1). Togo: National Data Protection Authority launches as Cyber Defence Africa strengthens cyber resilience. https://www.togofirst.com/en/itc/0104-16053-togo-national-data-protection-authority-launches (Accessed 5 February 2026)

velopments elevated the importance of an oversight institution capable of guiding responsible data management, clarifying compliance obligations and articulating the rights of individuals in relation to their personal information.

The authority's work in 2025 focused on issuing guidance to public and private operators, improving public understanding of data rights and clarifying the obligations that accompany the handling of personal information. This was particularly important in the context of expanding digital public services and centralising biometric identifiers. Many citizens expressed a growing expectation that data collected for public service delivery be handled transparently, securely and with clear limitations on secondary use. The authority's emergence offered an initial reference point for these expectations, although its limited resources and modest operational capacity underscored the scale of the challenge that lies ahead.

A significant regulatory development concerned the governance of video surveillance in public and semi-public spaces. The proliferation of cameras in commercial centres, residential compounds and public institutions had outpaced the existence of a formal oversight mechanism. In 2025, the data protection authority introduced a requirement that any installation of video surveillance systems in locations accessible to the public must undergo a formal notification and authorisation process. Operators must register surveillance systems, demonstrate that their purpose complies with national privacy standards and visibly display proof of authorisation. Recordings produced by systems that do not comply with these requirements may not be admissible in legal procedures. This measure signalled an effort to introduce order and accountability into an expanding surveillance ecosystem and to ensure that public security objectives do not erode the privacy rights of individuals.

While these institutional developments marked progress, they occurred within a cybersecurity environment that was becoming increasingly active and increasingly sophisticated. Cyber Defence Africa, established in 2019 through a public-private partnership, continued to serve as the national centre for cyber defence operations, functioning both as the national Security Operations Centre and as CERT.tg. Throughout 2025, CDA expanded its technical capacity, broadened its analytical functions and worked closely with public administrations, banks and service providers to detect intrusions and mitigate risks. Its public alerts on phishing attacks, fraudulent payment schemes, data theft attempts, and vulnerabilities affecting corporate and government systems have become more frequent, reflecting the growing exposure of the country to cyber threats.

CERT.tg's activities played an important preventive role by helping organisations recognise emerging threats and by encouraging citizens to adopt basic digital hygiene practices. These interventions were particularly relevant given the parallel expansion of digital identity, digital financial services and electronic platforms for administrative procedures. As more users engage in digital transactions, the risk of identity theft, fraud and manipulation of personal or financial data increases.
The visibility of CERT.tg in 2025 helped address these vulnerabilities and contributed to a more informed public conversation about digital security.

Cyber Defence Africa also deepened its cooperation with regional and international partners. Through capacity-building exercises, joint analysis initiatives, and cooperation agreements with peer institutions, the organisation participated in efforts to strengthen Africa's collective cyber resilience. The cooperation agreement signed in 2025 with a southern African state illustrated this outward engagement and signalled Togo's intention to position itself as an emerging actor in African cybersecurity.

These institutional developments took place in a political and social environment that remains sensitive to issues of surveillance and digital monitoring. Past allegations involving intrusive technologies created an enduring perception of risk among journalists, civil society organisations and political actors. Although no confirmed cases emerged in 2025, this perception shaped how many individuals interacted with digital platforms and how they interpreted the growing presence of cybersecurity institutions.
The overlap between cyber defence mandates, national security interests and data governance responsibilities requires careful management to avoid reinforcing concerns about privacy and undue monitoring.

The developments observed in 2025 highlight both the consolidation and the structural tensions inherent in the construction of a contemporary data and cybersecurity governance architecture within a rapidly digitalising environment.

Beyond the existence of Law No. 2019 014, the operationalisation[14] of the Instance de Protection des Données à Caractère Personnel marked a decisive institutional shift, transforming a statutory framework into an active supervisory mechanism capable of issuing guidance, framing compliance obligations and serving as a reference point for the protection of private life and personal data processing.

The introduction in 2025 of a formal declaration and authorisation regime for video surveillance systems[15] further translated abstract rights into enforceable administrative procedures. By requiring prior notification, documented justification and visible proof of authorisation for surveillance devices installed in publicly accessible spaces, the authority embedded legality and proportionality tests into everyday security practices, thereby strengthening procedural safeguards for individuals.

Taken together, these elements position Togo with a structured legal base, an identifiable oversight authority[16], a defined regulatory mechanism for surveillance technologies and an operational cyber defence infrastructure capable of responding to systemic risks. This integration constitutes a foundational condition for sustaining digital transformation while anchoring it within a framework attentive to rights, security and institutional accountability.

Privacy And State Surveillance

State surveillance shaped digital life in Togo throughout 2025 in ways that were both visible and subtle, forming a dense layer of control around a political landscape already marked by tension. The country entered the year with an unresolved legacy from the Pegasus spyware scandal. In 2021, forensic analysis by Amnesty International's Security Lab and reporting by international media confirmed that the phones of the investigative journalist Ferdinand Ayité and other Togolese journalists had been selected for potential infection with Pegasus, a sophisticated surveillance tool designed by the Israeli company NSO Group. The investigations provoked international concern, yet no public inquiry was held within the country. Ayité himself warned in an interview with Le Monde that the Togolese authorities had invested in listening systems and maintained privileged relations with Israeli networks composed of former intelligence operatives. These statements became an enduring reference point for many journalists and activists, shaping their understanding of digital vulnerability through 2025.

This history mattered because much of the country's political and social life has shifted to digital platforms. Young people, artists, journalists and civic actors increasingly relied on TikTok, Facebook, Instagram and WhatsApp to express their views, document grievances, and organise demonstrations. As concerns about the 2024 constitutional reform intensified, digital spaces became the primary arena for debate and mobilisation. When youth-led protests began in late May and gained momentum quickly throughout June, online expression assumed heightened political significance.

The state's response relied heavily on monitoring digital activity and using broad legal provisions from the 2018 cybercrime law. Human rights organisations reported that more than 100 individuals were arrested between June 5 and October 31 for conduct linked to online expression. Approximately 48 remained in detention at the end of the year. Testimonies from detainees and lawyers indicated that interrogations commonly focused on social media activity. People were confronted with screenshots of TikTok live sessions, Facebook comments or messages shared through WhatsApp groups and were asked to explain their links with specific accounts, organisers or diaspora figures. The pattern demonstrated that the authorities systematically used online traces as a central element in identifying participants and sympathisers in the mobilisation.

The arrest and treatment of the rapper Aamron brought these dynamics into sharp relief[17]. Aamron, who used TikTok and other platforms to critique political

14. CIO Mag. (2025, March 29). Togo: The Personal Data Protection Authority begins its mission. https://cio-mag.com/protection-des-donnees-personnelles-au-togo-lipdcp-entame-sa-mission/ (Accessed 5 February 2026)
15. Civic Medias. (2025, July 27). Togo: IPDCP launches official declaration process for video surveillance systems. https://civicmedias.info/cv/index.php/2025/07/27/togo-ipdcp-lancement-officiel-du-processus-de-declaration-des-dispositifs-de-videosurveillance/ (Accessed 5 February 2026)
16. The Guardian. (2025, July 10). One too many: Rapper's arrest sparks protests against Togo's ruling dynasty. https://www.theguardian.com/world/2025/jul/10/rapper-aamron-arrest-protests-togo-ruling-dynasty

17. République Togolaise. (2025, November 29). L'Internet Society déploie son premier réseau communautaire.

leaders, was detained at home, transferred to a psychiatric institution and later appeared in a video expressing apologies under unclear conditions. His case resonated deeply with young people because it illustrated how digital visibility could translate rapidly into personal vulnerability. For many, it confirmed that online expression no longer provided any degree of insulation from State intervention.

The experience of Traoré Leïla reinforced this perception. National media and activists reported that she had been arrested while breastfeeding her infant and remained in detention under security-related charges. Although details about her case are incomplete, she is widely described as a detainee arrested because of her perceived links to opposition networks. Her situation highlights the vulnerability of individuals who are suspected of being connected to political critics, regardless of whether this connection is made through digital interactions or social proximity.

These practices unfolded within a broader cybersecurity environment that continued to expand in capability as explained earlier with the creation of Cyber Defence Africa qnd the the national Security Operations Centre and CERT.tg. Throughout 2025, the institution monitored national networks in real time, issued alerts on phishing campaigns and cyber threats and strengthened its technical infrastructure. These capabilities are essential for protecting critical systems, but they also contribute to a public perception that the State has significant visibility into digital communications. The boundary between cybersecurity and surveillance is not always clear to users, particularly in a year marked by arrests and interrogations stemming from online activity.

The cumulative effect of these dynamics influenced patterns of online behaviour throughout 2025. Journalists exercised heightened caution when addressing politically sensitive subjects, often avoiding mainstream messaging platforms for substantive exchanges. Civil society actors redirected strategic discussions toward more discreet communication channels, mindful of the potential exposure associated with open digital spaces. Diaspora commentators, including exiled investigative journalist Ferdinand Ayité, who continued to analyse national political developments through regular live online programmes, were conscious that interactions with contacts inside the country could inadvertently place those individuals under scrutiny. Among younger users in particular, deliberate efforts to reduce digital visibility became more common, reflecting an awareness that the monitoring of digital traces had become embedded within the broader security posture of the state.

What defined state surveillance in Togo in 2025 was not the presence of a single system but the convergence of legal authority, technical capacity and political will. Digital expression was closely watched, online traces were used to identify and detain critics, and past revelations about spyware continued to shape public expectations. In this environment, the boundary between the private and the public sphere narrowed considerably and the digital space, far from offering protection, became one of the primary vectors through which the state exerted its security presence.

Developments in ICT and Emerging Technologies

ICT development in Togo in 2025 was characterised by the consolidation of digital public infrastructure and a deliberate shift toward emerging technologies as instruments of state modernisation. The government continued to treat digital transformation as a national priority, with an emphasis on the role of data, connectivity and innovation in improving administrative efficiency and stimulating economic development.

The year saw notable advancement in national work on artificial intelligence (AI). Authorities intensified consultations on the country's future AI strategy, framing AI as a tool to strengthen public administration, support decision-making, and modernise priority sectors such as agriculture, health, and education. Research institutions, technical experts and government bodies engaged in working sessions aimed at defining the foundations of an AI ecosystem capable of relying on local data, skilled human capital and clear governance principles. A series of national meetings gave visibility to these debates and placed AI within a larger conversation about economic competitiveness and public service reform.

Innovation in the education sector continued through Togo's association with the Giga initiative, the global school-connectivity programme led by UNICEF and the ITU. Giga uses artificial intelligence, satellite mapping and infrastructure modelling to identify unconnected schools and design cost-effective expansion strategies. For Togo, participation in Giga is more

than a connectivity exercise. It provides a structured methodology for mapping national infrastructure gaps and encourages integration of schools into broader rural broadband planning. It also strengthens cooperation with international partners and supports a longer-term vision in which connectivity becomes a fundamental layer of educational development. As Giga has now mapped more than 1 million schools globally and developed financing models based on aggregated demand, the approach provides practical tools for countries, including Togo, to design realistic national school connectivity plans.

Digital public administration also progressed in 2025, with continued efforts to strengthen interoperability between government systems and expand access to online public services. Institutional actors worked to modernise internal information systems and reorganise administrative processes around digital platforms. Several government bodies began relying more heavily on integrated data systems to monitor service delivery and improve operational efficiency. These efforts were supported by international partners through programmes aimed at public-sector digital governance, infrastructure development and institutional capacity building.

Emerging technologies featured prominently in discussions about economic transformation and national competitiveness. Authorities explored how innovation in data analytics, geospatial mapping and automation could be applied in domains such as land management, transport, agriculture and climate adaptation. Pilot projects in these areas reflected a growing interest in using technology to address longstanding structural challenges. Regional organisations and development partners provided additional platforms for exchange on responsible innovation, digital inclusion and the development of human capital for the technology sector.

Togo also pursued regional cooperation in the field of cybersecurity and digital resilience, recognising that emerging technologies require stable and secure infrastructure. Government agencies engaged in collaborative agreements with other African States, focusing on information sharing, mutual support for incident response and joint capacity building. These partnerships highlighted a willingness to situate national advances within a broader regional framework and to enhance Africa's collective preparedness for the digital economy.

Digital Inclusion

Digital inclusion in Togo in 2025 reflected a combination of progress and persistent structural constraints. Urban connectivity continued to improve, yet access remained uneven across regions, income groups and social categories. Rural communities, in particular, faced weaker coverage, limited electrification, and high costs that constrained the regular use of digital services. These disparities shaped daily access to information, education and administrative services.

A notable development occurred in November 2025 with the inauguration of the country's first community network in Atti Akakpé, implemented by the Internet Society of Togo in partnership with local stakeholders. The initiative introduced a locally managed model of connectivity designed for areas where commercial operators have little presence. It offered an alternative path for rural access, combining infrastructure with community participation and the possibility of local digital training. The experience demonstrated that targeted community-driven solutions can complement national digital strategies, especially in regions where infrastructure gaps remain significant.
Affordability continued to influence who could benefit from digital services. The cost of devices and mobile data remained high relative to average income, limiting sustained connectivity for many households. Students, informal workers and low-income families often relied on shared devices or intermittent access, which restricted their ability to engage fully with online learning, financial platforms or government services that increasingly operated digitally.

People with disabilities encountered additional obstacles in accessing digital platforms. Public sector systems were not consistently designed with accessibility requirements in mind. Assistive technologies such as screen readers or captioning were not always compatible with government interfaces. Advocacy groups continued to call for stronger integration of universal design standards in both public and private digital services.

Gender also shaped digital access. Women, especially in rural areas, reported lower device ownership, less frequent internet use and reduced access to digital training opportunities. Social constraints, economic limitations and safety concerns affected their participation in online spaces. Periods of heightened political activity brought additional risks of online harassment and intimidation directed at

women who engaged publicly on digital platforms.

Children and young people occupied an increasingly central position in national discussions about digital opportunity.

The Universal Service Fund remained an important instrument for addressing connectivity gaps, but public visibility into its operations was limited. Without clear reporting on allocation and implementation, it was difficult to determine the extent to which the fund supported underserved communities, persons with disabilities or low-income users. Civil society continued to advocate for greater transparency to ensure that the fund played its intended role in reducing inequalities in digital access.

Digital literacy varied widely among population groups. Young people often learned informally through social networks, while older adults and rural residents faced greater challenges navigating online platforms or using digital tools required for public services. As administrative systems expanded online, the need for broad-based digital competence became more apparent across the country.

These intersecting factors shaped the digital inclusion landscape of 2025. Connectivity expanded, but real access depended on affordability, geography, skills and social circumstances. The emergence of community-driven models, such as the Atti Akakpé network[18], added a promising dimension to the national landscape, demonstrating how local initiatives can help address gaps that national infrastructure alone cannot immediately fill.

18. République Togolaise. https://www.republicoftogo.com/toutes-les-rubriques/high-tech/l-internet-society-deploie-son-premier-reseau-communautaire (Accessed 5 February 2026)

Conclusion

Togo's digital trajectory in 2025 revealed a country advancing rapidly in the construction of modern public infrastructure while confronting the limits of a governance environment under significant strain. Investments in digital identity, public service platforms, connectivity initiatives and early work on artificial intelligence confirmed the growing centrality of technology in national development. These reforms broadened the state's administrative capabilities and offered a foundation for long-term transformation.

At the same time, the year exposed the tensions that arise when technological progress unfolds alongside a deteriorating civic and political climate. The widespread use of the cybercrime law against online expression, the arrests that followed digital mobilisation, the disruptions affecting major platforms during public demonstrations and the constrained information environment all demonstrated how digital systems can become intertwined with political control. The lack of operational access to the information framework and limited transparency in several areas of public administration further complicated the relationship between digital governance and public trust.

Digital inclusion continued to depend heavily on geography, income, gender and skills. The inauguration of the Atti Akakpé community network illustrated the potential of community-driven solutions, while the Giga initiative offered a structured approach to school connectivity. Yet, many citizens still faced barriers that limited their ability to fully benefit from the country's digital transformation.

The developments of the year highlighted a central question for the future of digital governance in Togo. The country has built important technical foundations and signalled a clear ambition. Its next steps will depend on the degree to which these systems can operate within a framework that protects rights, encourages transparency and ensures that technology strengthens the relationship between citizens and the state rather than narrowing it.

Recommendations

The Government should:

- Operationalise the 2016 Access to Information law by issuing the implementing guidelines and creating a functional mechanism for receiving, processing and appealing information requests.
- Reform provisions of the 2018 cybercrime law to ensure that offences related to insult and false information cannot be used to criminalise legitimate online expression.
- Strengthen the independence and operational capacity of the national data protection authority, ensuring that its oversight applies to both public and private actors processing personal data.
- Establish a coherent and enforceable safeguards framework governing the deployment of biometric identification systems, video surveillance infrastructures, automated decision making tools and the interception or analysis of digital communications, including phone calls. Such a framework should define transparent rules on purpose limitation, data minimisation, storage duration, access controls and independent oversight, ensuring that security and administrative objectives are pursued within clearly bounded legal parameters and subject to effective accountability mechanisms.
- Guarantee uninterrupted access to the internet during periods of public tension and adopt clear procedures aligned with regional human rights standards for any restriction on digital services.
- Improve rural connectivity by publishing transparent plans for infrastructure expansion and ensuring targeted use of the Universal Service Fund.
- Integrate accessibility standards into all public digital platforms and ensure that services can be used by persons with disabilities without barriers.

The Media should:

- Expand reporting on digital governance, data protection, artificial intelligence and the societal implications of digital transformation.
- Strengthen investigative work on public finance, procurement and digital infrastructure while maintaining strong ethical and editorial standards.
- Engage in structured dialogue with State institutions to clarify procedures for accessing public information and overcoming administrative blockages.
- Provide digital security training for journalists and newsrooms to reduce risks during periods of political sensitivity.

Civil Society Organisations should:

- Continue monitoring digital rights and documenting restrictions on online expression through rigorous and evidence-based methods.
- Expand community-based digital literacy programmes, particularly in rural areas and among women, youth and marginalised groups.
- Build partnerships with academic and technical communities to analyse the impact of digital identity systems, surveillance technologies and emerging AI policies.
- Engage with regional and continental bodies to strengthen cross-border advocacy and align national debates with broader African governance frameworks.

The Pivate Sector should:

- Improve the affordability of connectivity and digital services by developing accessible pricing models, especially for low-income and rural users.
- Adopt robust internal policies on data protection and privacy, ensuring full compliance with national legislation and global standards.
- Integrate accessibility and inclusive design into all digital products and platforms.
- Collaborate with universities, training centres and incubators to support the development of digital skills relevant to emerging technologies such as artificial intelligence, cloud services and geospatial systems.

The Score Index

Tanzania, 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 Access and Disruptions	P37	4	3	Infrastructure improved, but targeted platform disruptions during June and July protests reduced compliance with principles of open and uninterrupted access.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	3	3	Despite improvements in connectivity infrastructure and initiatives such as the expansion of fibre networks, participation in the Giga programme and the emergence of community connectivity projects, Togo still lacks a comprehensive policy framework specifically aimed at ensuring universal, equitable, affordable and meaningful access to the internet. In addition, no publicly available reports or verified data exist on the collection, management or effective use of the Universal Service Fund, making it difficult to assess its contribution to expanding connectivity or supporting underserved populations.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
False News Criminalisation	P22(2)	2	1	Provisions of the cybercrime law continued to criminalise online expression and were used extensively in 2025 to justify arrests linked to commentary on public affairs.
Sedition Legislation	P22(2)	3	2	The cybercrime law retained broad offences that facilitated the prosecution of online criticism, including TikTok videos and social media commentary The cybercrime law retained broad offences that facilitated the prosecution of online criticism, including TikTok videos and social media commentary
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	More than 100 individuals were arrested between June and October for online expression, and approximately 48 remained in detention at the year's end.
Data Protection Legislation.	P42	4	4	The data protection authority became operational in 2025 and introduced surveillance regulation, but enforcement capacity remained limited.
Online content Removal Without Process	P38 and P39(4)	2	2	Temporary restrictions on major digital platforms during protests were not accompanied by transparent or publicly communicated processes.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Invasion of Privacy of Communications	P41	1	1	Past Pegasus revelatons remained unresolved, and public perception of surveillance persisted, reinforced by the use of digital traces in investigations.
Failure to proactively Disclose Information	P29(3)	3	3	The 2016 access to information law remained inoperative, and ministries did not publish regular data or reports.
AI and Emerging Technologies Governance	P39(6)	2	3	National consultations on artificial intelligence expanded and policy foundations for AI governance began to take shape through multi stakeholder discussions and technical engagement with research institutions and public authorities. In October 2025, Togo also signed the United Nations Convention against Cybercrime, signalling increased engagement with emerging global governance frameworks related to digital technologies and cybersecurity. However, no national artificial intelligence strategy or formal regulatory framework was published during the year.
Adoption of specific Child Online Safety	P37(5)	2	2	Digital education expanded, but a comprehensive national framework for child online protection did not exist.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Digital Inclusion	P37(3)	2	3	Connectivity improved, and community networks emerged, yet rural, affordability and accessibility gaps remained substantial.
Total (out of 60):	2024: **29**	2025 **28**		Togo made progress in infrastructure and institutional development but experienced significant regression in freedom of expression, access to information and protection from arbitrary monitoring.

Togo's 2025 Score Index Compared to 2024

The 2025 Score Index reflects a slight decline compared to 2024, with the overall score decreasing from 29 to 28 out of 60. While the numerical change appears limited, the distribution of the indicators reveals a continued divergence between progress in institutional and infrastructural development and persistent pressures affecting fundamental digital rights. Compared to 2024, most downward movements relate to restrictions on online expression, the use of legal provisions to prosecute digital speech and ongoing concerns about transparency and surveillance.

In 2024, the country had already faced sustained concerns regarding prosecutions linked to online expression. The situation escalated significantly after the civic mobilisation of June and July 2025. According to the World Organisation Against Torture and partner organisations, at least 133 young Togolese activists were arbitrarily arrested from 5 June 2025 for having "spoken out or gathered peacefully," and 48 remained in detention at the time of their October 2025 statement. These figures illustrate the scale of the arrests following the mobilisation and reflect the increasingly fraught intersection between civic protest, digital expression and state security responses during the year.

Internet access also experienced a decline. In 2024, Togo maintained relatively stable connectivity despite regional outages. In 2025, however, targeted disruptions of platforms used for communication during the protests reduced the country's alignment with the ACHPR principles on open and uninterrupted access. The change was not due to infrastructure weakness but rather to the use of access restrictions in a moment of political tension.

The indicators related to false news and sedition offences remained among the lowest in the index. Their impact became more visible in 2025 as legal provisions governing sedition and cybercrime were increasingly used in prosecutions related to online publications and social media commentary. In the previous year, these provisions were mainly identified as problematic in principle. During 2025 they became operational instruments in the prosecution of digital expression, particularly among young users active on platforms such as TikTok, Instagram and Facebook.

The score on access to information did not improve. The structural limitation identified in 2024 remained unchanged. The 2016 access to information law continued to lack effective implementation, and ministries did not systematically publish public data or reports. The suspension of two major international broadcasters during a period of political tension further constrained access to independent information.

Privacy and surveillance concerns also remained significant. Although no new spyware investigations were disclosed in 2025, the continued resonance of the Pegasus revelations, combined with the use of digital traces and social media monitoring in investigations linked to protest activity, reinforced public perceptions of vulnerability and maintained the indicator at the lowest level.

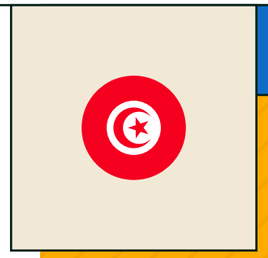
Not all developments were negative. Data protection legislation maintained a relatively strong score due to the operationalisation of the national data protection authority and the introduction of regulatory oversight for surveillance systems. This institutional development represents a

consolidation of the country's data governance architecture, even though enforcement capacity remains limited.

Some progress was also observed in digital inclusion. The inauguration of the first community network in Atti Akakpé demonstrated innovative approaches to rural connectivity, while the continuation of school connectivity efforts under the Giga initiative provided additional momentum for expanding access to digital infrastructure.

The indicator on emerging technologies also improved. While no national artificial intelligence strategy was formally published in 2025, consultations expanded and the institutional ecosystem around AI governance became more visible. The signature of the United Nations Convention against Cybercrime in October 2025 further signalled engagement with emerging international governance frameworks related to digital technologies.

Overall, the comparison with 2024 highlights a persistent structural tension in Togo's digital environment. Infrastructure development, cybersecurity capabilities and emerging technology governance continued to advance. At the same time, restrictions affecting freedom of expression, transparency and safeguards against surveillance remained significant. The slight decline in the overall score therefore reflects the growing weight of these civic and rights related concerns within the broader digital transformation trajectory.



Tunisia

By Anonymous

Executive Summary

Tunisia's digital landscape presents a complex interplay of progress and repression. The country has advanced digital infrastructure, but this progress is overshadowed by a growing crackdown on digital rights and freedoms. The government's increasing surveillance of online activities, coupled with the arbitrary arrest of journalists and activists, has created a climate of fear and self-censorship. Misuse of laws to target critical voices and the erosion of privacy rights are major concerns.

This report captures the evolving achievements and challenges that define Tunisia's digital landscape in 2025. It covers the dynamics of internet freedom, the right to privacy, data protection, access to information and digital inclusion. Additionally, the report assesses the country's score based on the TheScore Index developed by Paradigm Initiative to assess countries' compliance with the African Commission on Human and Peoples' Rights' Declaration of Principles on Freedom of Expression and Access to Information. The employed methodology involved a thorough review of government reports, media sources, and existing literature to comprehensively evaluate quantitative and qualitative aspects of digital rights and inclusion in the country.

Introduction

Tunisia, a North African nation of approximately 12 million people, embarked on a democratic transition following the 2011 revolution.[1] However, since 2021, President Kais Saied's consolidation of power has led to a significant repression of human rights and freedoms as evidenced by the imprisonment of political dissidents, the crackdown on peaceful protests and the increasing prosecutions against social media users.[2]

Tunisia is a signatory to several international human rights treaties, including the International Covenant on Civil and Political Rights[3]. Regionally, Tunisia ratified the African Charter on Human and Peoples' Rights, which guarantees individuals the right to receive information and the right to express and disseminate information. While these commitments underscore the country's obligations to protect fundamental rights, recent developments have raised concerns about their implementation.

Despite constitutional provisions for the primacy of international treaties, the current political climate has created challenges in upholding these commitments. The tension between democratic principles and authoritarian tendencies has significant implications for Tunisia's digital rights landscape.

Tunisia's score suggests that it is moderately compliant with the Declaration of Principles of Freedom of Expression and Access to Information in Africa.

Internet access and disruptions

According to the International Telecommunication Union's ICT Development Index 2025, 76.2% of the Tunisian population uses the Internet, while 68.6% of households have internet access at home. In 2025, the country had a robust mobile network infrastructure, with a high mobile broadband coverage rate of 97.2 per 100 inhabitants.[4]

Overall, Tunisia's internet penetration continued to grow, reaching 50.2% for broadband internet and 89.3% for mobile data.[5] In 2025, mobile traffic climbed from 301 in 2024 to 351 Petabytes (PB). Fixed data traffic escalated from 1,555 PB in 2024 to 1,989 PB.[6] This expansion was driven predominantly by strong subscriber adoption of fibre optic and data box technologies, alongside the phased decline of the adoption of Asymmetric Digital Subscriber Line (ADSL) technology.[7] This technological migration is directly evidenced by average monthly consumption rates, which stood at approximately 270 GB for ADSL and exceeded 700 GB for fibre connections.[8]

According to Ookla's Speedtest Global Index, Tunisia's average mobile download speed increased from 26.17 Mbps in 2024 to 64.08 in 2025, while the average upload speed increased from 14.60 Mbps in 2024 to 17.21 Mbps in 2025. For fixed broadband, both download and upload speeds saw significant improvements. Download speeds increased from 10.90 Mbps to 18.07 Mbps, while upload speeds jumped from 3.86 Mbps to 6.68 Mbps, ranking 146th globally.[9]

The commercial launch of 5G services in Tunisia in February 2025 served as the direct catalyst for the observed improvements in national internet speed metrics.[10] This milestone established Tunisia as the first North African nation to commercialise 5G technology, consequently positioning it as the regional leader in the

1. Al Jazeera, "Timeline: Tunisia's uprising", Jan 23, 2011, https://www.aljazeera.com/news/2011/1/23/timeline-tunisias-uprising (accessed on 29 January 2026).
2. Inkyda, "Kais Saied: jeopardizing rights and freedom", July 2023, https://inkyfada.com/en/2023/07/27/threats-rights-freedom-kais-saied-tunisia/ (accessed on 29 January 2026).
3. United Nations Treaties Collection, "International Covenant on Civil and Political Rights", https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf (accessed on 29 January 2026).
4. International Telecommunication Union (ITU), "Tunisia ICT Development Index 2025", https://datahub.itu.int/dashboards/idi/?e=TUN&y=2025 (Accessed on 15 November 2025).
5. INTT, "Tableau de bord trimestriel TR2- 2025", https://www.intt.tn/upload/files/TB-Trimestriel-TR2-2025.pdf (Accessed on 15 November 2025).
6. Instance Nationale des Télécommunications (INTT), "Tableau de Bord Trimestriel, 3e Trimestre 2025" [Quarterly Dashboard, 3rd Quarter 2025], p. 1, https://www.intt.tn/upload/files/TB%20Trimestriel-TR3-2025%20(1).pdf (accessed on 29 January 2026).
7. "Rapport du régulateur tunisien: la data tire la croissance au troisième trimestre 2025" [Report of the Tunisian regulator: Data drives growth in the third quarter of 2025], THD.tn, https://www.thd.tn/rapport-du-regulateur-tunisien-la-data-tire-la-croissance-au-troisieme-trimestre-2025/ (accessed on 28 January 2026).
8. Instance Nationale des Télécommunications (INTT), "Tableau de Bord Trimestriel, 3e Trimestre 2025" [Quarterly Dashboard, 3rd Quarter 2025], p. 1, https://www.intt.tn/upload/files/TB%20Trimestriel-TR3-2025%20(1).pdf (accessed on 29 January 2026).
9. Speedtest Global, "Tunisia,", https://www.speedtest.net/global-index/tunisia (Accessed on 15 November 2025).
10. La Presse, "Tunisie, première en Afrique du Nord à lancer la 5G," La Presse de Tunisie, February 14, 2025, https://www.lapresse.tn/2025/02/14/tunisie-premiere-en-afrique-du-nord-a-lancer-la-5g/ (accessed on 29 January 2026).

Speedtest Global Index.[11]

As part of the national digital transformation strategy, the Instance Nationale des Télécommunications has commissioned a study to evaluate the feasibility and potential deployment of Non-Geostationary Satellite fixed high-speed internet access.[12] This measure follows earlier service experiments, such as those with Starlink in October 2023.[13] Results from that study have not yet been released.

In November 2025, the Medusa submarine cable landed in the Tunisian coastal town of Bizerte, marking an important advancement in Tunisia's international connectivity infrastructure. This project positions Tunisia as the first African country to connect to this new generation network.[14] The fibre pair offers an initial capacity of 22Tbps (Terabytes per second), substantially augmenting the country's existing international bandwidth.[15]

Regarding affordability, Tunisia ranked 9th cheapest in Africa for mobile data in Q3 2025, with average monthly costs of US$1.51 per GB.[16]

Following the 2024 census, the National Institute of Statistics (INS) recently published figures revealing a significant digital divide in Tunisia, driven by geographical, economic, and educational disparities. Internet usage among individuals is substantially higher in urban areas (81.4%) compared to rural areas (61%). This geographical disparity is closely mirrored in equipment access, with computer usage standing at 40.2% in cities versus only 19.4% in rural areas. Interestingly, INS figures show a slight reverse gender gap, with 77.4% of women using the internet compared to 75.8% of men. Furthermore, internet usage directly correlates with educational attainment, reaching 60.1% of those with a secondary education but dropping sharply to only 17.9% among those with a primary education. Ultimately, despite ongoing network investment, the INS data confirms that bridging this complex socio-economic and educational access gap remains a core national challenge.[17]

Freedom of Expression and Access to Information

In 2025, Tunisia continues to witness a notable decline in free speech online. The year saw the sustained arrest and prosecution of diverse public figures, including prominent political figures[18], parliamentarians[19], journalists[20], environmental and social activists[21], and social media influencers[22], frequently based on their online commentary or publications. This broadening crackdown has been accompanied by the strategic use of various legal instruments, including the counterterrorism law, the penal code, the military justice

11. Karim Yaici, "5G Helped Egypt and Tunisia Uplift Mobile Performance to New Levels," Ookla Research, September 10, 2025, https://www.ookla.com/articles/5g-north-africa-2025 (accessed on 28 January 2026).
12. Instance Nationale des Télécommunications (INTT), "Appel d'offres n°02/2025," March, 2025, https://intt.tn/fr/index.php?typeactu=89&actu=1025 (accessed on 29 January 2026).
13. Adoni Conrad Quenum, "Tunisia tests satellite Internet in three cities," We Are Tech Africa, October 4, 2023, https://www.wearetech.africa/en/fils-uk/news/telecom/tunisia-tests-satellite-internet-in-three-cities (accessed on 29 January 2026).
14. Walid Naffati, "Medusa arrive à Bizerte : la Tunisie devient la première porte d'entrée de l'Afrique dans le nouveau réseau sous-marin Europe–Méditerranée," THD - Tunisie Haut Debit, November 3, 2025, https://www.thd.tn/medusa-arrive-a-bizerte-la-tunisie-devient-la-premiere-porte-dentree-de-lafrique-dans-le-nouveau-reseau-sous-marin-europe-mediterranee/ (accessed on 29 January 2026).
15. La Presse, "Tunisie Telecom célèbre l'atterrissement du câble sous-marin Medusa à Bizerte : un tournant stratégique pour la connectivité nationale et internationale," La Presse de Tunisie, November 1, 2025, https://www.lapresse.tn/2025/11/01/tunisie-telecom-celebre-latterrissement-du-cable-sous-marin-medusa-a-bizerte-un-tournant-strategique-pour-la-connectivite-nationale-et-regionale/ (accessed on 29 January 2026).
16. "RAMP Index Insights, Quarter 2, 2025," Research ICT Africa (RIA), July 24, 2025, https://researchictafrica.net/2025/07/24/ramp-index-insights-quarter-2-2025/ (accessed on 29 January 2026).
17. Institut National de la Statistique (INS), "Accès et usage des Technologies de l'Information et de la Communication (TIC)" [Access and usage of Information and Communication Technologies (ICT)], INS, 2024 Census Data, p. 1, September 2025, https://www.ins.tn/sites/default/files-ftp3/files/publication/pdf/TIC-FR.pdf (accessed on 29 January 2026).
18. Tunisie Telegraph, "القضاء يصدر أحكامه في قضية المحامي محمد علي عباس" (The Judiciary issues its rulings against Lawyer Mohamed Ali Abbas), Tunisie Telegraph, November 4, 2025, https://tunisie-telegraph.com/a-la-une-%D8%A2%D8%AE%D8%B1-%D8%A7%D9%84%D8%A3%D8%AE%D8%A8%D8%A7%D8%B1/mohamed-ali-abbes/ (accessed on 29 January 2026).
19. Mosaique FM, "جندوبة: الحكم ابتدائيا على عضو بمجلس النواب بالسجن لثلاث سنوات" (Jendouba: Preliminary sentence of three years in prison for a member of the House of People's Representatives), Mosaique FM, November 18, 2025, , https://www.mosaiquefm.net/ar/جهة-جندوبة-الحكم-ابتدائيا-على-عضو-بمجلس-النواب-بالسجن-لثلاث-سنوات/1480866 (accessed on 28 January 2026).
20. Kashf Media, "نافع الجريبي: سنتان سجنا دون وجه حق في قضية مزعومة بمبنى بلا دولت الصاري" (Nafeh Al-Aribi: Two years in prison against Boughlab due to a non-existent post), Kashf Media, July 10, 2025, https://kashfmedia.com/2025/07/10/نافع-الجريبي-سنتان-سجنا-دون-وجه-حق-في-قضية-مزعومة-بمبنى-بلا-دولت-الصاري/ (accessed on 29 January 2026).
21. Ultra Tunisia, "محامي: عامان سجنا دون الدخول بملف تصفح الهواتف على معتصم الموسوي 54" (Lawyer: Two years in prison against activist Moncef El Houaidi under Decree 54), Ultra Sawt, October 7, 2025, https://ultratunisia.ultrasawt.com/محامي-عامان-سجنا-دون-الدخول-بملف-تصفح-الهواتف-على-معتصم-الموسوي-54/ (accessed on 29 January 2026).
22. Kapitalis, "القضاء التونسي يقول كلمته بخصوص 7 من صناع المحتوى" (The Tunisian Judiciary Says Its Final Word Regarding 7 Content Creators), Kapitalis, February 5, 2025, https://kapitalis.com/anbaa-tounes/2025/02/05/القضاء-التونسي-يقول-كلمته-بخصوص-7-من-صناع-المحتوى/ (accessed on 29 January 2026).

code and specific decrees like Decree Law 2022-54.[2324]

A severe demonstration of this escalation was the case of Saber Chouchen, who was sentenced to death in October 2025 for his social media posts under charges including "assault intended to change the form of the state" (Penal Code) and "dissemination of false information" (Decree 54).[25] This judgement, rendered purely for online expression, marked an extreme use of disproportionate judicial responses against online speech. However, following widespread public pressure, the President granted a pardon to Chouchen, leading to his release.[26]

The National Syndicate of Tunisian Journalists documented, between October 2024, and October 2025, 149 incidents of violence against journalists, including 46 technology-based attacks, 23 cases of incitement, 13 cases of publication-linked legal prosecution, five cases of harassment, two cases of verbal assault, two cases of censorship, and one case of publication ban. According to the unit, 13 gender-based attacks were also reported.[27]

In particular, Decree Law 2022-54 has been used to silence dissent, with several journalists and activists facing prosecution and imprisonment for their online activities. The decree prescribes prison terms of up to 10 years for disseminating false news, among other speech-related offences. A group of parliament members proposed a legislative initiative to amend several chapters of Decree 2022-54. After being stalled for months by the Parliament's Bureau, the legislative proposal was referred to the General Legislation Committee for review and discussion in mid-2025.[28] In November 2025, the Head of the Rights and Freedoms Committee confirmed that the committee is conducting hearing sessions with advocates, including civil society organisations.[29]

Social media users, including relatives of detainees and those living abroad, were also prosecuted under Decree 2022-54, the counterterrorism law and penal code. In November 2025, the Tunis court of first instance sentenced Elyes Chaouachi,[30] political activist and son of a detained political opponent, and Mohamed Samti,[31] blogger and political activist, in absentia to 16 years in prison.[32],[33] The charges were largely based on their vocal online activism, including criticisms of the justice system and advocacy for other political prisoners. Chaouachi also reported facing nine additional legal cases, which include accusations for divulging protected information (counterterrorism law), committing an offence against the Head of State (penal code), spreading hate speech and defaming others (Decree 2022-54).[34] During the coverage period, pressure on Tunisia's independent media and civil society continued, notably through regulatory action against online media platforms. In October 2025, authorities ordered the temporary suspension of the Nawaat Journalists' Association, the entity managing the long-standing investigative site Nawaat, citing alleged non-compliance with Decree Law No. 88 concerning funding for associations. Nawaat, disputing the claim and asserting its adherence to all

23. Hivos, "Freedom of Expression in Tunisia: Legal Mapping", https://hivos.org/document/freedom-of-expression-in-tunisia-legal-mapping/ (accessed on 29 January 2026).
24. Decree-Law No. 2022-54 of September 13, 2022, relating to the fight against offenses relating to information and communication systems, https://legislation-securite.tn/latest-laws/decret-loi-n-2022-54-du-13-septembre-2022-relatif-a-la-lutte-contre-les-infractions-se-rapportant-aux-systemes-dinformation-et-de-communication/ (accessed on 29 January 2026).
25. Intersection Association – Saber chouchane," Intersection, October 6, 2025, https://intersection.uno/freedom-faces/%D8%B5%D8%A7%D8%A8%D8%B1-%D8%B4%D9%88%D8%B4%D8%A7%D9%86/ (accessed on 29 January 2026).
26. Hume, Tim, AFP, and Reuters. "Tunisia pardons man sentenced to death over Facebook posts." Al Jazeera. October 7, 2025. Accessed November 19, 2025. https://www.aljazeera.com/news/2025/10/7/tunisia-pardons-man-sentenced-to-death-over-facebook-posts (accessed on 29 January 2026).
27. SNJT, "98th Annual Report on the Safety of Journalists", November 2025, https://snjt.org/wp-content/uploads/2025/11/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1.pdf (accessed on 29 January 2026).
28. Najla Ben Salah, "تبحبضغ صاصتما قرواتم ما قرخأتم قافتسا ،54 موسرملا حيقنت: لدعتلل مأ ةأجافم؟" (Amendment of Decree 54: A Late Awakening or an Anger Absorption Maneuver?), Nawaat, July 4, 2025, https://nawaat.org/2025/07/04/تقافتسا-54-موسرملا-حيقنت-مأ-ةأجافم-مسوان/ (accessed on 29 January 2026).
29. Mosaique FM, "محمد عليّ: سجلنا تقدما ونحن نقترح المرسوم 54 بعد إحالته إلى لجنة التشريع (Muhammad Ali: We recorded progress towards amending Decree 54 after referring it to the legislation committee)," Mosaique FM, November 4, 2025,https://www.mosaiquefm.net/ar/تونس-طوارئ/1476342/محمد-عليّ-سجلنا-تقدما-ونحن-نقترح-المرسوم-54-بعد-إحالته-إلى-لجنة-التشريع (accessed on 29 January 2026).
30. Elyes Chaouachi, Facebook Profile, accessed November 22, 2025, https://www.facebook.com/elyes.chaouachi.58/ (accessed on 29 January 2026).
31. Mohamed Samti, Facebook Profile, accessed November 22, 2025, https://www.facebook.com/Medsam123 (accessed on 29 January 2026).
32. "Divulgation, diffamation et entente en vue d'actes violents: les détails du jugement contre Elyes Chaouachi" (Disclosure, Defamation, and Agreement with a View to Violent Acts: Details of the judgement Against Elyes Chaouachi), Business News, November 20, 2025, https://businessnews.com.tn/2025/11/20/divulgation-diffamation-et-entente-en-vue-dactes-violents-les-details-du-jugement-contre-elyes-chaouachi/1373992/ (accessed on 29 January 2026).
33. La Presse de Tunisie, "Elyes Chaouachi déféré devant la chambre criminelle antiterroriste" (Elyes Chaouachi Referred to the Anti-Terrorist Criminal Chamber), La Presse de Tunisie, November 8, 2025, https://www.lapresse.tn/2025/11/08/elyes-chaouachi-defere-devant-la-chambre-criminelle-antiterroriste/ (accessed on 29 January 2026).
34. Elyes Chaouachi, Facebook post, https://www.facebook.com/elyes.chaouachi.58/posts/pfbid038F2xqgYRjZgKaW5MfgXyWjarnMZwDWC9Hn7W4sf7DZtskwgUjaSiuxyK83fX5MUDl (accessed on 22 November 2025).

administrative regulations, characterised the one-month suspension as a "political decision" following a sustained period of official harassment, investigations, and financial oversight.[35] Concurrently, the youth-focused digital media outlet, Boubli also received an official notification to cease its activities.[36] These suspension notices triggered widespread local and international condemnation, with organisations including the National Union of Tunisian Journalists and the International Federation of Journalists characterising it as a significant escalation in the crackdown on free speech.[37]

Individuals with significant following on social media platforms, particularly women and members of the LGBTQIA+ community, became targets of online harassment, defamation, and incitement campaigns.[38] In February 2025, a gender non-conforming content creator was sentenced to a two-year prison term and a TND1,000 (approximately US$330) fine under Article 234 of the penal code for "violating morals by inciting minors to debauchery" over social media videos.[39]

Data Protection and Cybersecurity

Tunisia's legal framework includes provisions for privacy and data protection enshrined in the 2022 Constitution[40] and the 2004 Personal Data Protection Law.[41] Despite these legal safeguards, Tunisians' privacy rights still face vulnerabilities. The 2004 Personal Data Protection Law is outdated and does not effectively address the technological advancements and new challenges related to personal data, including the specificity of biometric data. Its numerous shortcomings, particularly in safeguarding privacy, grant the public authorities undue power over personal data, undermining citizens' fundamental rights.[42]

The prolonged state of emergency, renewed in January 2025,[43] grants government agencies extensive powers to access electronic devices without judicial oversight. This has raised concerns about monitoring those perceived as critical of the government.[44] Additionally, Decree-Law 2022-54 further eroded privacy rights. It allows law enforcement agencies to access personal data without a judicial warrant and mandates telecommunications providers to retain user data for extended periods.[45]

Civil society organisations have documented instances where the mobile phones of opposition politicians and activists have been seized and their communications monitored without proper legal authorisation.[46],[47] This has raised concerns about the extent of government surveillance to target individuals and suppress dissent.

The arbitrary arrest and prosecution of activists based on the content found on

35. La rédaction. "Nawaat will not be silenced." Nawaat. October 31, 2025. https://nawaat.org/2025/10/31/nawaat-will-not-be-silenced/ (accessed on 29 January 2026).
36. Boubli, photo post, October 15, 2025, Facebook, https://www.facebook.com/photo?fbid=826401253241605&set=a.199992262549177 (accessed on 22 November 2025).
37. International Federation of Journalists. "Tunisia: Government suspends investigative media platform amid crackdown on free speech." IFJ. November 5, 2025. https://www.ifj.org/media-centre/news/detail/category/press-releases/article/tunisia-government-suspends-investigative-media-platform-amid-crackdown-on-free-speech (accessed on 29 January 2026).
38. Fédération internationale pour les droits humains, "Tunisie : nouvelles attaques et actes d'intimidation contre DAMJ et ses membres", October 10, 2024, https://www.fidh.org/fr/themes/defenseurs-des-droits-humains/tunisie-nouvelles-attaques-et-actes-d-intimidation-contre-damj-et-ses (accessed on 29 January 2026).
39. Amnesty International, "Tunisia: Authorities Step Up Crackdown on LGBTI Individuals with Wave of Arrests," February 6, 2025, https://www.amnesty.org/en/latest/news/2025/02/tunisia-authorities-step-up-crackdown-on-lgbti-individuals-with-wave-of-arrests/ (accessed on 22 November 2025).
40. The Constitution of the Tunisian Republic of July 25, 2022, https://legislation-securite.tn/latest-laws/decret-presidentiel-n-2022-691-du-17-aout-2022-portant-promulgation-de-la-constitution-de-la-republique-tunisienne (accessed on 29 January 2026)./
41. Law No. 2004-63 of July 27, 2004, relating to the protection of personal data, https://legislation-securite.tn/latest-laws/loi-organique-n-2004-63-du-27-juillet-2004-portant-sur-la-protection-des-donnees-a-caractere-personnel/ (accessed on 29 January 2026)..
42. Nawaat, 3Journée internationale de protection des données personnelles : En Tunisie, c'est toujours l'inertie!", Jan 2015, https://nawaat.org/2015/01/29/journee-internationale-de-protection-des-donnees-personnelles-en-tunisie-cest-toujours-linertie/ (accessed on 29 January 2026).
43. تمديد حالة الطوارئ إلى غاية 31 ديسمبر 2025" (Extension of the state of emergency until December 31, 2025), Mosaïque FM, accessed November 22, 2025, https://www.mosaiquefm.net/ar/أخبار-تونس-وطنية/1374694/تمديد-حالة-الطوارئ-إلى-غاية-31-ديسمبر-2025 (accessed on 29 January 2026).
44. Amnesty International, "Tunisia Repressive state of emergency bill a threat to human rights,", March 15, 2019, https://www.amnesty.org/en/latest/news/2019/03/tunisia-repressive-state-of-emergency-bill-a-threat-to-human-rights/ (accessed on 29 January 2026).
45. "Decree n° 2022-54 relating to the fight against crimes related to information and communication systems," , https://legislation-securite.tn/latest-laws/decret-loi-n-2022-54-du-13-septembre-2022-relatif-a-la-lutte-contre-les-infractions-se-rapportant-aux-systemes-dinformation-et-de-communication/ (accessed on 29 January 2026).
46. Kapitalis, "Tunisie : Qui a utilisé le smartphone de Chaima Issa", April 2023, https://kapitalis.com/tunisie/2023/04/24/tunisie-qui-a-utilise-le-smartphone-de-chaima-issa-apres-sa-saisie/ and (accessed on 29 January 2026); Webso, "Ennahda met en garde contre l'utilisation du téléphone de Rached Ghannouchi", May 2023, https://www.webdo.tn/fr/actualite/national/ennahda-met-en-garde-contre-l-utilisation-du-telephone-de-rached-ghannouchi/205704 (accessed on 29 January 2026).
47. Women Journalists without chains, 'Statement of Condemnation by Women Journalists Without Chains", December 12, 2024, https://www.wjwc.org/news-en/statement-of-condemnation-by-women-journalists-without-chains/ (accessed on 29 January 2026).

their phones underscores the deterioration of digital rights. The cases of the two Tunisian students, Dhia Hamdi and Adam Hammami, exemplify how digital evidence can be used to silence critical voices. In September 2024, the two Tunisian students were arrested and their phones confiscated. The authorities subsequently charged them under Article 67 of the Penal Code for committing an obscene act against the President of the Republic, citing graffiti images found on their phones.[48] In October 2025, the case against them was dismissed, and their phones were returned.[49]

Data Breaches and Misuse

As of October 2025, the National Cybersecurity Agency (ANCS) maintained the national cybersecurity alert level at "very high."[50] ANCS specialists estimate that the period spanning 2024 to 2025 saw over 20,000 cyberattacks directed against Tunisian public and private institutions.[51] In a significant cybersecurity incident in July 2025, the National University Network and the infrastructure of the Al-Khawarizmi Computing Centre, operating under the Ministry of Higher Education and Scientific Research, were subject to a cyberattack.[52] While official sources confirmed the cyberattack, they did not disclose the breach's scope. Unofficial reports, however, suggest the incident exposed sensitive personally identifiable information of thousands of students, including governmental identifiers (National Identity Cards), academic records, and contact information.[53]

A separate incident involved the hacking and tampering of the national university orientation system. Following complaints from recent graduates regarding manipulated applications, prosecutors charged a detained student who had failed the final high school exam with forgery and intentional alteration of electronic data. The suspect claimed the tampering was accidental.[54]

The ANCS[55], the public prosecutor's office[56] and various institutions[57] repeatedly disseminated public advisories concerning phishing and hacking activities targeting users on social media.

Acknowledging the severity and increase of cyber threats, the Minister of Communication Technologies announced the finalisation of the Cybersecurity Strategy 2026–2030, which is pending approval. This successor to the existing 2020–2025 strategy[58] will prioritise flexible protection for national infrastructure, legislative updates, and specialised talent development.[59]

Digital and Biometric IDs

In September 2025, Tunisian authorities

48. Committee for Justice, "Tunisia: CFJ observes trial of 2 Tunisian activists due to anti-normalization activities ", November 8, 2024, https://www.cfjustice.org/tunisia-cfj-observes-trial-of-2-tunisian-activists-due-to-anti-normalization-activities/ (accessed on 29 January 2026).
49. Kashf Media, "عدم مهام الخروج في حق الشابين ضياء حمدي وأدم هماني" [Dismissal of the Case Against the Two Young Men, Dhia Hamdi and Adam Hammami], October 3, 2025, https://kashfmedia.com/2025/10/03/عدم-مهام-الخروج-في-حق-الشابين-ضياء-حمدي/ (accessed on 29 January 2026).
50. Agence Nationale de la Cybersécurité (ANCS) [Tunisia], "Graphe des Alertes Nationales" [Graph of National Alerts], https://www.ancs.tn/fr/node/451/ (accessed November 24, 2025).
51. Mosaique FM, " البنية التحتية لشبكات المعلومات تتعرض لأكثر من 20 ألف هجوم سيبراني خلال الفترة الممتدة بين 2024 و2025" [Twenty thousand Cyberattacks Targeted Tunisian Institutions Between 2024 and 2025], October 8, 2025, https://www.mosaiquefm.net/ar/تونس-اخبار-تونس-جهة-المهدية-المنستير-سوسة-صفاقس-قابس-مدنين-تطاوين-قفصة-توزر-قبلي-كبلي-الوادي-تطاوين/1466721/20-ألف-هجمة-سيبرانية-تستهدف-مؤسسات-تونسية-بين-2024-و2025 (accessed on 29 January 2026).
52. "Tunisia – Higher Education: Al Khawarizmi Centre Targeted by Cyberattack," Tunisie Numérique, July 10, 2025, https://news-tunisia.tunisienumerique.com/tunisia-higher-education-al-khawarizmi-center-targeted-by-cyberattack/#:~:text=A%20statement%20issued%20Thursday%20stated,Technologies%20and%20the%20National%20Cybersecurity (accessed on 29 January 2026).
53. "Alleged Hacking of University Websites 150000 Tunisian Students Potentially Affected," Trovit, https://trovit.tn/news/piratage-presume-de-sites-universitaires-150e280af000-etudiants-tunisiens-potentiellement-touches#:~:text=This%20point%2C%20as%20well%20as,media%20testimonials%2C%20without%20official%20verification (accessed on 24 November 2025)
54. Mosaique FM, "شبهات تلاعب بالتوجيه الجامعي: 8 بطاقات إيداع بالسجن ضد تلميذ" [Suspicions of Manipulation in University Orientation: 8 Detention Orders Against a Student], August 12, 2025, https://www.mosaiquefm.net/ar/تونس-أخبار-تونس-جهة-المهدية-المنستير-سوسة-صفاقس-قابس-مدنين-تطاوين/1447548/شبهات-تلاعب-بالتوجيه-الجامعي-8-بطاقات-إيداع-بالسجن-ضد-تلميذ (accessed on 29 January 2026).
55. "L'ANSI met en garde contre la propagation de campagnes de phishing sur les réseaux sociaux" [ANSI warns against the spread of phishing campaigns on social networks], La Presse, August 9, 2025, https://www.lapresse.tn/2025/08/09/lansi-met-en-garde-contre-la-propagation-de-campagnes-de-phishing-sur-les-reseaux-sociaux/ (accessed on 29 January 2026).
56. Mosaique FM, "سليانة: النيابة العمومية تحذر المواطنين من عمليات تحيّل على فايسبوك" [Siliana: Public Prosecution Warns Citizens of Fraud Operations on Facebook], November 4, 2025, https://www.mosaiquefm.net/ar/أخبار-تونس-جهة-سليانة/1476306/النيابة-العمومية-تحذر-المواطنين-من-عمليات-تحيل-على-فايسبوك (accessed on 29 January 2026).
57. Mosaique FM, "البريد التونسي يحذر مستعملي D17 من التصيّد والقرصنة على فيسبوك" [Tunisian Post Warns D17 Users of Phishing and Hacking on Facebook], February 7, 2025, https://www.mosaiquefm.net/ar/تونس-أخبار-تونس-جهة-المهدية-المنستير-سوسة-صفاقس-قابس-مدنين-تطاوين/1377661/البريد-التونسي-يحذر-مستعملي-d17-من-التصيد-والقرصنة-على-فيسبوك (accessed on 29 January 2026).
58. Agence Nationale de la Cybersécurité (ANCS) [Tunisia], "Stratégie Nationale de la Cybersécurité 2020-2025" [National Cybersecurity Strategy 2020-2025], https://www.ancs.tn/fr/strategie-nationale-de-la-cybersecurite-2020-2025-0 (accessed on 24 November 2025).
59. Mosaique FM, "وزير تكنولوجيات الاتصال: هجمة سيبرانية في العالم كل 39 ثانية" [Minister of Communication Technologies: A Cyberattack Occurs Globally Every 39 Seconds], October 8, 2025, https://www.mosaiquefm.net/أخبار-تكنولوجيات-الاتصال-هجمة-سيبرانية-في-العالم-كل-39-ثانية/1466550/وزير-تكنولوجيات-الاتصال-هجمة-سيبرانية-في-العالم-كل-39-ثانية (accessed on 29 January 2026).

announced the imminent launch of the new biometric identity card.[60] Following the adoption of the regulatory law in 2024, civil society organisations expressed concerns regarding the potential misuse of personal data, especially in light of the proposed centralised database of biometric data, which would be under the control of the Ministry of the Interior.[61] They cite concerns about the possibility of data breaches exposing sensitive personal information, the potential for public authorities to misuse the data for surveillance or repression, and the lack of sufficient legal and regulatory frameworks to prevent these harms and provide redress for individuals.[62]

In 2025, Tunisia continued the rollout of its mobile digital identity (Mobile ID), a voluntary service initiated in 2022. This ID is accessible to all citizens 18 and older and provides electronic access to a range of public and private services. As of November 2025, a total of 400,154 mobile IDs had been issued.[63]

Access to Information

In August 2025, the Tunisian government closed the headquarters of the National Authority for Access to Information (INAI) and administratively relocated its personnel to the Prime Minister's office.[64] Established in 2017 under Organic Law No. 2016-22, the INAI was a cornerstone for the constitutional right of access to information in Tunisia.[65] Its formal dissolution followed years of institutional undermining: the authority's binding decisions were routinely disregarded by public bodies without consequence, and key board positions were deliberately left vacant for extended periods, ultimately stripping the INAI of both its legal enforceability and moral authority.[66] International and local civil society organisations strongly condemned the move, viewing it as part of a broader trend since 2021 to dismantle the independence of key oversight institutions.[67]

While the Organic Law No. 22 of 2016 on Access to Information remains formally in force, its efficacy is compromised by the absence of an independent oversight body and a pervasive operational environment marked by increased government opacity and the imposition of unlawful barriers to information access. In recent years, media access to government information has declined. Authorities have limited their interactions with the press, making it difficult for journalists to verify information from official sources.[68] In its annual report, the National Syndicate of Tunisian Journalists documented 16 incidents of information withholding, with the majority of cases originating from local governance and public relations roles.[69] As Gabes governorate witnessed large-scale demonstrations over the pollution crisis, civil society organisations criticised the delays in disclosing environmental data and called on authorities to ensure full transparency and access to environmental information.[70]

While Tunisia has previously made progress in establishing the legal and institutional foundations for access to information, the efficacy of the law is compromised by the dissolution of the

60. "Tunisie : vers le lancement imminent de la carte d'identité biométrique" [Tunisia: Towards the imminent launch of the biometric identity card], La Presse, September 21, 2025, https://www.lapresse.tn/2025/09/21/tunisie-vers-le-lancement-imminent-de-la-carte-didentite-biometrique/ (accessed on 29 January 2026).
61. Access Now, "Eight years in the making: Tunisia's controversial Biometric ID and Passport Bills risk rights", Access Now, March 7, 2024, https://www.accessnow.org/press-release/tunisia-biometric-id-passport-bills-passed/ (accessed on 29 January 2026).
62. Access Now, "Tunisia: Statement on Proposed National ID Card", January 2023, https://www.accessnow.org/press-release/tunisia-statement-proposed-national-id-card/ (accessed on 29 January 2026).
63. Ministère des Technologies de la Communication (MTC). "Home". MobileID Tunisia, https://www.mobile-id.tn/ (accessed 24 November 2025)
64. Tunisie Telegraph, "رئاسة الحكومة تؤكد حل هيئة النفاذ إلى المعلومة" [Presidency of the Government Confirms Dissolution of the Access to Information Authority], Tunisie Telegraph, https://tunisie-telegraph.com/a-la-une-رئاسة-الحكومة-تؤكد-حل-هيئة-النفاذ-إلى-/ (accessed on 29 January 2026).
65. ARTICLE 19, "Tunisia: An end to transparency – and the last safeguard of democracy," ARTICLE 19, August 28, 2025, https://www.article19.org/resources/tunisia-democracy-at-risk-as-access-to-information-authority-is-dissolved/ (accessed on 29 January 2026).
66. Legal Agenda, "إغلاق مقر الهيئة النفاذ إلى المعلومة... مسار طويل من الاستنزاف يُتوّج بالإعلان عن إغلاق مقر الهيئة النفاذ إلى المعلومة" [Closing the Headquarters of the Access to Information Authority... A Long Path of Exhaustion Culminates in Termination], Legal Agenda, https://legal-agenda.com/إغلاق-مقر-الهيئة-النفاذ-إلى-المعلومة-مسار/ (accessed on 29 January 2026).
67. Syndicat National des Journalistes Tunisiens (SNJT), "بيان: النقابة الوطنية للصحفيين التونسيين تدين قرار إغلاق مقر الهيئة النفاذ إلى المعلومة" [Statement: The National Syndicate of Tunisian Journalists Condemns the Decision to Close the Headquarters of the Access to Information Authority], SNJT, August 20, 2025, https://snjt.org/2025/08/20/27735/ (accessed on 29 January 2026).
68. Mosaique FM, "Zied Dabbar: Les journalistes pris pour cibles par la magistrature", March 2024, https://www.mosaiquefm.net/fr/national-tunisie/1254101/zied-dabbar-les-journalistes-pris-pour-cibles-par-la-magistrature (accessed on 29 January 2026).
69. Syndicat National des Journalistes Tunisiens (SNJT), "تقرير النقابة الوطنية للصحفيين التونسيين السنوي حول واقع حرية الصحافة وحرية التعبير" [SNJT Annual Report on the State of Press Freedom and Freedom of Expression], SNJT, 2025, https://snjt.org/wp-content/uploads/2025/11/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1.pdf (accessed on 29 January 2026).
70. Tunisia: Uphold the right to protest and access to environmental information," Article 19, October 20, 2025, https://www.article19.org/resources/tunisia-uphold-the-right-to-protest-and-access-to-environmental-information/ (accessed on 29 January 2026).

independent oversight authority and a general environment characterised by increased government opacity, the imposition of unlawful administrative and legal barriers to access, and the concurrent decline of media freedom.

AI and Emerging Technologies

Tunisia has demonstrated an interest in emerging technologies like artificial intelligence (AI), but its progress in this area has been relatively modest. Despite initiating discussions on AI governance in 2018, concrete policy advancements have been limited.[71] Tunisia's process toward a National Artificial Intelligence Strategy has been marked by several initiatives and is currently in the final stages of drafting and consultation, though not yet formally adopted by the government.[72] The 2004 Personal Data Protection Law[73] applies to the automated processing and non-automated processing of personal data.

As reported in 2025, the government began deploying Artificial Intelligence (AI) tools for public policy development. The Development Planning Commission reportedly used AI to draft the 2026–2030 national development plan by deploying AI analysis of sector-specific indicators.[74]

In the Global Innovation Index, Tunisia ranked 76th out of 139 countries, moving up five spots from its 2024 position.[75] The country's performance is driven by strong areas like human capital, particularly its 2nd global ranking for science and engineering graduates, and knowledge and technology outputs. However, challenges remain in its institutional, infrastructure, market, and business sophistication.[76]

Tunisia still faces challenges in fully harnessing the potential of emerging technologies. To accelerate its technological advancement, the country needs to invest in research and development and create a favourable regulatory environment for innovation.

Digital Inclusion

In March 2025, the Ministry of Communication Technologies launched the "Universal Coverage with Communication Networks" project to address the digital divide by ensuring the provision of high-speed communication networks across the country, particularly targeting small and remote settlements. The Minister of Communication Technologies publicly articulated the expectation that telecommunications operators must fulfil a social responsibility to provide this universal service, beyond their existing contractual duties.[77] In June 2025, the Ministry announced a tender specifically aimed at procuring high-speed internet and communication network coverage for 103 currently unconnected residential areas spanning 15 governorates.[78] This project is integrated within a broader 2025–2026 digital transformation program, which is defined by its 138 constituent projects across four primary areas: modernising administrative services, promoting the digital economy, strengthening cybersecurity, and advancing digital infrastructure.[79]

71. Agence Nationale de la Promotion de la Recherche Scientifique, "National AI Strategy: Unlocking Tunisia's Capabilities Potential,", September 2018, https://www.anpr.tn/national-ai-strategy-unlocking-tunisias-capabilities-potential/ (accessed on 29 January 2026).
72. "La Tunisie prépare sa stratégie nationale de l'intelligence artificielle" [Tunisia prepares its national artificial intelligence strategy], La Presse de Tunisie, November 5, 2025, https://www.lapresse.tn/2025/11/05/la-tunisie-prepare-sa-strategie-nationale-de-lintelligence-artificielle/ (accessed on 29 January 2026).
73. Law No. 2004-63 of July 27, 2004, relating to the protection of personal data,https://legislation-securite.tn/latest-laws/loi-organique-n-2004-63-du-27-juillet-2004-portant-sur-la-protection-des-donnees-a-caractere-personnel/ (accessed on 29 January 2026).
74. "Plan de développement 2026-2030 : L'intelligence artificielle utilisée pour définir les priorités stratégiques" [Development Plan 2026-2030: Artificial intelligence used to define strategic priorities], La Presse, July 9, 2025, https://lapresse.tn/2025/07/09/plan-de-developpement-2026-2030-lintelligence-artificielle-utilisee-pour-definir-les-priorites-strategiques/ (accessed on 29 January 2026).
75. Global Innovation Index, "Tunisia ranking in the Global Innovation Index 2024", https://www.wipo.int/gii-ranking/en/tunisia (accessed on 29 January 2026).
76. "Tunisia Climbs to 76th in Global Innovation Index: Ranked Among Top Overperformers," TMO Mag, October 25, 2024, https://tmo-mag.com.tn/tunisia-climbs-to-76th-in-global-innovation-index-ranked-among-top-overperformers/#:~:text=Tunisia%20has%20risen%20five%20places,held%20between%202018%20and%202023 (accessed on 29 January 2026).
77. Mosaique FM, "وزير التكنولوجيات وعدي مشغلي الاتصالات لتوفير التغطية للجميع" [Technology Minister Calls on Telecom Operators to Provide Coverage for All], March 26, 2025, https://www.mosaiquefm.net/ar/تونس-وطنية/1395244/وزير-التكنولوجيات-وعدي-مشغلي-الاتصالات-لتوفير-التغطية-للجميع (accessed on 29 January 2026).
78. Turess, "إطلاق طلب عروض لتأمين التغطية الشاملة بشبكات الاتصال والإنترنت ذات التدفق العالي لفائدة 103 مناطق" [Launch of a Tender to Ensure Comprehensive Coverage of Communication Networks and High-Speed Internet for 103 Regions], June 24, 2025, https://www.turess.com/arrakmia/1849337 (accessed on 29 January 2026).
79. Presidency of the Government, "مجلس وزاري حول متابعة تقدّم مشاريع التحوّل الرقمي للإدارة" [Ministerial Council on Monitoring the Progress of Administrative Digital Transformation Projects], September 16, 2025, https://pm.gov.tn/ar/article/mjls-wzary-hwl-mtabt-tqdwm-mshary-althwwl-alrqmy-lladart (accessed on 29 January 2026).

Child Online Safety

In November 2025, the Tunisian government formally adopted the National Charter for the Protection of Children Online, a joint initiative between the Ministry of Family, Women, Childhood & the Elderly and the Ministry of Communication Technologies.[80] This Charter primarily functions as a voluntary framework, focusing on reinforcing social responsibility rather than establishing immediate binding legal obligations. It is closely integrated with the National Action Plan (NAP) against online violence toward children, launched earlier, in partnership with UNICEF.[81] To support the Charter's implementation, the Ministry of Family, Women, Childhood & the Elderly reportedly conducted a legislative assessment in 2025 to identify shortcomings in existing laws regarding children's digital protection. The findings will inform legislative reforms and facilitate the creation of practical guidance for key stakeholders.[82]

Universal Service Fund (USF)

Tunisia's Universal Service Fund (USF), established in 2001 and subsequently amended, mandates telecom operators to contribute a portion of their revenue to support universal service initiatives, including internet access.[83]

Despite efforts to develop a comprehensive universal service policy, progress has been limited.[84] The government has collected a 1% telecoms fee for 'universal service development' since 2001, but has failed to provide consistent and transparent information on how these funds are utilised.[85] To address the digital divide, the government has pursued alternative strategies, such as the "white zones" initiative to extend internet coverage to remote areas and the "Edunet 10" project to connect educational institutions.

80. "Un pacte national pour protéger les enfants dans l'espace numérique" [A National Pact to Protect Children in the Digital Space], Mosaique FM, November 2025, https://www.mosaiquefm.net/fr/national-tunisie/1481005/un-pacte-national-pour-proteger-les-enfants-dans-l-espace-numerique (accessed on 29 January 2026).
81. UNICEF Tunisia, "National Action Plan (NAP) Against Violence Affecting Children (VAC) Online (2023-2025)," UNICEF, 2023, https://www.unicef.org/tunisia/media/8121/file/PAN%20VAC%20online-ang.pdf (accessed on 29 January 2026).
82. "Protection de l'enfance en ligne : la Tunisie adopte un Pacte national" [Online Child Protection: Tunisia Adopts a National Pact], Nessma TV, November 19, 2025, https://www.nessma.tv/fr/nationale/actu/protection-de-l-enfance-en-ligne-la-tunisie-adopte-un-pacte-national/561798 (accessed on 29 January 2026).
83. Arrêté du ministre des technologies de l'information et de la communication du 30 décembre 2013, fixant la liste des services universels des télécommunications. https://www.intt.tn/upload/txts/fr/arr%C3%AAt%C3%A9_du_ministre_des_technologies_du_30_d%C3%A8cembre_2013_fixant_la_liste_des_services_universels.pdf (accessed on 17 December 2025).
84. INT 'workshop «pour l'élaboration d'une politique de service universel des télécommunications en tunisie»' http://www.intt.tn/fr/index.php?typeactu=89&actu=538 (accessed on 17 December 2025).

Conclusion

The findings presented in this report point to Tunisia's commendable progress in enhancing internet connectivity, strengthening cybersecurity, and implementing innovative digital services. However, concerns raised by civil society regarding transparency, online freedoms and privacy underscore the need for a careful and balanced approach. While advancements in digital inclusion showcase Tunisia's commitment to progress, challenges related to declining freedom of expression highlight the importance of safeguarding individual rights.

85. THD, "GSMA issues critical opinion on draft Digital Code", October 2018, https://www.thd.tn/la-gsma-donne-un-avis-critique-sur-le-projet-du-code-du-numerique/ (accessed on 17 December 2025).

Recommendations

The Government should:

- Strengthen Digital Rights Protection: Prioritise legislative initiatives that uphold human rights principles and safeguard the freedoms enshrined in the Tunisian Constitution.
- Enhance Transparency and Accountability: Restore the institutional capacity of the Access to Information Authority. Implement an open communication plan that upholds citizens' right to access information. Publish comprehensive reports on the Universal Fund's activities and funded projects.
- Cease Unjustified Prosecutions: Refrain from referring journalists on state security charges outside the legal framework governing the profession.
- Accountability for Assaults: Conduct thorough investigations into incidents involving assaults on journalists by public agents and ensure accountability.
- Reform Data Protection Laws: Revise existing data protection laws.
- Review Restrictive Laws: Revise legal measures like Decree-Law No. 2022-54 to align with international standards for freedom of expression.
- Establish robust governance frameworks: Develop and implement clear regulations and guidelines for the development and use of AI, addressing risks and ensuring responsible innovation.
- Commit to digital accessibility: Guarantee the compliance of all public digital platforms and information systems with accessibility standards and ensure effective stakeholder engagement in designing and implementing inclusive digitisation policies.

Civil Society Organisations should:

- Advocate for Digital Rights: Continue advocating against laws and decrees that threaten digital rights.
- Promote Privacy Awareness: Conduct public awareness campaigns to educate citizens about their right to privacy.
- Demand Transparency: Advocate for transparency in digital policies and project implementation.
- Foster Digital Literacy: Contribute to promoting digital literacy and cybersecurity awareness among the public.

The private sector should:

- Uphold Ethical Standards: Adhere to data protection principles and human rights in all operations.
- Ensure Data Privacy: Implement robust data protection measures to safeguard user information.
- Promote Digital Inclusion: Contribute to initiatives that promote digital literacy and access for marginalised groups.

The Score Index

Tunisia, 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)	5	5	No recorded disruption of access to the internet and other digital technologies
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	3	3	While the promotion of universal, equitable, affordable and meaningful access to the internet is stated in some laws such as the telecommunication code and policies such as the National Strategic Plan for the ICT sector, there are still gaps such as the non-existence of a comprehensive universal service policy.
False News Criminalisation	P22(2)	1	1	Several legal texts including penal code and Decree 2022-54 do criminalise publication of false news with prison sentences and fines. Examples: Article 24 of Decree 2022-54 mandates up to ten-year prison terms to punish the use of communications networks to “produce, spread, disseminate... false news” or to “slander others, tarnish their reputation, financially or morally harm them.”
Sedition Legislation	P22(2)	1	1	Several legal texts including penal code and Decree 54 do criminalise sedition with prison sentences and fines
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	1	1	In 2025, Tunisia witnessed a growing number of prosecutions and long prison sentences against journalists, Human Rights Defenders (HRDs) and citizens for online activity. Media outlets faced increasing pressure, including regulatory action against online media platforms and restrictions on journalist access.
Data Protection Legislation.	P42	3	3	The 2004 data protection law is considerably outdated.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	4	4	Formal cases of content removal and blocking are mostly transparent, and the decisions can be appealed through the courts. Between January and June 2025, 26 government requests for 46 user/account data were made to META. All of which were made through a domestic legal process.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Invasion of Privacy of	P41	2	2	Current legal texts, such as Decree 54 and the state of emergency law, fail to comply with international human rights standards. Concerns include the absence of adequate procedural safeguards, such as notification of surveillance and the right to appeal.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	2	1	While most governmental agencies have websites and social media accounts, some of them do not update or disclose information regularly. see access to information section
AI and Emerging Technologies national strategies	P39(6)	3	3	While Tunisia has a data protection law, it is considered outdated and no specific policies have been communicated regarding emerging tech
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	4	4	Tunisia's laws, including the Personal Data Protection law and the Child Protection Code, aim to protect children online, but face implementation gaps. Efforts include the adoption of a National Charter for the Protection of Children Online,
Digital Inclusion	P37(3)	4	4	Tunisia deployed several initiatives in an effort to bridge the digital divide: including the "Universal Coverage" project targeting remote areas, and the "Edunet 10" project providing high-speed internet to schools. However, information regarding the use of the Universal Service Fund is not publicly nor transparently available.
Total (out of 60):		2024: **34**	2025 **34**	



Uganda

By Sandra Aceng

Executive Summary

The 2025 Uganda Londa report employs TheScore Index developed by Paradigm Initiative to evaluate the state of digital rights and inclusion in Uganda. The report concentrates on themes such as freedom of expression, privacy, access to information, and the impact of legal frameworks on digital engagement, aiming to measure compliance with the African Commission on Human and Peoples[1]47' Rights (ACHPR) Declaration on Freedom of Expression and Access to Information (The Declaration) using a mixed-methods approach, incorporating quantitative data and case studies to analyse key thematic areas. The report notes significant progress in Uganda's digital infrastructure since 2016, including higher internet penetration and the introduction of legal measures like the Data Protection and Privacy Regulations 2021. However, it also highlights ongoing critical issues, including internet shutdowns, censorship, and a digital divide exacerbated by socioeconomic factors. The report advises increasing public awareness of digital rights, strengthening the enforcement of data protection laws, and ensuring fair access to digital resources, especially in rural areas and among marginalised groups, to foster a more inclusive digital environment.

Introduction

The Republic of Uganda is a landlocked country in East Africa, bordered to the east by Kenya, to the north by South Sudan, to the west by the Democratic Republic of the Congo, to the south-west by Rwanda, and to the south by Tanzania.[1] However, 30.03% of Uganda's population is urban (15,430,672 people in 2025), while 72.3 % lived in rural areas at the start of 2025[2] with a median age of 16.9 years.[3] 50.4% of the population is female, while 49.6% is male[4] and its population increased by 1.4 million, or 2.8%, between early 2024 and the start of 2025.[5] Since 1986, Uganda's president has remained Yoweri Museveni under the National Resistance Movement (NRM) political party.[6]

The 2025 Londa Uganda report analyses digital rights and inclusion in Uganda, offering critical recommendations for improvement and compliance with the Declaration using TheScore Index developed by Paradigm Initiative.

Uganda has progressed in developing its digital infrastructure and legal frameworks for the digital economy which has led to the significant growth of internet penetration with a high proportion of the population having access to a broadband signal, expansion of mobile money and digital banking which has led to increased access to financial services,[7] the enactment of legal frameworks such as the Data Protection and Privacy Act, 2019 and the establishment of the Personal Data Protection Office (PDPO) in 2021 are notable legislative steps toward safeguarding personal data and privacy; and the adoption of various e-governance platforms and a "chain-linked approach' to integrate digital technologies into public service

1. Uganda https://en.wikipedia.org/wiki/Uganda (accessed on November 15, 2024 at 16:00 EAT)
2. Simon Kemp. (3 March 2025). Digital 2025: Ugada https://datareportal.com/reports/digital-2025-uganda (accessed on November 8, 2025)
3. Uganda Population https://www.worldometers.info/world-population/uganda-population/ (accessed on November 8, 2025)
4. DIGITAL 2025: UGANDA https://datareportal.com/reports/digital-2025-uganda (accessed on November 8, 2025)
5. DIGITAL 2025: UGANDA https://datareportal.com/reports/digital-2025-uganda (accessed on November 8, 2025)
6. Uganda https://en.wikipedia.org/wiki/Uganda (accessed on November 8, 2025 at 15:47 EAT)
7. Fiona Luboga. (Sep 5, 2024). Uganda's Journey of Progress and Digital Transformation since Independence- https://ict.go.ug/media/articles/ugandas-journey-of-progress-and-digital-transformation-since-independence

delivery, including the justice system, to improve efficiency and transparency.

Despite this progress, critical digital rights issues remain unresolved and, in some cases, have worsened. These include internet shutdowns, censorship, and social media blocks during elections, which severely restrict access to information. Platforms such as Facebook remain blocked as of December 2025. Repressive laws, such as the 2011 Computer Misuse Act (amended in 2022), have been used against users, and surveillance technologies, including facial recognition, lack transparency and safeguards. A digital divide persists between urban and rural areas and along gender lines, due to limited access to smartphones, electricity, and digital literacy. Reliance on a national digital ID system marginalises about 40% of the population without IDs.[8] Additionally, awareness of digital rights is low, and enforcement of data laws remains weak.

Internet Access And Disruptions

Internet access remains a fundamental human right in Uganda, according to Uganda's 1995 Constitution, specifically Article 29(1)(a), which guarantees the right to freedom of expression, including the freedom to receive and impart information and ideas through any media of one's choice.[9] Uganda has seen various efforts, including advocacy by civil society organisations promoting digital rights and legislation aimed at improving access to internet services.[10] However, challenges remain, including restrictions during social disturbances and internet censorship. In January 2025, there were 14.2 million internet users in Uganda, which increased by 1.0 million (+7.8%) between January 2024 and January 2025, with an internet penetration rate of 28% of the total population[11] Uganda's internet adoption rate increased by a relative 4.9% (+130 basis points) during the same period. Factors such as limited access to electricity in rural areas, low digital literacy levels, and the high cost of internet-enabled devices such as computers and smartphones are some of the obstacles affecting internet usage.[12] Despite widespread network availability, recent GSMA data indicates that 4G population coverage has reached 96%, yet internet adoption remains low (22%), which creates a significant usage gap.[13] This significant disparity is due to various persistent barriers, including the high cost of smartphones, sector taxes, and limited digital literacy among the populace.[14]

Laws and measures for fostering meaningful access include the Uganda Communications Act, 2013[15], digital literacy programs implemented by the government[16] and various organisations in Uganda, affordability initiatives to reduce internet costs, and deployment of community networks by the government and organisations to improve internet access in remote areas.[17]

In 2025, there were several discussions with Tanzania to develop a resilient network and increase bandwidth through the new route provided by Kilimanjaro Telecom to address long-standing challenges with last-mile connectivity and reliability to lower the cost of internet in Uganda.[18] By July 2025, Uganda had started assembling its own local production of digital devices to reduce costs and expand access at the Namanve and Mbale industrial parks.[19] Additionally, in 2025, Airtel Uganda and MTN Uganda significantly

8. Michael Aboneka. (2025).Uganda's Digital ID Barrier Worsens as Court Delivers Blow to Access https://digitalrightsalliance.africa/ugandas-digital-id-barrier-worsens-as-court-delivers-blow-to-access/
9. Constitution of the Republic of Uganda https://ulii.org/akn/ug/act/statute/1995/constitution/eng@2018-01-05 (accessed on February 06, 2025 at 2:28 pm South African time)
10. https://www.ucc.co.ug/download-category/performance-reports/ (accessed on February 09, 2025)
11. Simon Kemp. (3 March 2025). Digital 2025: Uganda https://datareportal.com/reports/digital-2025-uganda (accessed on November 8, 2025)
12. Gillwald, A., Mothobi, O., Tusubira, F., & Ndiwalana, A. (2019). The State of ICT in Uganda (Policy Paper No. 8; Series 5: After Access – Assessing Digital Inequality in Africa). Research ICT Africa. https://researchictafrica.net/wp-content/uploads/2019/05/2019_After-Acces s-The-State-of-ICT-in-Uganda.pdf (accessed on November 8, 2025)
13. What is the Digital Divide? (GSMA) https://www.gsma.com/breaking-barriers-closing-the-digital-divide/ (accessed on January 31, 2026)
14. Simon Kemp. (3 March 2025). Digital 2025: Uganda https://datareportal.com/reports/digital-2025-uganda (accessed on November 8, 2025)
15. https://www.ucc.co.ug/download/uganda-communications-act-2013/ (accessed on January 13, 2026)
16. Digital Literacy Training for Local Government OfficersPDM https://ict.go.ug/media/news/digital-literacy-training-for-local-government-officers#
17. Ambrose Okai. (22 May 2025). Oyam Women Embrace Rural Broadband to Bridge Digital Divide https://ugandaradionetwork.net/story/oyam-women-embrace-rural-broadband-to-bridge-digital-divide (accessed on November 30, 2025)
18. Amon Katungulu. (July 22, 2025). Uganda and Tanzania Strengthen ICT Partnership to Boost Regional Digital Connectivity https://nilepost.co.ug/news/274541/uganda-and-tanzania-strengthen-ict-partnership-to-boost-regional-digital-connectivity (accessed on November 28, 2025)
19. The Independent. (July 22, 2025). Uganda and Tanzania strengthen ICT partnership https://www.independent.co.ug/uganda-and-tanzania-strengthen-ict-partnership/ (accessed on November 28, 2025)

advanced their 5G networks, enhancing coverage and service quality, especially in rural areas.[20] Despite this progress, Uganda's internet connectivity remains uneven, with some areas having high speeds while others remain underdeveloped, particularly in rural regions. The most popular form is mobile data, which is more prone to fluctuations due to factors such as network congestion during peak usage times and weather conditions. Although urban regions benefit from faster and more stable connections due to the expansion of fibre and 4G/5G networks, a digital divide between cities and rural areas remains, and the country's overall average still lags behind that of developed nations.[21] As of November 2025, 35 internet service providers (ISPs) were connected to the Uganda Internet Exchange Point (UIXP).[22]

The cost of internet access and devices is the primary barrier to internet access and use, particularly for low-income households. The average price of one gigabyte (GB) of prepaid mobile data is US$1.11 (approximately UGX5,000), representing up to 16.2% of the average Ugandan's monthly income.[23] This is higher than the Broadband Commission's "1 for 2" target, which recommends that 1GB of data should cost no more than 2% of the average monthly income to be considered affordable because Ugandans spend roughly US$2.87 per month on internet data, which is a significant burden when weighed against mandatory basic needs or services such as food and healthcare.[24] Internet costs are affected mainly by the 5% digital services tax introduced in July 2023 by the Uganda Revenue Authority (URA), which continues to impact the digital ecosystem by targeting non-resident companies that earn income from providing digital services in Uganda.

The government has also continued to enforce a 12% tax on internet data as part of a tax package adopted under the Excise Duty (Amendment) Act 2021.[25] Research on the 12% tax found that it disproportionately affected women's access to the Internet.[26] By early 2025, 37.6% of Uganda's social media user identities were female, while 62.4% were male, with 16.9 % of Uganda's total internet user base (regardless of age) using at least one social media platform in January 2025.[27] Even though the prices of data are competitive in the East Africa region, Uganda still lags behind Kenya and Rwanda in terms of overall affordability relative to average income.[28]

The device cost is relatively high, with smartphones priced at US$38-39, which represents approximately 39% of GDP per capita and 96% of income for the poorest 40% of Ugandans.[29] This is mainly due to taxation, which accounts for approximately 35% of an entry-level smartphone's price, thereby further hindering internet access. This makes future phones the most commonly owned for their affordability and durability.[30] The high cost of internet devices and data services, relative to income, creates a digital divide in Uganda. Despite improved coverage, affordability keeps many offline.[31]

In 2025, there were no reported connectivity restrictions or new government-imposed limitations on social media platforms, although access to Facebook remained restricted, hence partial social media restrictions.[32] However, some users can still access Facebook using virtual private networks (VPNs) and selected Wi-Fi networks.[33] According to NetBlocks,

20. Joan Kaberia. (December 17, 2025). Airtel Expands 5G Beyond Kampala https://cioafrica.co/airtel-expands-5g-beyond-kampala/ (accessed on January 31, 2026)
21. What is the Internet Speed Like in Uganda? https://allinafricasafaris.com/what-is-the-internet-speed-like-in-uganda/ (accessed on November 30, 2025)
22. The Uganda Internet eXchange Point https://www.uixp.co.ug/networks (accessed on November 28, 2025)
23. Paul Murungi. (Wednesday, September 06, 2023). Internet users spend average of Shs5,000 on data monthly https://www.monitor.co.ug/uganda/business/markets/internet-users-spend-average-of-shs5-000-on-data-monthly-4359906 (accessed on January 31, 2026)
24. Dorothy Nakaweesi. (Thursday, September 25, 2025). Internet surge: Ugandans are spending more on data than ever before https://www.monitor.co.ug/uganda/business/markets/internet-surge-ugandans-are-spending-more-on-data-than-ever-before--5205000 (accessed on November 30, 2025)
25. Posted at 7:07 PM · Apr 29, 2021 via user: Nemz @AmanyaNemz https://twitter.com/Parliament_Ug/status/1387800653356060672 (accessed on November 30, 2025)
26. Rehema Kahunde. (February 2, 2023). Taxation, gender, and internet access: lessons from Uganda https://global-dev.blog/taxation-gender-and-internet-access-lessons-uganda/ (accessed on November 30,2025)
27. Simon Kemp. (3 March 2025). Digital 2025: Uganda https://datareportal.com/reports/digital-2025-uganda (accessed on November 30, 2025)
28. Dorothy Nakaweesi. (Thursday, September 25, 2025). Internet surge: Ugandans are spending more on data than ever before https://www.monitor.co.ug/uganda/business/markets/internet-surge-ugandans-are-spending-more-on-data-than-ever-before--5205000 (accessed on November 30, 2025)
29. Betty Ndagire. (Wednesday, November 12, 2025). 70 percent of Ugandans remain offline, says GSMA https://www.monitor.co.ug/uganda/business/technology/70-percent-of-ugandans-remain-offline-says-gsma--5261488 (accessed on January 31, 2026)
30. Betty Ndagire. (Wednesday, November 12, 2025). 70 percent of Ugandans remain offline, says GSMA https://www.monitor.co.ug/uganda/business/technology/70-percent-of-ugandans-remain-offline-says-gsma--5261488
31. Digital divide widens as smartphone costs keep millions of Ugandans offline, says report https://www.ugbulletin.co.ug/digital-divide-widens-as-smartphone-costs-keep-millions-of-ugandans-offline-says-report /
32. Arthur Arnold Wadero. (Friday, August 12, 2022). Facebook to remain shut as govt talks with tech giant stall https://www.monitor.co.ug/uganda/news/national/facebook-to-remain-shut-as-govt-talks-with-tech-giant-stall-3912172 (accessed on November 30, 2025)
33. Timothy Kalyegira. (Sunday, December 07, 2025). Museveni's Facebook 'ban' https://www.monitor.co.ug/uganda/magazines/people-power/museveni-s-facebook-ban--5288966#story (accessed on January 31, 2026)

which calculates the economic cost of internet shutdowns utilising the Cost of Shutdown Tool (COST), it estimates that since Facebook was blocked in Uganda in January 2021, Uganda loses annually US$347,559,903, approximately UGX1,294,269,808,851.[34] As of early 2025, 38.6 million cellular connections were active in Uganda, accounting for 76.2% of the population. This means that the number of mobile connections in Uganda increased by 3.9 million (+11.1%) between the start of 2024 and the beginning of 2025.[35] Based on GSMA Intelligence data, it is suggested that now 86.5% of mobile connections in Uganda are considered "broadband", meaning they connect via 3G, 4G, or 5G mobile networks, and the rise of eSIMs has made this even easier over recent years.[36] However, the 2024 National Population & Housing Census report highlighted significant differences in internet usage by gender, with 11% of men reporting internet use compared with 8% of women. It also showed regional disparities, with Buganda (19%) having the highest proportion of internet users, whereas Karamoja (3%) had the lowest. Uganda has made progress in internet access and digital engagement, aligning with the ACHPR Principle 38 on non-interference in the context of media and freedom of expression, as set out in the Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019).

Online freedom of expression and access to information

Uganda's legal system grants broad powers to restrict digital expression. The Computer Misuse Act, 2022, under Section 29(5), criminalises many online activities, such as "sending unsolicited messages" and "sharing malicious information," with vague terms that grant authorities broad powers to arrest content protected by the Constitution. Even though false news (2004) and sedition (2010), which were contained in the Penal Code Act (Cap. 120), were repealed, their manifestations remain through practices.[37] The Ugandan government has continued to restrict free expression online, cracking down on social media users and imposing multi-year prison sentences. A May 2025 report from Access Now documented at least 17 individuals who were arbitrarily detained or charged under Uganda's anti-LGBT+ laws from May 2023 to March 2025 after online entrapment or deception.[38] Freedom House and WOUGNET also report that women's freedom of expression is also limited by online gender-based violence, trolling, and self-censorship.[39]

Concerns remain about the accessibility of information related to the ACHPR's operations and its independence from government influence.[40]

Uganda was one of the first African countries to establish a right-to-information law with the Access to Information Act (ATIA) in 2005, followed by the Access to Information Regulations in 2011, which aligns with the principle of guaranteeing legal rights to access information held by public bodies.[41] This legislation aims to promote access to information, foster government transparency, and encourage citizen participation in decision-making. Since the enactment of ATIA, the Ugandan government has initiated several programs to enhance access to information, including the Ministry of ICT and National Guidance, which is responsible for formulating ICT policies and managing national infrastructure. There is supposed to be an Information Commission to oversee the act's implementation and handle complaints, though it has not yet been established, which leaves a major gap in the legal and institutional framework.[42] Most of these efforts are positive but insufficient when considered against the legal rights guaranteed. This is because it is hampered by challenges such as political will and slow response times. Increased efforts in public education are necessary

34. Netblocks Cost of Shutdown Tools https://netblocks.org/cost/
35. Simon Kemp. (3 March 2025). Digital 2025: Uganda https://datareportal.com/reports/digital-2025-uganda (accessed on November 30, 2025)
36. Ibid
37. Uganda Steps Up Pressure on Social Media Critics Ahead of 2026 Polls https://cipesa.org/2025/04/uganda-steps-up-pressure-on-social-media-critics-ahead-of-2026-polls/ (accessed on November 30, 2025)
38. Access Now. (19 May 2025). How Uganda's anti-LGBTQ+ laws entrap people online https://www.accessnow.org/uganda-anti-lgbtq-entrapment-laws/ (accessed on November 30, 2025)
39. Women's Freedom of Expression: What Are The Challenges & Their impacts to women's participation in Digital Spaces? https://wougnet.org/womens-freedom-of-expression-what-are-the-challenges-their-impacts-to-womens-participation-in-digital-spaces/ (accessed on November 30, 2025)
40. Ronald Musoke, 'Uganda: Is UCC Going Rogue?'(5 December 2017) The Independent (Kampala) https://allafrica.com/stories/201712050069.html (accessed on November 18, 2024)
41. CIPESA, 'The State of Access to Information in Uganda' https://cipesa.org/wp-content/files/briefs/report/Position-Paper-The-State-of-Access-to-Information-in-Uganda.pdf (accessed on November 19, 2024)
42. AFIC. (31/05/2024). Access to Information in Uganda: Prospects and Hurdles https://www.africafoicentre.org/access-to-information-in-uganda-prospects-and-hurdles/ ((accessed on November 30, 2025)

to bridge the gap between legislation and practical application.

Additionally, Uganda's 1995 Constitution guarantees citizens the right to access information held by the state, with some limitations for security and privacy.[43] This right is also recognised by international frameworks, including Article 19 of the International Covenant on Civil and Political Rights and Article 9 of the African Charter on Human and Peoples' Rights.[44] The Access to Information Act of 2005 grants citizens the right to access information, but in practice, many face challenges.[45] Section 3(d) of the Act requires that citizens access information within 21 days. However, delays caused by fear and bureaucracy often make this right difficult to exercise, especially for journalists and human rights enforcers. These barriers hinder residents' access to information, thereby contradicting the principle of expeditious access outlined in the ACHPR. While the Act should allow public access to information affecting citizens, Article 41 of the Constitution and other sections limit this right to information held by public bodies, excluding private companies and civil society, because it is the duty of state actors to provide information necessary to protect human rights.

In contrast, non-state actors do not have the same obligations. However, this exclusion of other entities raises concerns about the practicality and efficiency of accessing information, which is critical to compliance with Principle 26(a) of the ACHPR. The ATIA primarily covers information from public bodies, excluding private entities, and limits access to protect rights. Despite these obstacles, radio is still the primary information source with 68% of Ugandans relying on it, though its usage is declining, especially in urban areas.[46] Television usage remains widely used as a source of information and entertainment. Internet and social media usage have increased.[47] Word of mouth as a source of information rose significantly from 4% to 16%.[48]

In 2025, Uganda's regulatory environment for online content raised concerns about its alignment with the principles set out in the ACHPR, particularly the rights to freedom of expression and access to information. In recent years, the Ugandan government has implemented stringent measures under the Computer Misuse (Amendment) Act, 2022, specifically Section 3 (Unauthorized Access), Section 4 (Unauthorized Use of Computer Misuse), Section 5 (Cyber Harassment), Section 6 (Cyberbullying), and Section 7 (False or Misleading Information) which lay together the groundwork for increased control and regulation of online speech, which many critics perceive as a means to stifle dissent and limit freedom of expression in Uganda, and additionally through actions by the Uganda Communications Commission (UCC) to control online discourse, often justifying them as necessary for national security and public order. However, human rights experts broadly view these laws and their enforcement as failing to respect rights, owing to vague language, lack of transparency, and their use to suppress dissent and media freedom.[49]
Government-controlled content includes Facebook blocking, platform monitoring and requests, media bans, internet shutdowns, platform content removal, and regulations on social media use, as well as the monitoring and potential removal of content deemed inappropriate by authorities. For instance, in October 2025, a government ban was imposed on the Nation Media Group, which drew criticism from civil society for breaching press freedom and constitutional rights.[50] Additionally, the government is actively acquiring social media monitoring tools and invoking laws such as the Computer Misuse Act to prosecute users of platforms such as TikTok, YouTube, and X (formerly Twitter) for online speech.[51] Between April and June 2025, TikTok removed more than 1.5 million Ugandan videos for violations, including hate

43. https://cipesa.org/wp-content/files/briefs/report/Position-Paper-The-State-of-Access-to-Information-in-Uganda.pdf (accessed on November 11, 2024)
44. https://cipesa.org/wp-content/files/briefs/report/Position-Paper-The-State-of-Access-to-Information-in-Uganda.pdf (accessed on November 11, 2024)
45. https://chapterfouruganda.org/sites/default/files/downloads/The-Access-to-Information-Act-2005.pdf (accessed on November 11, 2024)
46. 'The power of radio in Uganda's climate fight' (February 12, 2025) https://acme-ug.org/2025/02/12/the-power-of-radio-in-ugandas-climate-fight/ (accessed on November 30, 2025)
47. Stephen Kalema. (7 February 2025). Radio listenership on Decline: How Digital and On-Demand Content Are Reshaping Uganda's Media Landscape https://www.watchdoguganda.com/news/20250208/177745/radio-listenership-on-decline-how-digital-and-on-demand-content-are-reshaping-ugandas-media-landscape.html (accessed on November 30, 2025)
48. https://www.independent.co.ug/radio-still-most-popular-media-in-uganda/ (accessed on November 11, 2024)
49. Uganda Steps Up Pressure on Social Media Critics Ahead of 2026 Polls https://cipesa.org/2025/04/uganda-steps-up-pressure-on-social-mStrategiesedia-critics-ahead-of-2026-polls/
50. CPJ. (October 30, 2025 12:36 PM EDT). Ugandan authorities ban Nation Media Group from parliamentary, presidential coverage https://cpj.org/2025/10/ugandan-authorities-ban-nation-media-group-from-parliamentary-presidential-coverage/ (accessed on December 2, 2025)
51. NOELYN NASSUUNA AND HELEN NAMYALO KIMBUGWE. (7 April 2025). Uganda's Move to Procure Social Media Tracking Tool: A New Threat to Digital Rights and Freedoms https://www.defendersprotection.org/wp-content/uploads/2025/04/Ugandas-Move-to-Procure-Social-Media-Tracking-Tool-.pdf (accessed on December 2, 2025)

speech, misinformation, and obscenity.[52] Uganda ranked 29th worldwide for video deletions during this period.[53] This figure surpasses Kenya's 592,000 and South Africa's 420,000. Thousands of videos in Nigeria were also affected.[54] Facebook has been continuously blocked, and during a presidential address on youth concerns on November 30, 2025, President Yoweri Kaguta stated, "I had to teach Facebook a lesson. They thought that without them Uganda wouldn't survive. We had to make sure that Facebook knows we are unstoppable".[55] This prompted Ugandan citizens to anticipate additional 'lessons' ahead of the January 2026 presidential elections.

In July 2025, Google's actions were found to violate Uganda's Data Protection and Privacy Act 2019 by failing to register as a data controller and by illegally transferring data, highlighting ongoing regulatory issues and gaps in legal oversight. On November 8 2024, four Ugandan complainants filed a complaint with the Uganda Personal Data Protection Office (PDPO) against Google for failing to register and for conducting cross-border data transfers without approval. On November 5 2025, Google withdrew its appeal following discussions led by the ICT Minister, marking a significant milestone in African digital rights and platform accountability.[56] Google acknowledged the PDPO's authority, began compliance efforts, and emphasised that Ugandan data rights are non-negotiable. Uganda has a complex legal framework governing digital rights, including Article 29 of the Ugandan Constitution, which guarantees freedom of speech, expression, and the press.

The Computer Misuse (Amendment) Act 2022 is the main law for regulating online content, which criminalises various online actions such as sharing "malicious information," engaging in "Hate speech" (vaguely defined), using social media under a "disguised or false identity," and distributing "unsolicited information." In January 2023, the Constitutional Court annulled Section 25 of the 2011 Act, which penalised "offensive communication," but the 2022 amendment, specifically Section 17, retained similar broad provisions.[57]

Recent years have seen a rise in arbitrary arrests, judicial harassment, and torture of environmental and land rights defenders. Lawyer Eron Kiiza, known for environmental and rule-of-law advocacy, was detained. This trend reflects broader suppression of rights to peaceful assembly and expression under Ugandan law (Article 29 of the Constitution) and international law (Articles 19 and 21 of the ICCPR).[58]

On March 13 2025, two journalists were injured and their equipment confiscated at a private residence where Opposition Leader Joel Ssenyonyi and NUP Secretary-General Lewis Rubongoya visited to investigate ballot pre-ticking ahead of the Kawempe North by-election. Stephen Kibwiika of NTV/Spark TV was severely assaulted during the event on March 12.[59] Kibwiika, a journalist, faced severe harassment while covering suspected electoral misconduct in Kawempe. After receiving a tip-off from the Leader of the Opposition, he and his team witnessed individuals removing vehicle number plates. They were violently attacked by plainclothes assailants, resulting in Kibwiika sustaining injuries from batons and kicks, and ultimately surrendering his camera.[60] This incident highlights a troubling trend of violence against journalists, including Thomas Kitimbo of NBS TV, who was injured and had his phone taken, underscoring the broader attacks on media freedom during the Kawempe North campaign.[61] When HRNJ-Uganda contacted the police, Deputy Spokesperson Luke Oweyesigire denied any security involvement and urged that any complaints be filed at Kawempe Police Station for investigation.[62] The Kawempe North by-election has seen violence, with over five journalists attacked, including Miracle Ibra of Top Television, who was hospitalised in critical condition, Steven Mbidde of NTV, Stephen Kibwiika, and Thomas Kitimbo of NBS TV.[63]

Such practices have led to self-censorship that stifles dissent and suppress-

52. https://www.instagram.com/reel/DQ56DUsD51u/?hl=en (accessed on January 31, 2026)
53. TikTok deletes 1.5 million videos posted by Ugandans https://www.trtafrika.com/english/article/c2d9004f3b13 (accessed on December 2, 2025)
54. Ibid
55. https://www.facebook.com/AtekerTv/posts/president-kaguta-museveni-i-had-to-teach-facebook-a-lesson-they-thought-that-wit/1331784655628337/ (accessed on January 31, 2026)
56. Emmanuel Ngwa. (28 November 2025). Google withdraws appeal in Uganda privacy case — victory for digital rights across Africa? https://ngwaspenn.com/google-withdraws-appeal-in-uganda-privacy-case-victory-for-digital-rights-across-africa/ (accessed on December 2, 2025) ecological and rule-of-law
57. Uganda Steps Up Pressure on Social Media Critics Ahead of 2026 Polls https://cipesa.org/2025/04/uganda-steps-up-pressure-on-social-media-critics-ahead-of-2026-polls/ (accessed on December 2, 2025)
58. Ibid
59. HRNJ Uganda. (March 13, 2025). Escalating Attacks on Journalists During Kawempe North By-Election Raise Serious Concerns https://hrnjuganda.org/?p=10151 (acessed on December 3, 2025)
60. Ibid
61. Ibid
62. HRNJ Uganda. (March 13, 2025). Escalating Attacks on Journalists During Kawempe North By-Election Raise Serious Concerns https://hrnjuganda.org/?p=10151 (accessed on December 3, 2025)

es critical voices, which are crucial to a healthy democratic society. The ACHPR emphasises the importance of freedom of expression as an inherent feature of democratic governance. Article 9 of the Charter explicitly states that every individual shall have the right to express and disseminate their opinions within the law. Uganda's current approach to content moderation and censorship may be inconsistent with these commitments, as it significantly limits citizens' ability to engage freely in public discourse. Moreover, the enforcement of content moderation policies often lacks transparency and due process, further complicating the situation. Reports of arbitrary arrests and harassment of journalists, bloggers, and activists have highlighted the risks faced by those who seek to express dissenting opinions or share information that counters government narratives.[64] Advocacy efforts are vital in promoting a more open and accountable governance framework in an increasingly connected world.

Gendered disinformation

Addressing gendered disinformation is crucial for ensuring a fair electoral landscape and combating gender inequality in Uganda.[65] Disinformation often manifests through the manipulation of information, demonisation of gender equality ideals, and various forms of abuse, including trolling and body shaming. Women, specifically women in leadership, journalists and human rights defenders, are frequently the primary targets of gendered disinformation, which marginalises their decision-making participation. Women leaders in Uganda, Kenya, and South Africa have reported experiencing AI-generated deepfake assaults and threats of physical violence, a rising concern in 2025.[66] A survey across Ethiopia, Kenya, Uganda, Senegal, and South Africa found 28% of women experienced online violence.[67]

63. Consolate Namyalo. (March 12, 2025). NUP's Rubongoya, Journalist Injured in Kawempe By-Election Drama https://chimpreports.com/nups-rubongoya-journalist-injured-in-kawempe-by-election-drama/ (acessed on December 3, 2025)
64. Brian Byaruhanga, 'Navigating the Threats To Journalism in Uganda' (June 30, 2023) https://cipesa.org/2023/06/navigating-the-threats-to-journalism-in-uganda/ (accessed on January 14, 2025)
65. Muhamadi Matovu, 'How gender focused misinformation impacts women in Ugandan politics' (WED 10 JUL, 2024 12:35) https://nilepost.co.ug/politics/206987/how-gender-focused-misinformation-impacts-women-in-ugandan-politics (accessed on November 18, 2024)
66. Pius Serugo. (Tuesday, December 2, 2025). Digital violence in East and Southern Africa: Urgent action needed to protect women and girls online https://nilepost.co.ug/news/307562/digital-violence-in-east-and-southern-africa-urgent-action-needed-to-protect-women-and-girls-online (accessed on December 3, 2025)
67. Ibid

Additionally, 42% of female African parliamentarians reported online death, rape, or abduction threats.[68] Martha Karua, a female politician from Kenya, was targeted for being a woman and single, accused of indecisiveness and responsible for the 2008 post-election chaos, with social media blamed for taking part in violence.[69] The impact of gendered disinformation extends beyond individual harm; it undermines public discourse and diminishes women's credibility, discouraging their political engagement. Many women withdraw from political processes due to intimidation tactics, while those with multiple identities often face heightened discrimination and hate speech. For instance, former Speaker of Parliament Rebecca Kadaga and Doreen Nyandura have been identified as targets of gendered disinformation campaigns.[70]

Another example is Dr Miria Matembe, a well-known politician and women's rights advocate, who filed a defamation lawsuit against Ofono Opondo, a government spokesperson, for making sexist comments about her during Uganda's political show on NBS Frontline, including claims that her husband left her for a housemaid.[71] The civic space for women journalists is shrinking due to gender-based violence, affecting their well-being and press freedom.[72] In Uganda, fear of attacks often prevents critical reporting. The mental health crisis among journalists worsens, with many suffering from burnout, trauma, and anxiety. New threats include disinformation, cyber-attacks, online media regulation, and ethical issues related to AI. Furthermore, a Sudanese hacker compromised Uganda's telecoms, with leaked data exposing journalists to identity theft and potential harm.[73]

68. IPU report highlights widespread sexism & violence against women MPs in Africa https://www.bgipu.org/activity-reports/widespread-sexism-and-violence-against-women-in-african-parliaments-according-to-new-ipu-report/ (accessed on December 3, 2025)
69. https://www.facebook.com/groups/thekenyatimes/posts/1377113230217692/ (accessed on December 3, 2025)
70. WOUGNET. (March 2025). Women in Journalism and Politics: Countering Gendered Disinformation in Uganda https://wougnet.org/download/women-in-journalism-and-politics-countering-gendered-disinformation-in-uganda (accessed on December 3, 2025)
71. Sandra Aceng. (24 September 2025). The Role of Multistakeholderism in Countering Gendered Disinformation in Africa https://www.genderit.org/feminist-talk/role-multistakeholderism-countering-gendered-disinformation-africa (accessed on December 3, 2025)
72. Examining the gendered dimensions of Journalists safety based on Unesco's JSI on IN Kenya, Tanzania and Uganda https://www.africafoicentre.org/examining-the-gendered-dimensions-of-journalists-safety-based-on-unescos-jsi-on-in-kenya-tanzania-and-uganda/ (accessed on November 18, 2024)
73. AFIC. (20/06/2025). One Step Forward, Two Steps Back: Uganda's Slippery Media Landscape in 2024 https://www.africafoicentre.org/one-step-forward-two-steps-back-ugandas-slippery-media-landscape-in-2024/ (accessed on December 3, 2025)

Misinformation also politicises gender equality efforts, silencing women and perpetuating negative perceptions of their roles. Gender stereotypes and hypersexualisation in politics aim to discredit women, causing many to withdraw from public life. Social media enables the rapid dissemination of harmful narratives, and anonymity can be exploited to spread derogatory comments and misinformation. Additionally, algorithms that prioritise engagement may promote divisive content, further marginalising women candidates and reinforcing gender stereotypes. Although laws like the Computer Misuse Act exist, there is a lack of specific policies addressing gendered disinformation in Uganda.[74] Some laws, like those against hate speech and disinformation, have been misused to silence women, journalists, and activists instead of protecting them. Organisations now push for laws on Technology-Facilitated Gender-Based Violence (TFGBV) to fill legal gaps, holding offenders and service providers accountable. The Sexual Offences Bill doesn't define TFGBV, limiting its effectiveness.[75]

While Part I of the Bill mentions sexual offences and digital platforms, it lacks a clear TFGBV definition, making it less effective against online sexual offences. It's crucial to include a clause defining TFGBV in accordance with international standards and Ugandan law, including the 1995 Constitution, the Data Protection Act 2019, the Computer Misuse (Amendment) Act 2022, the Penal Code Cap 120, and the Uganda Communications Act 2013.[76]

Data Protection and Cybersecurity

Uganda's legal framework is supported by the Data Protection and Privacy Act 2021 and the Personal Data Protection Office (PDPO), the regulator. This sets a comprehensive basis of data handling because the law applies to all entities controlling or processing personal data by mandatory registration with the PDPO, including offshore ones handling Ugandan citizens' data.[77] n2025, Uganda has seen some significant development in its data protection enforcements, such as Uganda's PDPO's increased enforcement, issuing a landmark ruling against Google LLC—the first criminal conviction under the country's Data Protection and Privacy Act, Cap 97.[78] Dated July 18 2025, the verdict finds Google breached data transfer rules and must comply within 30 days. The case originated from an November 8 2024 complaint by four Ugandans, accusing Google of unlawfully collecting, processing, and transferring their data without safeguards.[79] This sets a precedent for multinational companies on platform accountability.

Additionally, some of the cases of personal data misuse by the state and private sector include Uganda's first data protection conviction on July 10 2025, which marks a significant milestone in digital privacy enforcement through a case against Nano Loans Microfinance Ltd. The director was found guilty of operating without PDPO registration and unlawfully processing personal data, resulting in a fine and a criminal record.[80] This shifts data violations from civil to criminal offences, impacting sectors such as finance, healthcare, and e-commerce. It encourages companies to review compliance, emphasising data protection at the executive level, particularly in debt recovery involving borrower information.[81] The case sets a regional precedent, demonstrating that data laws can be enforced amid rapid digital growth in East Africa. This case confirms that digital rights are enforceable and underscores the importance of legal compliance to foster trust and growth in Africa's digital economy.[82]

In December 2025, a finance manager at Vuka Africa Ltd was fined UGX100,000, approximately US$27, and if he defaulted, sentenced to two months in jail after

74. https://nilepost.co.ug/politics/206987/how-gender-focused-misinformation-impacts-women-in-ugandan-politics (accessed on November 18, 2024)
75. CIPESA. (February 25, 2025). CIPESA and Partners Advocate for Inclusion of Technology-Facilitated Gender-Based Violence in Uganda's Sexual Offences Bill https://cipesa.org/2025/02/cipesa-and-partners-advocate-for-inclusion-of-technology-facilitated-gender-based-violence-in-ugandas-sexual-offences-bill/ (accessed on December 3, 2025)
76. Ibid

77. Paul Mbuga and Ruth Muhawe. (23 July 2025). Uganda's Data Protection regulator clarifies compliance requirements for offshore entities https://www.dlapiperafrica.com/en/uganda/insights/2025/CLIENT-ALERT (accessed on December 5, 2025)
78. Business Times Uganda. (July 25, 2025). Uganda's data protection office finds google in breach of privacy law https://businesstimesug.com/ugandas-data-protection-office-finds-google-in-breach-of-privacy-law/ (accessed on December 3, 2025)
79. Ibid
80. Alice Namuli Blazevic., Patrick Mugalula. (30 September 2025). Uganda's First Data Protection Conviction: A New Era for Digital Privacy Enforcement in Africa https://lexafrica.com/2025/09/uganda-data-protection-conviction-digital-privacy-enforcement-africa/ (accessed on December 4, 2025)
81. Ibid
82. Ibionline and offline privacyd

admitting to not registering the company with the PDPO before handling client data.[83] This act violated Section 29 (1) of the Data Protection and Privacy Act 2019 and regulations 15 of the Data Protection and Privacy Regulations 2021.[84] The case underscores the need to enforce the mandatory registration requirement for all data controllers and processors in the country.

While Article 27 of the Constitution protects individuals' privacy,[85] the Data Protection and Privacy Act of 2019, effective April 2021, faces challenges in enforcement.[86] NITA Uganda and UCC have raised awareness by providing guidelines and digital security training, though reaching SMEs remains a considerable challenge.[87] Additionally, on 3rd September 2025, NITA-U and the Personal Data Protection Office launched the "Beera Ku Guard" campaign, a nationwide effort to empower Ugandans to protect their personal data and privacy. It aims to raise awareness of cybersecurity, data protection, and online and offline privacy. Uganda's cybersecurity strategy 2022-2026 aims to strengthen digital security but raises human rights concerns due to its broad language, particularly in the Computer Misuse Act.[88] Terms like "unlawful access" and "misuse" could unfairly criminalise legitimate activities such as political expression and information sharing. The 2011 Act's vague language may be exploited against critics and journalists, granting law enforcement extensive surveillance powers and potentially infringing on privacy.[89] The Personal Data Protection Office (PDPO) introduced a Data Protection and Privacy Compliance Toolkit after stakeholder consultations last year to help organisations comply with the Data Protection and Privacy Act, Cap 97, reflecting Uganda's commitment to data protection.[90] Uganda's Ndaga Muntu digital ID system is transitioning to a more secure 'smart ID' with biometric capabilities, with nationwide renewal and registration starting in May 2025. About 17.2 million new registrations and 5 million renewals are planned before the 2026 elections. The new ID system will feature security features such as Multiple Laser Images (MLI), Machine-Readable Zones (MRZ), QR codes, and 2D barcodes, with plans for e-IDs without expiry dates.[91] The government emphasises the ID's importance for access to services such as education, pensions, and banking, warning that all services will rely on it. Civil society is disappointed that a June 2025 High Court ruling upheld the ID's mandatory use despite 40% of the population lacking one, risking increased digital exclusion for vulnerable groups.[92] Despite these issues, digital ID also faces challenges related to digital exclusion, awareness, registration efficiency, and the lack of alternatives. Civil society advocates for transparent, rights-based oversight to protect privacy and prevent misuse. This adherence to ACHPR's Principle 42 on privacy and the protection of personal data will ultimately reinforce democratic participation and public trust.

Uganda's domestic laws align with principles in the regional and international instruments such as the AU Convention on Cybersecurity and Personal Data Protection (the Malabo Convention) and the African Charter on Human and Peoples' Rights, specifically principle 42 concerning personal data protection legislation.[93] However, the country has not yet ratified the Malabo Convention.[94]

Privacy and surveillance

Uganda's legal framework enables widespread surveillance justified by security

83. Juliet Kigongo. (Thursday, December 04, 2025). Kampala finance manager sentenced over illegal data collection https://www.monitor.co.ug/uganda/news/national/kampala-finance-manager-sentenced-over-illegal-data-collection-5286350 (accessed on December 5, 2025
84. Ibid
85. CONSTITUTION OF THE REPUBLIC OF UGANDA, 1995. https://www.ngobureau.go.ug/sites/default/files/laws_regulations/2020/12/Uganda%20Constitution%201995.pdf (accessed on November 28, 2024)
86. Privacy Scorecard Report 2021 https://www.unwantedwitness.org/wp-content/uploads/2021/11/Privacy-Scorecard-Report-2021.pdf (accessed on November 18, 2024
87. Business Times Uganda. (August 4, 2025). Cybersecurity and data protection challenges facing SMEs in Uganda https://businesstimesug.com/cybersecurity-and-data-protection-challenges-facing-smes-in-uganda/ (accessed on December 3, 2025)
88. https://v45.diplomacy.edu/resource/ugandan-national-cybersecurity-strategy-2022-2026 (accessed on December 5, 2025)
89. https://cipesa.org/2025/04/uganda-steps-up-pressure-on-social-media-critics-ahead-of-2026-polls/ (accessed on December 5, 2025of ID)
90. PDPO Launches Toolkit to Empower Organizations Comply https://www.pdpo.go.ug/news/pdpo-launches-toolkit-to-empower-organizations-comply (accessed on December 4, 2025)
91. Davidson Ndyabahika. (May 19, 2025). ResearchUganda's National ID Delivers $1.35 for Every $1 Invested https://news.mak.ac.ug/2025/05/ugandas-national-id-delivers-1-35-for-every-1-invested/ (accessed on December 5, 2025)
92. Michael Aboneka. (2025). Uganda's Digital ID Barrier Worsens as Court Delivers Blow to Access https://digitalrightsalliance.africa/ugandas-digital-id-barrier-worsens-as-court-delivers-blow-to-access/ (accessed on December 5, 2025)
93. Media Defence.(February 2025). Data Privacy and Data Protection – sub-Saharan Africa https://www.mediadefence.org/resource-hub/data-privacy-protection-sub-saharan-africa/ (accessed on December 5, 2025)
94. Ratify the Malabo Convention, a call to Government of Uganda as we mark the Human Rights Day, 2019 https://www.unwantedwitness.org/ratify-the-malabo-convention-a-call-to-government-of-uganda-as-we-mark-the-human-rights-day-2019/ (accessed on December 5, 2025)

concerns but raises human rights concerns. Laws like the Regulation of Interception of Communications Act, 2010, allow monitoring with judicial approval, but oversight is limited, creating opacity and accountability problems.[95] The Anti-Terrorism Act, 2002, grants broad powers that are often used to target opposition, journalists, and activists. The Uganda Communications Act, 2013, gives the Communications Commission control over infrastructure and surveillance, with SIM registration aiding monitoring.[96] The 2011 Computer Misuse Act, amended in 2022, criminalises vague online offences that are frequently used against journalists and activists. Although the 2019 Data Protection and Privacy Act establishes data principles, it excludes security data, allowing unchecked surveillance. These laws foster extensive monitoring with limited oversight, risking privacy, free expression, and civic participation.[97] The 2017 Anti-Terrorism Act permits the interception of communications without sufficient judicial oversight, impacting civil society and freedoms. It also highlights laws that lead to arbitrary arrests and criminalise dissent.[98] Human rights defenders, journalists, and opposition members face increased surveillance, harassment, and imprisonment, eroding democracy. For instance, Canary Mugume, a journalist from NBS Television, stated that Apple had previously sent him a warning message, indicating he was a potential target of government-linked spyware intended to monitor his personal or professional data.[99] Southeast Asian spyware targeted opposition groups and civil society, compromising devices. Israeli-made surveillance software, mainly used by police, extracts data to track dissenters, lawyers, and journalists.[100] The 2025 cyber surveillance report notes a rise in phishing and malware attacks targeting civil society, disrupting campaigns and threatening the use of encrypted apps.[101] Growing fear of infiltration undermines trust, discourages organisation, and suppresses protests. NGOs face suspension or are forced to share sensitive data under anti-government accusations. Overall, laws like the Computer Misuse Act create a chilling effect, causing activists and journalists to self-censor out of fear.[102]

Safe city initiatives and national ID systems have increasingly adopted facial recognition technology, sparking concerns over privacy, discrimination, and freedom of assembly as human rights issues. Data breaches pose a significant threat, risking long-term harm to individuals.[103] Alongside breaches, there are worries about unauthorised surveillance and the potential misuse of biometric information. The safe city programme also employs facial recognition CCTV in public spaces. Using biometrics for mass surveillance is a serious infringement on the right to privacy, a fundamental human right outlined in Article 27(2) of the 1995 Ugandan Constitution.[104] Additionally, there are concerns that biometric surveillance could reinforce societal biases and discrimination[105], and that awareness of law enforcement's real-time facial recognition efforts may undermine civil liberties.[106]

In April 2025, Uganda also embarked on a journey to purchase social media tracking tools through UCC, capable of monitoring and tracking social media activity, including users who use VPNs to access Facebook, which has been blocked since the January 2021 national elections.[107]On December 4 2025, the Uganda Communications Commission (UCC) cautioned people using VPNs to access Facebook that

95. Franklin Draku. (Tuesday, August 05, 2025). Ugandans under State surveillance ahead of 2026 elections https://www.monitor.co.ug/uganda/special-reports/elections/ugandans-under-state-surveillance-ahead-of-2026-elections--5143732 (accessed on December 5, 2025)
96. Franklin Draku. (Tuesday, August 05, 2025). Ugandans under State surveillance ahead of 2026 elections https://www.monitor.co.ug/uganda/special-reports/elections/ugandans-under-state-surveillance-ahead-of-2026-elections--5143732 (accessed on December 5, 2025)
97. Franklin Draku. (Tuesday, August 05, 2025). Ugandans under State surveillance ahead of 2026 elections https://www.monitor.co.ug/uganda/special-reports/elections/ugandans-under-state-surveillance-ahead-of-2026-elections--5143732 (accessed on December 5, 2025)
98. Franklin Draku. (Tuesday, August 05, 2025). Ugandans under State surveillance ahead of 2026 elections https://www.monitor.co.ug/uganda/special-reports/elections/ugandans-under-state-surveillance-ahead-of-2026-elections--5143732 (accessed on December 5, 2025)
99. https://www.biometricupdate.com/202508/fresh-concerns-over-impact-of-ugandas-expanding-digital-surveillance (accessed on 31 January 2026)
100. Surveillance/Spyware: An Impediment to Civil Society, HRDs and Journalists in East & Southern Africa https://www.unwantedwitness.org/wp-content/uploads/2025/06/Report-06.06.2025-FINAL.pdf (accessed on December 5, 2025)
101. https://www.unwantedwitness.org/wp-content/uploads/2025/06/Report-06.06.2025-FINAL.pdf (acessed on 31 January 2026)
102. Franklin Draku. (Tuesday, August 05, 2025). Ugandans under State surveillance ahead of 2026 elections https://www.monitor.co.ug/uganda/special-reports/elections/ugandans-under-state-surveillance-ahead-of-2026-elections--5143732 (accessed on December 5, 2025)
103. https://www.identity.com/privacy-concerns-with-biometric-data-collection/ (accessed on December 5, 2025)
104. Uganda's facial recognition technology threatens Privacy https://www.unwantedwitness.org/ugandas-facial-recognition-technology-threatens-privacy/ (accessed on December 5, 2025)
105. https://www.identity.com/the-intersection-of-artificial-intelligence-ai-and-biometrics/ (accessed on December 5, 2025)
106. https://www.identity.com/the-intersection-of-artificial-intelligence-ai-and-biometrics/ (accessed on December 5, 2025)
107. Surveillance and digital rights principles for use of FRT: Policing FRT the rights riks and harms https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/policing-frt-the-rights-risks-and-harms/ (accessed on December 5, 2025)

they are subject to legal action.[108] This is a significant privacy invasion, mass surveillance and potential censorship under the guise of national security.

The Parliament has multiple accountability committees that oversee governance by fulfilling their constitutional roles of passing legislation and scrutinising the executive branch. However, these committees face challenges in ensuring their reports are accepted and that the government takes prompt corrective action. Uganda's oversight system violates ACHPR principles 38 and 39(4) regarding online Content Removal Without Process, as the government frequently blocks social media during elections or protests and employs tracking tools without transparent, public, or judicial procedures, thus breaching due process. Principle 41 (Invasion of Privacy) allows broad, unreviewed powers under the Anti-Terrorism Act; the absence of independent oversight, vague legal language, and lack of accountability mechanisms heighten the risk of arbitrary, unlawful interference. Intelligence agencies report directly to the President, further compounding concerns.

Developments in ICT and emerging technologies

Uganda is currently in the foundational stage of developing a comprehensive AI regulation that aligns with UNESCO's global ethical standards, with a strong emphasis on human rights and economic development and ensuring ethical data governance, aiming to finalise it in 2025.[109] Concerns about artificial intelligence (AI) are growing as computer scientists predict that intelligent systems will increasingly take over decision-making tasks from humans.[110] According to the 2024 Government AI Readiness Index report by Oxford Insights, Uganda ranks 132 out of 193 countries in AI development based on government, technology, and infrastructure.[111] Despite this low ranking, local AI experts and organisations have trained 2,567 individuals to train one million Ugandans by 2030 to improve perceptions of generative AI.[112] The Ugandan government is also deploying AI technologies in various agencies to enhance efficiency, improve accuracy, address environmental challenges, bolster security, and provide personalised services to citizens.[113] Debates have taken place regarding the inclusion of AI regulations in the upcoming Copyright and Neighbouring Rights (Amendment) Bill, 2025.[114] However, the Uganda Registration Services Bureau (URSB) dismissed suggestions from legal experts and the Law Development Centre (LDC) to incorporate AI regulation into the Bill.[115] Additionally, Section 8 faced criticism for overlooking digital streaming platforms, which leads to income losses for artists. There have also been proposals for a platform accountability framework, including mandatory registration, transparency reports, algorithm disclosures, and revenue-sharing rules, to ensure creators receive at least 50% of net profits.[116]

The Ugandan government is actively applying AI across vital sectors such as agriculture, health, finance, and education.[117] These initiatives demonstrate how Uganda's digital transformation is enhancing services, increasing productivity, and improving citizens' quality of life, especially Uganda's active move toward a significant effort to establish a formal regulatory framework through actions such as drafting the Artificial Intelligence Bill, 2025.[118] Collaboration with the legal community, academia, and the United Nations aims to establish necessary regulations. It is also essential to consider the ethical concerns and social implications of AI adoption, including data privacy, security risks, the digital divide, and job displacement. Addressing these issues is vital for achieving sustainable outcomes in Uganda. The integration of AI technologies in Uganda has the potential to improve efficiency and security, but it must align with the ACPHR's principles, including Principle 39.

108. Stuart Ampaire. (December 4, 2025). UCC Warns Facebook Users: 'You Are Not Invisible' https://chimpreports.com/ucc-warns-facebook-users-you-are-not-invisible/ (accessed on December 5, 2025)
109. Uganda AI Regulation: Digital Policy and Legal Framework https://digital.nemko.com/regulations/uganda-ai-regulation (accessed on December 5, 2025)
110. https://www.independent.co.ug/ugandans-fear-artificial-intelligence/ (accessed on November 9, 2024)
111. Government AI Readiness Index 2024 https://oxfordinsights.com/ai-readiness/ai-readiness-index/ (accessed on January 8, 2024)
112. https://www.ntv.co.ug/ug/news/business/uganda-ranks-low-on-global-ai-index-as-experts-aim-to-train-1-million-4824128#google_vignette (accessed on November 16, 2024)
113. https://apsdpr.org/index.php/apsdpr/article/view/770
114. Prisca Wanyenya. (August 23, 2025). Lawyers Warn Uganda Risks Exploitation Without AI Copyright Safeguards https://parliamentwatch.ug/news-amp-updates/lawyers-warn-uganda-risks-exploitation-without-ai-copyright-safeguards/ (accessed on December 5, 2025)
115. Ibid
116. Ibid
117. Fiona Luboga. (Mar 20, 2025). Shaping Uganda's AI Future https://ict.go.ug/media/news/shaping-ugandas-ai-future (accessed on December 5, 2025)
118. https://www.scribd.com/document/846217865/Artificial-Intelligence-Bill-Draft (accessed February 5, 2026)

Digital Inclusion

Uganda advances digital inclusion for persons with disabilities (PWDs) by providing grants for digital literacy and training, reaching more than 1,000 PWDs, and by advocating for accessible ICT. Uganda's Constitution affirms principles of non-discrimination and accessibility. Therefore, exclusion from ICT services isolates PWDs from vital resources such as e-government, e-health, and e-commerce.[119] Laws such as the Persons with Disabilities Act, 2019, require more vigorous enforcement to ensure accessibility and active participation. Initiatives like the National Digital Observatory are advancing the goal of fostering digital inclusion and accessibility. They act as a centralised platform that supports PWDs, ensuring their inclusion in Uganda's digital transformation.[120] A call for proposals from the Uganda Communications Commission (UCC) and the Uganda Communications Universal Service Access Fund (UCUSAF) seeks to promote digital inclusiveness for Persons with Disabilities (PWDs) through ICT innovation and digital literacy initiatives.[121] The ICBVI course on general digital skills training for the visually impaired, under UCC/UCUSAF, is in progress, aiming to equip PWDs with digital skills for empowerment.[122]

Uganda is focused on strengthening existing legislation, such as the Computer Misuse Act 2011 and the Anti-Pornography Act 2014, to improve child online safety[123], in line with the African Union's digital protection initiatives for Uganda.[124] Nonetheless, new, comprehensive online-only laws are still under development, prioritising the integration of digital safety into broader policies such as the National Child Policy, enhancing reporting mechanisms (Sauti 116)[125], and tackling child sexual abuse material (CSAM) through stricter penalties and capacity-building, led by UNICEF and local authorities.[126]

Universal Service Fund (USF)

The Universal Service Fund, known as the Uganda Communications Universal Service and Access Fund (UCUSAF), aims to expand telecommunications access in unserved and underserved areas that are not commercially viable for licensed operators. By extending telecommunications access, UCUSAF helps bridge the digital divide and improve equity while supporting SDG 11 for sustainable cities.[127] UCUSAF receives annual contributions from licensed telecom operators, who pay a 2% levy on their gross revenues, ensuring that underserved populations gain access to essential communication services.[128]

In May 2025, MTN Uganda announced a contribution of UGX 50.55 billion (US$14.3 million) to the UCC's Universal Service and Access Fund, up from UGX 42.5 billion (about US$12 million) the previous year.[129] Similarly, Airtel Uganda contributed UGX 37.9 billion to the UCUSAF, reinforcing its commitment to expanding digital connectivity across Uganda.[130] This is an 11.4% increase from last year's contribution. To ensure Uganda has safe, fast, reliable, and affordable communication services, Airtel Uganda also launched Uganda's first Spam Alert service as part of its responsible citizenship efforts to combat the global SPAM challenge.[131]

In July 2025, UCUSAF enrolled Trainers of Trainees (ToTs) in its maiden e-learning project, aimed at enhancing digital learning in Ugandan primary schools through a Digitally Enabled Community Development (ECD) approach, in line with the Uganda Communications Act 2013 and

119. https://ict.go.ug/media/news/government-formulates-national-ict-for-disability-policy
120. Digital Inclusion: A Fundamental Right For Persons With Disabilities In Uganda (19 May, 2025) https://app.ict4personswithdisabilities.org/news/14 (accessed on December 5, 2025)
121. https://www.ucc.co.ug/wp-content/uploads/2024/12/Call-for-Proposals-for-UCCUCUSAF-PWD-Support-Grant-V2.pdf (accessed on December 5, 2025)
122. https://ict.go.ug/media/news/digital-inclusion-for-the-visually-impaired-in-uganda (accessed on December 5, 2025)
123. https://isoc.ug/wp-content/uploads/2018/10/Advancing-the-plight-of-child-online-in-Uganda.pdf (accessed on December 5, 2025)
124. https://5rightsfoundation.com/africa-leads-as-first-region-to-adopt-child-online-safety-policy/ (accessed on December 5, 2025)
125. https://endviolenceagainstchildrenconference.org/wp-content/uploads/2024/11/Uganda-1.pdf (accessed on December 5, 2025)
126. https://www.unicef.org/uganda/what-we-do/child-protection (accessed on December 5, 2025)
127. UCUSAF -Access Infrastructure Program https://www.ucc.co.ug/ucusaf/access-infrastructure-program/ (accessed on November 18, 2024)
128. JAVIRA SSEBWAMI, 'Airtel pays UGX 34.8Billion to rural telecom fund' (April 4, 2024) https://www.pmldaily.com/business/2024/04/airtel-pays-ugx-34-8billion-to-rural-telecom-fund.html (accessed on November 18, 2024)
129. Mtn Uganda (12 May 2025). MTN Uganda announces UGX 50.55 billion contribution to UCC's Universal Service and Access Fund https://www.mtn.co.ug/mtn-uganda-announces-ugx-50-55-billion-contribution-to-uccs-universal-service-and-access-fund/ (accessed on December 5, 2025)
130. https://extensia.tech/airtel-uganda-contributes-ugx-37-9-billion-to-national-digital-inclusion-fund/ (accessed on December 4, 2025)
131. ChimpReports. (May 13, 2025). Airtel Uganda Contributes Shs37Bn to UCC in Support of Universal Access https://chimpreports.com/airtel-uganda-contributes-shs37bn-to-ucc-in-support-of-universal-access/ (accessed on December 5, 2025)

UCUSAF Strategy IV. Collaborating with Nkumba University, the DECEDA initiative leverages community structures and digital technology to deliver quality education to resource-scarce rural schools, building upon the Holistic E-Learning Platform (HELP). Furthermore, UCUSAF supports over 1,417 secondary and tertiary institutions with computer labs and plans to launch a pilot E-Classroom in selected primary schools by September 2025.[132]

In March 2025, Members of Parliament also called for increased funding to improve ICT access. A report by the Committee on ICT and National Guidance on the fund's operations highlights a shortage of computers in secondary schools, resulting in overcrowded labs and limited hands-on time for students.[133] An assessment revealed that while 90% of respondents own a phone (38% have smartphones), only 10% have reliable internet access, and 62.4% have yet to experience the Internet. More than 80% of respondents earn less than 500,000 Ugandan shillings per month. Despite this, 77% are members of savings groups, primarily relying on paper-based ledgers for record-keeping, which pose challenges such as fraud and delays—only 3% use automated systems, signalling a need for improvement.

The Uganda Communications Commission (UCC) distributed 16,344 tablets to disadvantaged communities in 91 districts through the Uganda Communications Universal Service and Access Fund (UCUSAF).[134] This initiative aims to enhance the use of Information and Communication Technology (ICT) in rural areas, where educational facilities are severely lacking. Currently, there are only 5,000 schools in rural areas, compared with 10,000 in urban areas, resulting in low school attendance and high dropout rates among children. Many rural schools lack electricity and qualified teachers, prompting the need for solar-powered tablets pre-loaded with educational content. Through UCUSAF, UCC distributed more than 150 tablets to residents in Kalungu District. This tablet distribution is part of UCUSAF's ongoing efforts to improve digital inclusion across Uganda. Having already delivered over 19,000 devices to 120 villages across the country, the programme aims to reach additional households, ensuring every community stays connected in the digital era.[135]

The E-Class Project, launched in partnership with World Vision Uganda, aims to enhance learning in Buikwe, Nakasongola, and Mpigi districts by incorporating digital tools into classrooms. Thirteen schools were selected to participate in this initiative, each receiving 40 tablets, a laptop, a projector, a charging station, and internet access.[136] For many students, this marks their first exposure to digital devices, expanding their access to academic content and enriching teachers' lesson delivery.[137]

UCUSAF is exploring future collaborations with institutions like Makerere University Business School (MUBS) to leverage ICT for educational enhancement and digital inclusion.[138] A grant application opened in May 2025 for partners to fund a device financing mechanism that helps underserved and unserved communities afford smartphones at half the price, with UCC contributing 50% of the device cost through a cost-sharing model.[139] Device financing will change the lives of many Ugandans, especially by giving ordinary citizens affordable access to smartphones and other essential tools.[140]

Children's rights online

Concerns about children's online safety are increasing as technology evolves, highlighting challenges in protecting their privacy in digital spaces. Although various regional treaties, such as the African Charter on Human and Peoples' Rights and the Malabo Convention, address child protection, they often do not explicitly safe-

132. https://uccinfoblog.com/2025/07/08/ucusaf-flags-off-trainers-for-maiden-e-learning-project/ (accessed on December 4, 2025)
133. https://www.parliament.go.ug/news/3634/mps-advocate-better-funding-improve-ict-access (accessed on December 4, 2025)
134. https://www.monitor.co.ug/uganda/news/national/ucc-moves-to-ratchet-up-digital-inclusion-learning-4879042 (accessed on December 4, 2025)
135. https://techreviewafrica.com/news/2058/uganda-communications-commission-distributes-tablets-to-kalungu-district-boosting-digital-inclusion (accessed on December 5, 2025)
136. https://spyreports.co.ug/bridging-the-digital-divide-e-class-project-transforms-learning-in-ugandan-schools/ (accessed on December 5, 2025)
137. https://spyreports.co.ug/bridging-the-digital-divide-e-class-project-transforms-learning-in-ugandan-schools/ (accessed on December 5, 2025)
138. https://news.mubs.ac.ug/principal-meets-ucusaf-director-to-explore-future-collaborations/ (accessed on December 5, 2025)
139. https://www.ucc.co.ug/wp-content/uploads/2025/05/Call-for-proposals22-05-25.pdf (accessed on December 5, 2025)
140. https://nilepost.co.ug/business/281768/device-financing-models-empowering-ugandans-to-build-businesses-and-boost-incomes (accessed on December 5, 2025)

guard children's online privacy rights.[141] In Uganda, although privacy rights are constitutionally guaranteed, there is no comprehensive legislation specifically addressing online safety for children. Existing laws, including the Children Act and several cyber laws, provide some protections, but the rise in internet use, particularly during the COVID-19 pandemic, has heightened the risk of exploitation.[142] The Uganda Communications Commission (UCC) is actively promoting online safety for children through advocacy and awareness campaigns. They, along with the Computer Emergency Response Team (CERT), work to monitor online threats and encourage Internet Service Providers (ISPs) to implement parental controls. However, risks remain significant for children aged 12-17 who engage with social media platforms, where most exploitation occurs through known perpetrators.[143] Many children do not report incidents due to stigma, fear, or lack of trust in law enforcement. Uganda also faces broader issues such as poverty, high dropout rates, and mental health challenges that further jeopardise children's safety online.[144] The digital landscape, enhanced by AI tools, creates new opportunities for predators to target vulnerable youths, while a lack of digital literacy among parents and institutions exacerbates the risks children face in the online world.[145] Overall, there is an urgent need for targeted, evidence-based strategies to protect children from online harm.[146]

141. https://cipesa.org/wp-content/files/Child_Protection_and_Safety_Online_in_Africa_Report_.pdf (accessed on February 5, 2026)
142. Ibid
143. Ibid
144. https://nilepost.co.ug/news/308317/experts-warn-of-rising-online-child-exploitation-and-persistent-poverty-in-uganda (accessed on February 5, 2026)
145. Ibid
146. .

Conclusion

This report outlines a complex landscape of digital rights and inclusion, highlighting both notable progress and ongoing challenges. Overall, Uganda has made commendable progress in expanding its digital infrastructure and legal frameworks, yet the country continues to face significant challenges that impede full compliance with the ACHPR Declaration. Despite these gains, ongoing threats to freedom of expression, widespread censorship, and internet shutdowns point to the urgent need for reform. The continuing digital divide, particularly between urban and rural areas, along with barriers faced by marginalised groups, further complicates the digital rights environment. Moreover, public awareness regarding digital rights remains alarmingly limited, and the enforcement of existing data protection laws is insufficient. The score of 25 underscores the urgent need for reform in Uganda to address these systemic issues, promote human rights, and create an inclusive digital environment for all citizens. While Uganda has established a foundation for digital rights and inclusion, concerted reform efforts are necessary to unlock the full potential of its digital landscape. By focusing on these key development areas, Uganda can improve its ratings under ACHPR standards and foster a more inclusive, rights-respecting digital environment for all citizens.

Recommendations

The Government should:

- Enhance implementation of the Data Protection and Privacy Act, 2019, and ensure robust enforcement mechanisms. This includes regular audits and assessments to

ensure compliance by both public and private entities.
- Develop and implement policies that promote digital rights in accordance with the ACHPR Declaration. Create clear guidelines that protect freedom of expression and access to information.
- Invest in expanding internet infrastructure, particularly in rural areas, to bridge the digital divide.
- Enact legislation prohibiting arbitrary shutdowns of internet services and censorship, especially during elections and civil unrest, to uphold citizens' right to information.
- Amend repressive laws such as the Computer Misuse Act (Amendment) 2022 with problematic restrictions on "unauthorized access" and "abusive communication" broadly interpreted to suppress online dissent, and Penal Code Act (Cap. 120).
- Adopt transparent practices concerning surveillance technologies and data protection to build public trust in data management.
- Develop policies that include marginalised populations in the digital economy and ensure fair access to resources.

The Media should:

- Engage in investigative journalism that highlights issues related to digital rights and holds authorities accountable for breaches. This will contribute to transparency and awareness.
- Ensure media coverage includes perspectives from marginalised groups, particularly those in rural areas, to highlight their challenges and experiences with digital access.
- Collaborate with legal experts and digital rights organisations to ensure accurate reporting on laws and policies affecting digital rights, helping to inform the public.
- Embrace digital platforms to widely disseminate information, particularly during periods of censorship or restrictions on traditional media.

Civil Society Organisations should:

- Actively advocate for the protection of digital rights at local, regional, and national levels by lobbying for policy changes and engaging with government agencies.
- Offer training programs to empower citizens, especially marginalised groups, to understand their digital rights and how to advocate for them. Provide resources to help them understand legal protections and how to navigate the digital landscape.
- Conduct ongoing research to document violations of digital rights and assess the effectiveness of existing laws and policies. Share findings with stakeholders to promote accountability.
- Foster coalitions among civil society groups, the media, and private-sector stakeholders to build a united front to advocate for digital rights and inclusion.

The Private Sector should:

- Implement robust data protection policies that align with the national legal framework and international standards—Prioritise transparency in data use and user consent.
- Provide training and resources to enhance consumers' digital literacy, especially in underserved communities. This can empower users to utilise digital tools effectively and safely.
- Work towards making internet services and digital tools more affordable and accessible, particularly in rural and low-income areas, through innovative pricing models or subsidisation.
- Implement Corporate Social Responsibility initiatives to enhance digital rights, such as funding community-based internet projects or supporting NGOs working in this area.

The Score Index

Nigeria, 2025

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

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)	3	2	Even though internet penetration has increased and civil society efforts to improve access to internet services have intensified, Internet shutdowns and censorship during elections, as well as the effects of repressive laws, significantly limit access to information and hinder communication, thereby breaching fundamental rights.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	2	2	While some measures are in place, the lack of adequate laws to ensure equitable internet access and affordability highlights a critical gap that undermines equity and inclusion.
False News Criminalisation	P22(2)	1	1	While regulations may address misinformation, they often fail and undermine protections for freedom of expression. They can be misused against dissent, especially given the reference to arrests related to false news. Additionally, the existence of laws criminalising the spread of what is deemed "false news" imposes a severe limitation on freedom of expression.
Sedition Legislation	P22(2)	1	3	Sedition was repealed as an offence in the Penal Code Act. However, critical voices are silenced by laws such as the Computer Misuse (Amended) Act 2022, which restrict free expression and are used to stifle criticism, posing a serious threat to democratic norms. This creates a fear of expression among citizens and the media.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P22(2)	1	1	The prevalence of arbitrary arrests and harassment creates an atmosphere of fear and inhibits free speech and civil liberties.
Data Protection Legislation.	P42	4	3	While some data protection measures and regulations exist, including ongoing efforts to establish a framework and limited enforcement, there is no independent Data Protection Authority. Implementation remains inconsistent and insufficient, indicating significant challenges in practical implementation and public awareness of safeguards to protect personal privacy effectively.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
States interfere and require the removal of online content by internet intermediaries.	P38 and P39(4)	2	2	State interference in the removal of online content undermines free expression and signals censorship practices that severely restrict access to information and limit the diversity of online viewpoints. The mention of unclear laws that could lead to self-censorship and potential misuse of surveillance laws indicates significant challenges to freedom of expression.
Invasion of Privacy of Communications	P41	2	2	Continuous invasions of privacy constitute a significant violation of personal rights and undermine trust in digital communications.
Failure by the government to proactively disclose and disseminate information on digital technologies.	P29(3)	3	2	Uganda's legal environment lacks transparency and proactive disclosure related to digital technologies, indicating a failure to ensure access to information.
AI and Emerging Technologies National strategies	P39(6)	3	2	While some strategies may exist, such as the National AI Taskforce, their effectiveness and alignment with international standards require further evaluation and enhancement. This is because of substantial concerns over privacy, freedom of expression, and the overarching climate of surveillance and censorship affecting ICT and emerging technologies in Uganda. However, Uganda currently has a draft Artificial Intelligence Bill 2025[147], which aims to regulate the development and use of AI in Uganda.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	3	2	The current status of child digital safety and privacy in Uganda remains insufficient. While existing frameworks exist, they lack specific provisions to address children's online safety. More comprehensive policies and laws are needed to adequately address the unique risks children face in the digital environment, including online harassment and exploitation. Additionally, efforts to raise awareness and educate parents, guardians, and children about digital privacy are still limited. There's a pressing need for collaborative initiatives involving government, civil society, and tech companies to create a safer online experience for children. The African Union's recent adoption of a Child Online Safety and Empowerment Policy may affect upcoming initiatives in Uganda on child online safety and empowerment.
Digital Inclusion	P37(3)	3	3	There are efforts to improve digital inclusion, but disparities in access and utilisation indicate a need for more extensive initiatives. Barriers such as surveillance practices, limited access to technology, and privacy concerns hinder meaningful progress, leaving Uganda below the threshold for substantial compliance.
Total (out of 60):	2024: **39**	2025 **42**		

147. Uganda's AI Bill 2025 Overview https://www.scribd.com/document/846217865/Artificial-Intelligence-Bill-Draft (accessed on March 17,2026)

Zambia

By Anonymous

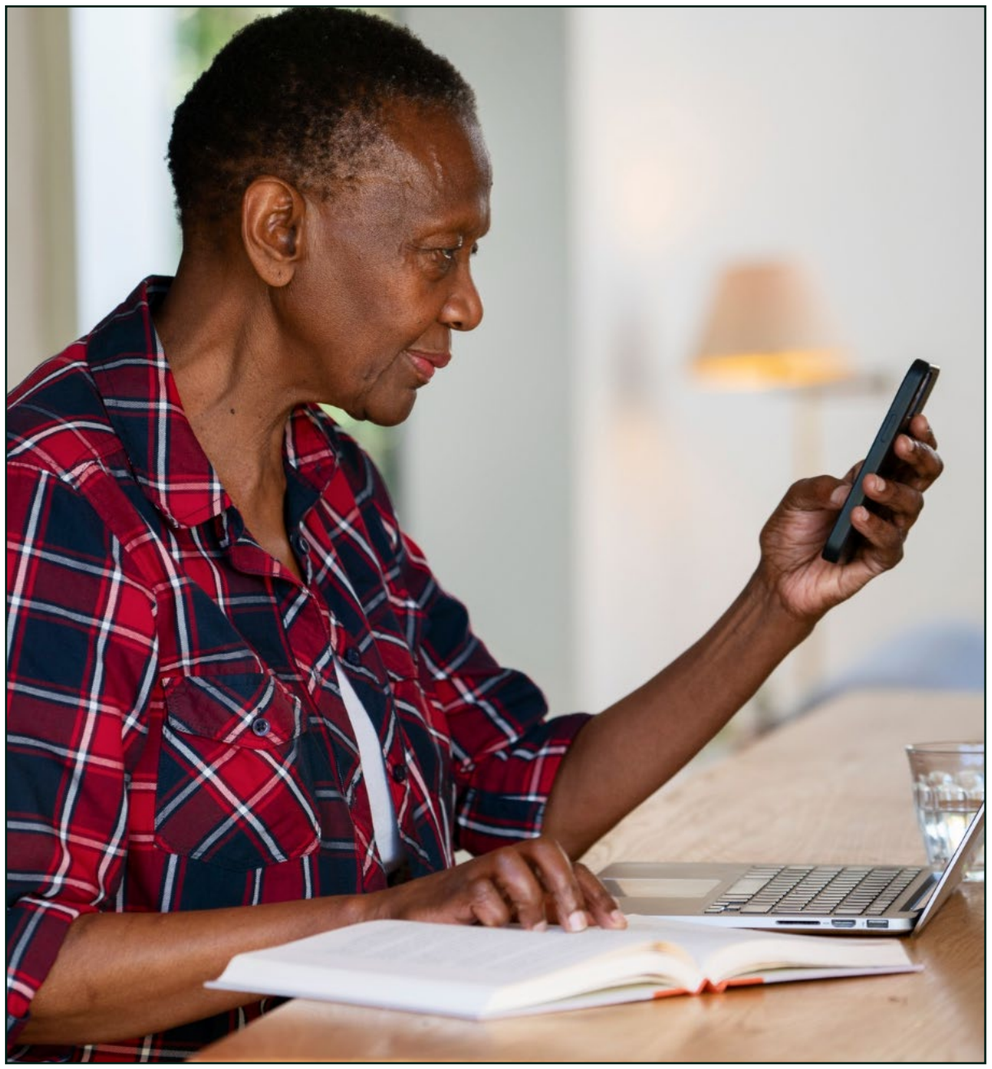
Executive Summary

The Londa Zambia report for 2025 provides an analysis of key developments and events within the country's Information and Communications Technology (ICT) and human rights landscape. It addresses thematic domains, including online freedom of expression, data protection, cybersecurity, digital inclusion, and the administration of the Universal Access and Service Fund. The methodology comprises a synthesis of desktop research, quantitative analysis, and consultations with subject-matter experts.

Zambia scores 40 out of 60 on Paradigm Initiative's TheScore Index, which evaluates compliance with key human rights elements, guided by the African Commission on Human and Peoples' Rights' Declaration of Principles on Freedom of Expression and Access to Information.

In 2025, the proliferation of connectivity services continued, supporting increased access for the Zambian population. Additionally, the National Artificial Intelligence Strategy was operationalised while the country launched the National Child Online Protection Strategy.

However, digital inclusion was hampered by quality of service and access challenges, driven by an acute energy crisis and high taxes towards the sector. The trend of the harassment and arrests of groups, such as opposition leaders and journalists, also continued. Policymakers also passed cyber legislation containing provisions that risk human rights violations and proposed a controversial Zambia Institute of Journalism Bill.



Introduction

Zambia is a landlocked Southern African country, whose economy and employment are heavily reliant on the mining and agricultural sectors. Zambia benefits from a stable democracy. The current president, Hakainde Hichilema, and his United Party for National Development (UPND), entered into power in August 2021.[1] This win was primarily driven by the youth, who spurred Hichilema's popularity on social media.

In 2025, Zambia experienced a slow but positive economic recovery, although many still live in poverty. Growing citizen dissatisfaction is increasingly expressed online, and there is also an increasingly charged atmosphere between the incumbent and opposition parties ahead of the August 2026 presidential elections.[2]

Zambia's eighth National Development Plan identifies Information and Communication Technologies (ICTs) as a vital part of the country's economic transformation. However, it notes that challenges such as limited infrastructure, low digital skills, and access to ICT devices exist.[3]

Several institutions play a role in Zambia's ICT sector; the Ministry of Technology and Science oversees ICT policy development and implementation, while the Zambia Information and Communications Authority (ZICTA) regulates the industry. The Electronic Government Division's SMART Zambia Institute manages and promotes electronic government services and processes to improve public service delivery.[4] The sector is also guided by the National Electronic Government Plan 2023-2026, which lays the foundation for enhanced service delivery, accessibility, transparency, and efficiency among the government, citizens, and the private sector. The Independent Broadcasting Authority regulates radio and television services.[5]

Zambia's ICT landscape is also shaped by frameworks including the National ICT Policy 2023, the National Digital Transformation Strategy 2023-2027, the Strategic Plan 2022-2026, and the Information and Communications Technologies Act of 2009.[6]

Internet access

Zambia's mobile market hosts four mobile network operators: Airtel Zambia, MTN, Zed Mobile, and the state-owned Zamtel. The latter is focused on 4G and eventual 5G coverage for data and voice. However, its services are currently concentrated in urban centres in the capital, Lusaka.[7] At the end of June 2025, Zambia had 24.5 million active mobile network subscriptions, a year-on-year growth of 12.1% and a penetration rate of 119.1%. Internet subscriptions also grew by 4.7% year-on-year, to 13.1 million.[8] Despite this, Zambia's data costs remain relatively prohibitive. According to the latest available data, Cable.co.uk's Worldwide Mobile Data Pricing 2022 report found that the average price of one gigabyte of data is US$8.01.[9]

Freedom of Expression and Access to Information

Zambia's National Constitution 2016[10] affirms the right to freedom of expression[11], assembly and association[12], access to information[13], and privacy.[14] It is also a signatory to regional and global human

1. BBC 'Zambia election: Hakainde Hichilema beats President Edgar Lungu" (2021) https://www.bbc.com/news/world-africa-58226695 (accessed on 30 October 2024).
2. Bulawayo 24 News 'Edgar Lungu, the Tonse Coalition, and Zambia's political landscape: A clash of visions ahead of the 2026 elections' (2024), (accessed on 27 November 2024).
3. Ministry of Finance and National Planning '8NDP (2022-2026)' https://www.mofnp.gov.zm/?wpdmpro=8ndp-2022-2026
4. Smart Zambia Institute https://www.szi.gov.zm/ (accessed on 21 November 2024)
5. Independent Broadcasting Authority Act (amended in 2010).
6. Kalemba 'Mutati launches ICT policy, digital transformation strategiis served byc plan' (2023) https://kalemba.news/busi ness/2023/10/14/mutati-launches-ict-policy-digital-transformation-strategic-plan/(accessed on 11 November 2024).
7. Fourth MNO (Zedmobile) services only available in Lusaka, https://zambianbusinesstimes.com/fourth-mno-zed-mobile-services-only-available-in-lusaka/(accessed on 19 November 2025)
8. ZICTA 'ICT Sector 2025 Mid-Year Market Report' (2025) chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.zicta.zm/uploads/9a0a836b-4e06-4fb2-b31b-6485ae3f4bea.pdf (accessed on 3 December 2025)
9. Cable.co.uk 'Worldwide Mobile Data Pricing 2022' (2023) https://www.cable.co.uk/mobiles/worldwide-data-pricing/ (accessed on 12 January 2024)
10. Constitution of Zambia Act 18 of 2016.
11. Constitution of Zambia Act 18 of 2016 art 20 n13 above.
12. n 13 above above, art 29.
13. n 13 art 21.
14. n 13, art 17.
15. African Commission on Human and People's Rights (ACHPR) Declaration on Freedom of Expression and Access to Information, https://www.achpr.org/legalinstruments/detail?id=69 (accessed 9 November 2025).

rights instruments, affirming the same, including the African Charter on Human and Peoples Rights (ACHPR)[15], the Windhoek Declaration for the Development of a Free, Independent and Pluralistic Press[16], the African Platform on Access to Information (APAI) Declaration[17] and the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention)[18], among others.

Regarding online freedoms, for 2025, Zambia retained its rating as "partly free" with a score of 62 on Freedom House's Freedom On The Net Index.[19] However, recent developments dimmed the government's commitment to freedom of speech and expression, particularly regarding citizens' use of social media platforms to express their opinions on socio-economic issues. 2025 also saw a ramping up of arrests of citizens, journalists, and opposition leaders for posts online, including those questioning the state or state-linked actors.

In October 2025, authorities arrested Chishimba Kambwili, a former Member of Parliament and outspoken critic of the UPND. He was charged with failure to present himself before an immigration officer before leaving the country for medical treatment.[20] This came days before he was due to be released from prison for a previous conviction of hate speech, for which he was sentenced to five months' imprisonment with hard labour.[21] The state also continued to use, still in effect, sedition laws to charge opposition leaders. In May 2025, Munir Zulu, an independent Member of Parliament, was sentenced to 18 months in prison with hard labour after being found guilty of seditious practices.[22]

Journalists have also been arrested in the course of their public-interest work. For example, in September 2025, a Zambian newspaper, The Mast, condemned the arrest of its journalist, Thandizo Banda, in the Copperbelt province. Banda was on assignment on a story about the murder charge of Maria Zaloumis, the daughter of Mwangala Zaloumis, the chairperson of the Electoral Commission of Zambia. The newspaper alleges that after Banda took pictures of Maria Zaloumis' entourage, he was physically attacked by the latter and police officers, who confiscated his cellphone.[23] In the same month, police services assaulted and seized the cellphone of Christopher Bazilio Banda, a reporter for Prime TV Eastern Province, covering a joint operation between the Road Traffic and Safety Agency and police for the impounding of unregistered motorbikes. The Eastern Province Police Command later apologised for this incident.[24]

Zambia has long been a signatory to the African Platform on Access to Information.[25] In December 2023, President Hakainde Hichilema enacted the long-awaited Access to Information law, and it came into effect in June 2024. However, stakeholders note that while the current law meets acceptable international standards, it still requires further refinement. They lament the placement of responsibility for monitoring compliance with the Act on the government through the Information Ministry, rather than an oversight body like the Human Rights Commission.[26] In August 2025, the government gazetted a Statutory Instrument, The Access to Information (General) Regulations, 2025, to operationalise the Act. It outlines procedures for submitting requests, timelines for responses to requests as well as the documentation required from requesters of the information.[27]

In 2025, the government also introduced the Zambia Institute of Journalism Bill, which aims to impose statutory media regulation through the establishment of the Council of the Zambia Institute of Journalism tasked with the licensing of journalists and regulating conduct

16. Universal Declaration of Human Rights (UDHR), https://www.un.org/en/aboutus/universal-declaration-of-human-rights (accessed on 9 November 2025).
17. African Platform on Access to Information https://www.africanplatform.org/ (accessed on 9 November 2025).
18. African Union Convention on Cyber Security and Personal Data Protection https://au.int/en/treaties/african-union-conven tion-cyber-security-and-personal-data-protection (accessed on 12 November 2025).
19. Freedom On The Net 2025, Zambia, https://freedomhouse.org/country/zambia/freedom-net/2025 (accessed on 2 December 2025)
20. Lusaka Times, 'Kambwili re-arrested Days before expected release' (2025) https://www.lusakatimes.com/2025/10/22/kambwili-re-arrested-days-before-expected-release/ (accessed on 28 October 2025).
21. High Court Upholds Sentence, Sends Kambwili to Prison for Hate Speech' (2025) https://zambianobserver.com/high-court-upholds-sentence-sends-kambwili-to-prison-for-hat-speech/ (accessed on 14 November 2025).
22. 'Munir Zulu Sentenced 18 Months in Jail' (2025) https://zambianobserver.com/munir-zulu-sentenced-18-months-in-jail/ (accessed on 14 November 2025).
23. The Mast, 'Arrest of our journalist unacceptable, regrettable', https://mastmediazm.com/2025/08/arrest-of-our-journalist-unacceptable-regrettable/ (accessed on 2 December 2025)
24. Zambia Reports, 'Police Allegedly Assault Prime Tv Reporter During Combined Operation With Rtsa In Chipata', https://zambiareports.news/2025/09/18/police-allegedly-assault-prime-tv-reporter-during-combined-operation-with-rtsa-in-chipata/ (accessed on 2 December 2025)
25. African Platform on Access to Information available athttps://www.africanplatform.org/ (accessed on 20 November 2025).
26. News Diggers 'Access to Information A Pandora's Box' (2023) https://diggers.news/guest-diggers/2023/12/19/access-to-in formation-bill-a-pandoras-box/ (accessed on 20 November 2025).
27. The Access to Information (General) Regulations, 2025, https://zambialii.org/akn/zm/act/si/2025/56/eng@2025-08-29 (accessed on 20 November 2025).

in the sector.[28] Stakeholders, including journalists and civil society, rejected the bill in its current form, arguing that it risks stifling the media's freedom of speech and its ability to report freely on public-interest stories.

According to Meta's data, between January and June 2025, the platform received eight requests for user data from the government of Zambia: five were legal process requests, and three were emergency disclosure requests. Meanwhile, the state also requested information for nine user accounts. Meta declined all of the requests.[29]

Data Protection and Privacy

The government enacted the Data Protection Act in 2021 and established a Data Protection Office and Commissioner.[30] It also introduced the Cyber Security Act, 2024[31], and the Cyber Crime Act, 2024.[32] These replace the Cyber Security and Cyber Crimes Act No. 2 of 2021, which was repealed in 2024. The Cyber Security Act, 2024, establishes the Zambia Cyber Security Agency and safeguards critical information and its infrastructure, among other objectives. The Cyber Crimes Act, 2024, criminalises unlawful activities associated with computer systems and information and communication technologies, while also ensuring the protection of individuals from cybercrimes and enhancing online safety for children.[33] This is set to be supported by the introduction of the National Child Online Protection Strategy (2025-2029) launched in November 2025. The Strategy clearly sets out actionable goals such as reducing child online abuse by 50% during the period. It also earmarked a $1.8 billion budget for the Strategy.[34]

However, stakeholders are concerned that elements of the cyber legislation give the authorities undue power over citizens' internet use, unjustified access to their private communications, extensive surveillance powers, vaguely defined crimes with highly punitive consequences, and power to suppress freedom of expression and dissent.[35] The laws were enacted with concerns largely left unaddressed.[36] However, the laws are not yet in force, and in 2025, individuals were charged under the Cyber Security and Cyber Crimes Act No. 2 of 2021. In December 2025, Ethel Chisono Edwards, an influencer and vlogger, was sentenced to 18 months in prison after pleading guilty to charges under the Act, for comments she made about President Hichilema.[37]

In March 2025, the Zambian Cabinet approved the Closed-Circuit Television Public Protection Bill No. 1 of 2025. The proposed legislation aims to regulate the use of CCTV systems in public and private spaces. Its stated goals include boosting crime prevention, strengthening community safety, making investigations more effective, and ensuring Zambia keeps pace with regional and global standards.[38] Although these are valid aims, the development of the Bill lacked transparency and sufficient stakeholder engagement to ensure the necessary safeguards, independent oversight, and strict limitations on access to the data, and on the processing, use, and storage thereof by authorities. This raises concerns about the law enabling surveillance of citizens and undue access to their personal data by authorities.

Zambia has not experienced a state-compelled internet shutdown since August 2021, the first of its kind in the country and coinciding with the presidential elections, for a change in power from the then-ruling Patriotic Front (PF), to Hichilema's UPND

28. The Zambian Observer, 'Zambia Institute of Journalism Bill of 2025-End of the Practice of Independent Journalism in Zambia- Amb. Emmanuel Mwamba' (2025) (accessed 20 November 2025).https://zambianobserver.com/zambia-institute-of-journalism-bill-of-2025-end-of-the-practice-of-independent-journalism-in-zambia-amb-emmanuel-mwamba/
29. Meta, 'Government Requests for User Data' https://transparency.meta.com/reports/government-data-requests/country/ZM/ (accessed 20 November 2025).
30. Zambia National Broadcasting Corporation (ZNBC) "Office of the data protection Commissioner coming" (2023) https:// www.znbc.co.zm/news/office-of-the-data-protection-commissioner-coming/ (accessed 15 November 2025).
31. The Cyber Security Act ,2025 https://www.parliament.gov.zm/node/12319
32. The Cyber Crime Act , 2025 https://www.parliament.gov.zm/node/12320.
33. Zambian Monitor, "Zambia's cabinet endorses new cyber security, cyber crimes legislation", (2024),https://www.zambiamonitor.com/zambias-cabinet-endorses-new-cyber-security-cyber-crimes-legislation/#google_vignette, (accessed on 20 November 2025).
34. 'National Child Online Protection Strategy (2025-2029)', Zambia Informationa and Communications Technology Authority, https://www.zicta.zm/media/publications (accessed on 1 January 2026)
35. News Diggers 'Govt Defers Cyber Security and Cyber Crime Bills' (2024) https://diggers.news/local/2024/12/06/laz-media-owners-other-csos-reject-enactment-of-cyber-laws/ (accessed on 13 November 2025).
36. Zambia's cybersecurity and cybercrimes laws raise digital rights concerns (2025) https://www.africafex.org/country-highlights/zambias-cybersecurity-athe surveillance of citizens and the authorities' undue access to their personal datand-cybercrimes-laws-raise-digital-rights-concerns#:~:text=In%20April%202025%2C%20the%20Zambian%20Parliament%20enacted%20two,digital%20rights%20and%20civil%20liberties%20in%20the%20country (accessed on 1 December 2025).
37. Zambian-American influencer sentenced to 18 months for hate speech (2025) https://www.bbc.com/news/articles/cvgqnklqge7o (accessed on 14 November 2025).
38. Press Reader, 'Cabinet approves Closed-Circuit Television Public Protection Bill 2025' (2025) https://www.pressreader.com/zambia/zambia-daily-mail-798j/20250312/281535116758974 (accessed on 14 November 2025).

party.[39] The upcoming elections will also be a test of the government's commitment to upholding rights to consistent connectivity despite a tense election period, with flare-ups of political violence already being reported.[40]

Meanwhile, cybercrime continues to threaten Zambia's security, economy, and population. Zambia achieved a score of 92.56 on the International Telecommunications Union's Global Cybersecurity Index.[41] However, it continues to face vulnerabilities and cyber threats. Cyber-related crimes between January 1 and June 30 2025, resulted in a loss of over ZMW111 million (US$5.86 million).[42] The Zambia Police Service also recorded 874 cyber-related cases in the period. In March 2025, Interpol announced that combined efforts from authorities in seven African countries, including Zambia, had resulted in the arrest of 306 suspects and the seizure of 1,842 devices. [43]

AI and Emerging Technologies

The government of Zambia is currently implementing its National Artificial Intelligence Strategy (2024-2026).[44] Only a small group of African countries have a dedicated artificial intelligence (AI) strategy, including Benin, Egypt, Mauritius, Morocco, and Senegal, among others.[45] The strategy comprises five focus areas: (i) Digital Trees to enhance connectivity, (ii) Reliable Data for efficiency and sustainability, (iii) Trust and Confidence to safeguard cyberspace, (iv) fostering innovation and entrepreneurship, and (v) creating partnerships. [46]

Implementation has been slow; however, positive developments include the partnership between the Ministry of Technology and Science, Ministry of Health, 73 Health Global and Pentatech, to implement a nationwide pilot testing remote health diagnostics and AI-based pharmacological analysis tools across the country.[47]

Digital Inclusion

Zambia's mobile market continues to grapple with quality of service (QoS) issues. In 2025, Operators' QoS deteriorated, with access to connectivity becoming even more challenging for those outside of the country's urban centres. In November 2025, the industry regulator noted that "the Zambian people deserve better", setting out instructions for providers to improve services.[48]

Zambia's acute electricity shortages, which began in 2024,[49] persisted in 2025, dampening digital inclusion efforts. The Zambia Electricity Supply Corporation Limited experienced periods when it could supply only three hours of power daily.[50] Operators lamented the high rollout costs for network infrastructure and the services they maintain due to this. They noted further impediments from high taxes, higher fuel prices to power generators, and a low smartphone penetration rate, weighing on the adoption of broadband services.[51] Thus, consumers have borne the brunt, struggling to remain connected.

39. The Verge 'WhatsApp, Twitter, and Facebook are reportedly blocked in Zambia during its presidential election' (2021)https://www.theverge.com/2021/8/12/22621875/whatsapp-twitter-facebook-blocked-zambia-presidential-election (accessed on 22 November 2025).
40. CAJ News, 'Concern over Zambia pre-election violence' https://cajnewsafrica.com/2025/09/08/concern-over-zambia-pre-election-violence/ (accessed on 2 December 2025)
41. International Telecommunications Union, Global Cybersecurity Index, (2025) https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
42. 'Press Reader,Over K111m lost to cyberrelated crimes since Jan' https://www.pressreader.com/zambia/zambia-daily-mail-798j/20250710/281582361644535 (accessed on 22 November 2025).
43. 'More than 300 arrests as African countries clamp down on cyber threats' (2025) https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats
44. Government of Zambia, 'Artificial Intelligence strategy launched, a stepping stone to wealth and job creation' https://www.mots.gov.zm/?p=4492 (accessed on 10 November 2025).
45. M Musoni, "Envisioning Africa's AI governance landscape in 2024" (2024) https://ecdpm.org/work/envisioning-africas-ai-governance-landscape-2024#:~:text=Currently%2C%20less%20than%2010%20African%20countries%20have%20national,Egypt%2C%20Morocco%2C%20Mauritius%2C%20Tunisia%2C%20Sierra%20Leone%2C%20and%20Senegal. (accessed on 4 November 2025).
46. Zambia Monitor 'Zambia launches artificial intelligence strategy to boost digital economy' (2024)https://www.zambiamonitor.com/zambia-launches-artificial-intelligence-strategy-to-boost-digital-economy/#google_vignette (accessed on 22 November 2025).
47. 'Zambia Deploys AI and Remote Diagnostics in 20 Facilities to Drive Nationwide Health Access', (2025), https://techafricanews.com/2025/06/16/zambia-deploys-ai-and-remote-diagnostics-in-20-facilities-to-drive-nationwide-health-access/ (accessed on 10 November 2025).
48. ZICTA 'Press Statement By ZICTA Director General, Eng. Collins Mbulo On The State Of Mobile Telecommunications Quality Of Service And Zicta's Interventions' (2025) https://www.zicta.zm:992/storage/uploads/zictaweb/a5ae4b64-a054-4d4e-90b3-ff8e54d584cd_1762324884.pdf (accessed on 3 December 2025)
49. International Growth Centre 'Lights out: Zambia's electricity crisis' (2024) https://www.theigc.org/blogs/lights-out-zambias-electricity-crisis#:~:text=Low%20water-levels%20at%20the%20main%20reservoirs%20for%20hydroelectric,businesses%20unprepared%20and%20without%20back-up%20sources%20of%20energy. (accessed on 10 November 2026)
50. Lusaka Times 'ZESCO Assures Minimum 3-Hour Power Supply Amidst Low Generation Capacity'https://www.lusakatimes.com/2025/11/06/zesco-assures-minimum-3-hour-power-supply-amidst-low-generation-capacity/ (accessed on 18 November 2025)
51. ZICTA 'Annual Market Report for the ICT Sector' (2024) chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://zicta.zm/market-reports/2024_annual_market_report.pdf https://www.zicta.zm/market-reports/2023_mid_year_market_report.pdf (accessed on 3 October 2025)

Since licensing SpaceX's Starlink in June 2023, the government has leveraged satellite technology to connect unserved and underserved areas. The SMART Zambia Institute is deploying Starlink to government institutions and public facilities.[52] Notably, in September 2025, the Institute deployed kits in one of Zambia's most remote areas, the Moomba Chiefdom, connecting a clinic and primary schools.[53]

The Ministry of Finance's 2026 Budget commits to constructing communications towers in underserved areas. The government also continued to roll out the Government Wide Area Network (GWAN) to public institutions. So far, 93 local authorities, 79 district administration offices and 29 schools have been connected to the GWAN, for a total of 438 sites. Additionally, to protect the installed equipment from power outages, the Government has installed solar energy in all 116 councils.[54]

The government has also strongly focused on boosting investment in ICT infrastructure. In September 2025, it announced a $120 million World Bank grant to increase internet access and digital services for the population. It is planned to extend 4G and 5G networks to cover 90% of the population by the end of 2025.[55] In November 2025, the government and the United Nations Development Programme partnered to provide internet access to 751 Zambian health facilities. This is part of the Smart Health Systems project, focused on modernising Zambia's digital health infrastructure.[56]

Digital IDs

In 2022, the government introduced the Integrated National Registration Information System project, a digital biometric national identity management system. The government pledged to register 100% of the population over 16 years old for digital ID cards within six months of rollout.[57] However, uptake has fallen significantly short, with a 2024 report by the UNDP noting 1.5 million have enrolled with biometric data.[58] In January 2025, SMART Zambia issued a general procurement notice for digital ID and trust services. It aims to develop a framework to identify citizens and enable access to public and private-sector services.[59] The government also partnered with Ethiopia, a regional leader in biometric ID adoption, to collaborate on the development and implementation of national ID systems.[60]

Universal Access and Service Fund

The Zambia Information and Communications Technology Authority (ZICTA) administers the country's Universal Access and Service Fund (UASF). It has been consistent in collecting the UASF, 1.5% of operator revenues. The governance and administration of the Fund have improved over the years through institutional reforms. While the Fund alone may not be sufficient to meet the country's ICT deficits, its overall impact is evident.

ZICTA's 2023 annual report, the latest available, notes that nearly half of the 58 new tower installations in 2024 were deployed in underserved areas. In 2023, the UASF utilised the fund to provide 845 computers, 25 printers, five smartboards, and 21 projectors to 25 institutions nationwide. The regulator began a project to connect 15 tertiary institutions to the internet. The aim was to provide low-cost broadband services to educational institutions nationwide, connecting 63 learning institutions. The UASF also provided customised ICT equipment for persons with disabilities; introduced connectivity and provided ICT equipment; and developed an e-learning platform. The con

52. SMART Zambia Institute https://www.szi.gov.zm/?p=5312
53. 'Smart Zambia Brings Starlink Internet to Remote Moomba Chiefdom' (2025) https://techafricanews.com/2025/09/29/smart-zambia-brings-starlink-internet-to-remote-moomba-chiefdom/ (accessed on 2 December 2025)
54. Government of Zambia, '2025 Budget Speech' (2024) https://www.zra.org.zm/wp-content/uploads/2025/09/2026-Budget-Speech.pdf (accessed on 30 October 2025).
55. TechAfrica News 'World Bank Grants Zambia $120M to Expand Digital Infrastructure'https://techafricanews.com/2025/09/19/world-bank-grants-zambia-120m-to-expand-digital-infrastructure/(accessed on 18 October 2025).
56. Ecofin Agency, 'Zambia, UNDP To Expand Internet Access Across 751 Health Facilities' Zambia, UNDP To Expand Internet Access Across 751 Health Facilities - Ecofin Agency (accessed on 2 December 2025).
57. Presidential Delivery Unit, 'Digital ID' (2025) https://www.pdu.gov.zm/digital-ids
58. UNDP, 'DPI Safeguards Come Online In Zambia's Next Phase of Digital Integration' (2024) https://www.undp.org/digital/blog/dpi-safeguards-come-online-zambias-next-phase-digital-integration (accessed on 12 November 2026).
59. Biometric Update 'Zambia issues general procurement notice for digital ID, trust services project' (2025) https://www.biometricupdate.com/202501/zambia-issues-general-procurement-notice-for-digital-id-trust-services-project (accessed on 12 November 2026).
60. 'Zambia, Ethiopia sign MoU to advance digital identity systems' (2025) https://apanews.net/zambia-ethiopia-sign-mou-to-advance-digital-identity-systems/ (accessed on 12 November 2026).

struction of 31 communication towers under the Communication Towers Program also began.[61]

Conclusion

It is positive that despite significant operational and financial constraints faced by telecommunications operators, the uptake of telecommunications services continued. This report also lauds the positive strides taken toward operationalising the country's AI strategy. If the country continues on this trajectory, it will be well-placed to build an integrated, accelerated ICT ecosystem that promotes meaningful accessibility, innovation, entrepreneurship, and an inclusive, resilient digital economy. However, certain steps taken by the government continue to raise concerns about the State's commitment to human rights principles, particularly freedom of speech. The enactment of the cyber legislation despite the reservations of stakeholders, as well as heightened arrests of journalists, civil rights defenders, and opposition leaders, is worrying, particularly as the country approaches general elections in 2026. Considering the gaps and concerns raised in this report, various recommendations are proposed to stakeholders.

Recommendations

The Government should:

- To ensure transparency in the operationalisation of the cyber legislation, conduct public sensitisation, and commit to preventing abuses of power, which the laws are vulnerable to in their current state.
- As the country heads to a general election in August 2026, the government is encouraged to commit to not shutting down the internet during the electoral process and after.
- It is commendable that the government has repealed the law regarding criminal defamation of the president. However, it is urged to take greater steps to uphold freedom of speech and repeal laws such as sedition and hate speech.
- Adopt greater transparency and regular reporting around the use of UASF and the progress.
- Bolster the Data Protection Commission's capacity and raise awareness of data protection among the private sector and citizens, in light of the rollout of digital IDs and public security information systems.
- Commit to the collection of data and digital ID systems in an ethical and non-discriminatory manner, without perpetuating surveillance practices. Also, ensure adequate public sensitisation on the risks and opportunities of the process.
- More needs to be done to promote public participation in AI adoption, uphold ethics and enhance transparency and safety in AI use. We encourage greater collaboration among Ministries and other stakeholders to ensure the AI Strategy is implemented in a rights-respecting manner.

1. ZICTA, "ICT Sector 2024 Mid-Year Market Report", (2024) (accessed on 12 November 2026).In light of

The private sector should:

- Telecommunications companies should commit to maintaining connectivity and access to digital platforms during the upcoming general elections.
- Engage with stakeholders, such as civil society, to ensure alignment of policies, practices, and the deployment of digital technologies and products with rights-respecting principles and standards.
- Play an active role in digital literacy efforts to educate and sensitise citizens about technology developments and deployments in the country, to ensure equitable digital inclusion and benefit from

Civil Society Organisations should:

- Increase focus on programmes to build the capacity of government, judiciary and state security institutions, especially as it relates to the impact of and use of emerging technologies such as AI and cyber legislation.
- Collaborate more to prevent bottlenecks and duplication of efforts.
- Continue to raise awareness of digital rights and digital inclusion in Zambia.

The Media should:

- Contribute to monitoring and documenting developments in digital rights and inclusion in Zambia through in-depth investigative pieces.
- Closely collaborate with civil society organisations to amplify messaging around issues of journalist rights and public interest issues.

The Score Index

Zambia, 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)	5	5	Except for a single instance in 2021, internet shutdowns have not been the norm in Zambia. 2025 recorded no internet shutdowns.
Laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	4	3	Zambia's eighth National Development Plan prioritises connectivity for all citizens. This is also a Universal Access and Service Fund law. ZICTA sets annual targets for its use. There remains a significant challenge around transparency about the total funds allocated and spent each year, how well the targets are being met, and regular, traceable reporting back to the public.
False News Criminalisation	P22(2)	3	3	Zambia saw an increase in arrests for social media posts deemed false news.
Sedition Legislation	P22(2)	2	2	Increased reliance on sedition charges, particularly targeting opposition leaders.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	2	2	Increased arrests and assaults, mainly of journalists reporting on government and governance issues.
Data Protection Legislation.	P42	4	4	Data Protection legislation has been enacted. Implementation and enforcement have been weak, and the independence of the data protection commissioner from the president's office is in question; they are appointed by the President.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	4	4	No instances reported in 2025; however, requests for information were made to social media platforms.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Invasion of Privacy of	P41	3	2	Not reported in 2025. However, the passing of the country's new cyber legislation may enable this.
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	4	3	Access to Information legislation exists, and the government is relatively proactive through digital inclusion exercises and roadshows. However, it has not been as proactive in providing information about emerging technology adoption.
AI and Emerging Technologies national strategies	P39(6)	4	3	AI Strategy and a National Digital Transformation Strategy exist. However, implementation has been relatively weak.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	2	3	No specific child online safety law exists, but there is a National Child Online Protection Strategy, and the cyber legislation focuses on child protection.
Digital Inclusion	P37(3)	3	3	A progressive rise in mobile and internet usage is evident in active investment to expand access. However, Quality of Service issues persisted in 2025.

Total (out of 60):	2024: **40**	2025 **39**

ZIMBABWE

By Mohamed Farahat

Executive Summary

This report highlights internet accessibility in Zimbabwe and assesses the regulatory landscape, providing information on available legislation related to internet access, data protection, freedom of expression, access to information, privacy and digital inclusion. The report provides recommendations to safeguard human rights by improving policies and practices in line with the African Commission on Human and Peoples' Rights' Declaration on Freedom of Expression and Access to Information (the Declaration). The country assessment involved a comprehensive desk review of relevant documents, including country reports, legislation and media reports. The report relied on Paradigm Initiative's TheScore Index to assess the country's compliance with the Declaration. The report analyses the Universal Service Fund (USF) initiatives, including allocations and implementation gaps. In 2025, there was no internet shutdown in Zimbabwe, demonstrating compliance with Principle 38(2) of the Declaration, unlike in 2023, when the nternet was shut down on the eve of the elections. Zimbabwe's overall score on TheScore Index is 34. The country achieved a moderate score in terms of compliance with the Declaration, as challenges remain in the arbitrary arrests of human rights defenders and journalists against Principle 20 (1) & (2) of the Declaration. Infringement on freedom of expression through the existence and application of sedition legislation and the criminalisation of false news remains a major threat to the realisation of the provisions of Principle 22 (2). Technology-Facilitated Gender-Based Violence (TFGBV) also features in the report, limiting opportunities for free expression online and contravening the tenets set out in the ACHPR Resolution 522.



Introduction

Zimbabwe is situated in the Southern African region and has a population of 15,178,957.[1] Human rights are guaranteed by the Constitution of Zimbabwe Amendment (No. 20) Act, 2013 (the Constitution); however, despite robust constitutional protections, there is a glaring gap between constitutional guarantees and practice.

Since 2016, Zimbabwe has adopted several laws, including those that criminalise online expression, such as the contested[2] Criminal Law (Codification and Reform) Act, No 10 of 2023[3] commonly known as the Patriotic Act, which in Chapter 3, Section 31 (a and b) makes it an offense to publish or communicate a statement that is wholly or materially false with the intent to undermine public confidence in law enforcement agencies or the state. Violators can face penalties of up to 20 years in prison for such offences. The overly broad provisions threaten freedom of expression and silence dissenting voices. The Interception of Communications Act of 2007[4] remains a key legal tool for government surveillance, requiring telecommunications providers in Chapter 3, Section 9 (1 and 2), to facilitate the interception and storage of communications and enabling real-time monitoring of online activities. The Act undermines Principle 41 of the Declaration, which emphasises the need for adequate safeguards in upholding the right to privacy, including prior authorisation by an independent and impartial judicial authority.

Although Zimbabwe is a signatory, it is among the 39 African countries that have not ratified the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), hindering the vision of a unified digital ecosystem in Africa. In 2021, Zimbabwe enacted the Cyber and Data Protection Act, which provides basic safeguards for personal data. The Criminal Law (Codification and Reform) Act was updated to cover electronic offences, such as cyberbullying, harassment and the transmission of information deemed 'false' by authorities, expanding state control and stifling free expression. To comply with the Declaration and international best practices, Zimbabwe needs to ensure improved access to information across government ministries and departments and desist from arbitrary arrests of the media. Zimbabwe has not revised its traditional gender-based violence policies to address online gender-based violence, despite a regional call for states to align with Resolution 522.

Internet Access and Disruptions

Guiding Policy

Zimbabwe launched the National ICT Policy (2022-2027), the National Broadband Plan (2023-2030), and the Smart Zimbabwe 2030 Master Plan in 2024 to accelerate digital transformation. Zimbabwe adopted a National Development Strategy (NDS1) in 2021, which sought to use ICT to improve the country's digital economy and entrench ICTs across all national development strategies to achieve universal access by 2030. The government set targets to increase internet penetration from 59.1% in 2020 to 75.4% by 2025 and to increase mobile penetration from 94.2% to 100% by 2025. NDS1 lapsed in 2025, and the government is in the process of formulating NDS2, with Parliament discussions already underway.[5] NDS 2 will cover the period 2026-2030, and one of the key pillars will focus on Science, Technology, Innovation, Digitalisation and Human Capital Development.

1. Zimbabwe National Statistics Agency (ZIMSTAT) 'Zimbabwe 2022 Housing and Cenus Report' https://www.zimstat.co.zw/wp-content/uploads/Demography/Census/2022_PHC_Report_27012023_Final. pdf (Accessed 27 October 2024).
2. Robert and Ethel Kennedy Human Rights Centre. Repeal the Patriotic Act to respect fundamental human rights https://rfkhumanrights.org/our-voices/zimbabwe-repeal-the-patriotic-act-to-respect-fundamental-human-rights/ (Accessed 15 November 2026)
3. Veritas https://www.veritaszim.net/sites/veritas_d/files/Crimcode%20%28updated%20to%202023.09%29.pdf (Accessed 17 November 2025)
4. Judicial Services Commission https://jsc.org.zw:8222/media/upload/Acts/2014/1120done.poffencesdf (Accessed 19 November 2025)
5. https://www.parlzim.gov.zw/download/national-assembly-hansard-11-november-2025-vol-52-no-2/ (Accessed 9 November 2025)

Government data shows that the internet penetration rate stood at 70.1% in 2023, 83.52%[6] in 2024 and dropped to 81.83%[7] at the end of the second quarter of 2025, reflecting a marginal dip in active internet or data subscriptions on a year-on-year basis. Despite the negative dip, the data depicts a positive progress towards achieving meaningful access. However, independent data shows that the internet penetration rate stood at 34.8%[8] in 2023, dropped to 32.6 %[9] in 2024 and rose to 38.4% in 2025[10]. Independent research data shows that Zimbabwe is far from reaching the goals set out in the NDS1. Figures from POTRAZ assess internet penetration relative to existing mobile penetration figures, while independent researchers assess internet penetration relative to the total population, making the independent researchers' figures an accurate representation of internet connectivity/access in Zimbabwe. Subscribers of Econet - a telecommunications service provider - spend US$1 for 1200 megabytes of data that lasts for one hour and US$3 for 650mb of data that lasts for 24hours.[11] For low-income users in Zimbabwe, who live on less than US$1.63 per day[12] (the minimum amount needed per day for individuals to not be deemed poor), meaningful access to the Internet is far from reach. Mobile network internet speed in Zimbabwe is 33Mbps.[13] Recommended internet speeds should be at least 100 Mbps for download and 10 Mbps for upload. The internet speed for Starlink is 51 Mbps.

Internet Disruptions

In the year under review, Zimbabwe did not experience a government-imposed internet shutdown. As a result of this development, Zimbabwe scored five points in 2025 under indicator 1 on internet shutdowns, depicting full compliance with Principle 38(2), which calls on states not to disrupt the internet. This demonstrates progress compared to 2023, when Zimbabwe experienced an internet disruption on the eve of the August 2023[14] harmonised elections.

In 2025, Zimbabwe implemented key reforms to enhance online freedom of expression. Zimbabwe passed the Broadcast Services Amendment Act, Act No. 2 of 2025, on May 23 2025. The Act amends the 2001 Broadcasting Services Act to include digital-age reforms, such as internet-based broadcasting. Zimbabwe also adopted a Media Policy[15]. The policy introduces co-regulation, an important aspect for a thriving media. In practice, state influence remains dominant as the state exerts control through restrictive laws and appointments. For example, while it is a Chapter 12 independent constitutional body, the Zimbabwe Media Commission's eight commissioners are appointed by the President from a list of 12 nominees provided (after an interview process) by the Committee on Standing Rules and Orders, which can lead to executive influence. Judicial and parliamentary oversight should be embedded in Zimbabwe's policy-making processes.

Online Freedom of Expression and Access to Information

The Media Policy in Section 4.8 on penalties and disincentives highlights that, while co-regulation exists, media organisations and journalists can still face civil lawsuits for defamation, privacy violations and the spread of falsehoods. This goes against Principle 22 (2) of the Declaration, as the policy further strengthens criminalisation of false news. The pen

6. TechZim 'Second Quarter Abridged Sector Performance Report' (2024) https://www.potraz.gov.zw/wp-content/uploads/2025/02/Third-Quarter-2024-Abridged-Sector-Performance-Report-Hmed-final.pdf (Accessed (Accessed 10 February 2025).
7. Postal and Telecommunications Authority of Zimbabwe https://www.potraz.gov.zw/wp-content/uploads/2025/09/2025-2nd-Quarter-Abridged-Sector-Performance-report-HM-final-ed.pdf (Accessed 10 November 2025)
8. Paradigm Initiative 'Zimbabwe Country Report' (2023) https://paradigmhq.org/wp-content/uploads/2024/06/Zimbabwe-Country-Report.pdf (Accessed 30 October 2024).
9. Data Reportal 'Digital 2024-Zimbabwe' (2024) https://datareportal.com/reports/digital-2024-zimbabwe?rq=zimbabwe (Accessed 30 October 2024).
10. https://datareportal.com/reports/digital-2025-zimbabwe (Accessed 12 November 2025)
11. Econet 'USD data Bundles' https://www.econet.co.zw/usd-data-bundles/ (Accessed 13 November 2025)
12. Zimstat 'Poverty Datum Line 2025' https://www.zimstat.co.zw/wp-content/uploads/Macro/Prices/PDL/2025/Poverty%20Datum%20Lines%20Front_%20Mar_%202025.pdf (Accessed on January 28, 2026)
13. Fast. https://fast.com/ (Accessed 12 November 2025process)
14. NetBlocks https://x.com/netblocks/status/1693997476691558644?s=20 (accessed 17 February 2026)
15. Veritas Zim 'Media Policy' https://www.veritaszim.net/sites/veritas_d/files/Media%20Policy%202025.pdf (Accessed 11 November 2025)

found guilty, Zaba could face a fine of up to US$300, imprisonment for up to a year, or both. Zaba was granted bail on July 4 2025. The application of sedition legislation remains a challenge in the Zimbabwe policy landscape, and such arrests limit free expression online and foster an atmosphere of self-censorship, directly impacting the achievement of Principles 20 (1) and (2).

The landscape in Zimbabwe is characterised by a tension between constitutional protections for free speech and the crackdown on dissent. Media freedom, protected in Section 61 of the Constitution, was under attack in the period under review. On February 24 2025, a senior journalist with Alpha Media Holdings and Head of News at HStv Blessed Mhlanga was detained by authorities after interviewing war veteran and ZANU-PF central committee member Blessed Geza, an outspoken critic of President Emmerson Mnangagwa's leadership. Mhlanga was charged with "transmitting data messages that incite violence or damage to property." On March 12, Mhlanga's case was postponed in the Zimbabwe High Court, and his bail application was denied. Justice Gibson Mandaza stated that more time was needed to review the case. On May 7, Mhlanga was granted provisional release[20] after 72 days.

Access to Information

Zimbabwe enacted the Freedom of Information Act in 2020 to repeal the Access to Information and Protection of Privacy Act (AIPPA) and empower interested stakeholders to have full and justified access to information. Under Article 5 of the Act, public and public commercial entities should have information disclosure policies and disclose information in the interests of public accountability or information that is required for the exercise or protection of a right. However, some entities are not compliant with the Act.[21]

16. Amnesty International https://www.amnesty.org/en/documents/afr46/9385/2025/en/ (Accessed January 14 2026)
17. Newsday 'Government institutions violating freedom of information act' (2024) https://www.newsday.co.zw/the-standard/news/article/200031734/govt-institutions-violating-freedom-of-information-act (Accessed 2 November 2024).

Entities such as POTRAZ do not have up-to-date information on their website to reflect work done in the year. In 2024, the Section on the Universal Service Fund included information on the first, second and third phases of the USF, dating as far back as May 2013. As of 2025, this information remains unchanged. In this section, no other information is available. In addition, in the fourth quarter of the year, the only sector performance report available on the website was the second-quarter report. POTRAZ shares some updates on social media platforms. While this is not a representative sample, there is a general trend amongst government websites to not display full information despite the comprehensive website guidelines that are in existence.[22] In this regard, Zimbabwe is mildly compliant with principle 29 (3) as government websites often carry outdated information.

Censorship and Content Removal

In 2025, no content removal cases were recorded. However, Meta and TikTok's 2024 transparency reports indicate that the government requested one content takedown. Reports for 2025 indicate that no cases[23] of content takedowns were recorded by social media platforms.

Data Protection and Privacy

Data protection and governance

Zimbabwe enacted the Cyber and Data Protection Act, 2021 (CDPA)[24] but has not ratified the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). The CDPA establishes baseline protections for personal information. In Part II, Section 6(2), the CDPA asserts the independence of the Postal and Telecommunications Regulatory Authority (POTRAZ) from "control by government or by political means." The Data Protection Authority is the Postal

18. Veritas https://veritaszim.net/sites/veritas_d/files/Final_Draft_Zimbabwe_Govt_Web_Guidelines_3_April_2018.pdf (Accessed 16 November 2025)
19. https://transparency.meta.com/reports/government-data-requests/country/SD/&sa=D&source=docs&ust=1771768464868635&usg=AOvVaw3AcPAdSA4tqWEbMYxNICQF

and Telecommunications Regulatory Authority of Zimbabwe, established under section 5 of the Postal and Telecommunications Act [Chapter 12:05]. Under Part III, Section 6 of the Postal and Telecommunications Act, Chapter 12:05, the President of Zimbabwe has the authority to appoint the Board that governs POTRAZ. POTRAZ is also structurally linked to the Ministry of ICT, Postal and Courier Services, adding to the challenges to the DPA's independence and presenting a potential conflict of interest when data breaches involve state-owned entities. POTRAZ's dual role affects compliance with Principle 42 (8), which calls for oversight mechanisms to be independent entities.

In a move that operationalises the CDPA, Zimbabwe gazetted the Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations (the Regulations), which came into effect on September 13 2024. The regulations impose a mandatory registration requirement on entities that process personal information, based on three tiers and the appointment of a Data Protection Officer to oversee Data Controllers' compliance with the Data Protection Act. The regulations outline breach notification expectations, compelling data controllers to notify the Data Protection Authority of any data breaches within 24 hours and requiring only that affected individuals be informed within 72 hours if there is a high risk to their rights. This poses a risk of harm to data subjects if a data breach remains unresolved within 72 hours, delaying transparency by data controllers. Zimbabwe should consider adopting best practices from South Africa's Protection of Personal Information Act Section 22(1, 2 and 3) and Section 49(3) of Zambia's Data Protection Act, which mandate notifying data subjects as soon as reasonably possible, in case of a breach. The gazetting of the regulations marks a significant step forward in Zimbabwe's implementation of the CDPA. However, effective enforcement is yet to be realised.

In alignment with the CDPA, following the launch[25] of the Data Protection Officer Training programme on June 6 2025, a total of 570 data controllers, including law firms, doctors' practices, health centres, municipalities, schools, churches, small and medium enterprises, corporations and parastatals received certificates. POTRAZ reported that so far, 560 DPOs have been trained and 45 data breach reports have been received and addressed by the authority.[26] Zimbabwe established a new data centre and upgraded the National Data Centre to Tier IV standards, aiming for 99.99% uptime for government digital systems. So far, it has installed an AI-powered disaster recovery infrastructure, including servers, routers and storage. A clear governance gap exists in Zimbabwe as it has not yet enacted an AI Policy, despite AI initiatives already underway.

Cybersecurity measures

On October 27 2025, Zimbabwe signed the United Nations Convention against Cybercrime Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, (Hanoi Convention), joining more than 60 countries in a landmark commitment to strengthen international cooperation against cyber threats. Zimbabwe's statement focused on aligning national legislation with global standards and building capacity within law enforcement and justice institutions to effectively implement the Convention. The signing of the Convention reflects alignment with Principle 42, which calls on states to adopt legal frameworks on the protection of personal information in accordance with international standards.

Online Gender-Based Violence

Zimbabwe is a signatory to the Beijing Declaration and Platform for Action 1995, the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW) 1991, Protocol to the African Charter on Human and People's Rights on the Rights of Women in 2007 and the SADC Protocol on Gender and Development 2009, all of which call on states to eliminate gender-based violence. The Cyber and Data Protection Act (2021) complements the aforementioned laws by

20. Postal and Te;lecommunications Regulatpry Authority of Zimbabwe ' Data Protection Act' https://www.potraz.gov.zw/wp-content/uploads/2022/02/Data-state-owned,state-ownedProtection-Act-5-of-2021.pdf (Accessed 11 November 2024).

21. Harare Instituite of Technology 'HIT enters intpo agreement with POTRAZ' https://www.hit.ac.zw/2023/11/09/hit-enters-into-agreement-with-potraz/ (Accessed 10 November 2024).
22. Postal, Telecommunications and Regulatory Authority of Zimbabwe https://www.potraz.gov.zw/?p=3120 (Accessed 15 November 2025)

being the country's first law to criminalise online violence. Zimbabwe has existing laws such as the Domestic Violence Act,[27] whose scope is more focused on "domestic" violence, with limited mentions of addressing harassment that happens through sending and delivering messages through electronic mail. Despite the adoption of Resolution 522, which aims to address digital violence against women by the African Commission on Human and Peoples' Rights (ACHPR) in 2022, TFGBV persists. A report[28] by Gender and Media Connect found that 63% of surveyed women journalists experienced TFGBV, with 436 incidents reported by 88 journalists. Hate speech was one of the most common violations, reported by 30%, along with misinformation and defamation and cyber harassment, reported at 18% and 16%, respectively, among other threats. While the resolution requires states to review or adopt laws that combat all forms of digital violence and expand the definition of gender-based violence to include digital violence against women, Zimbabwe has not yet updated its policies to effectively address TFGBV. Given the above, gaps remain as TFGBV persists with low engagement with formal reporting channels by survivors[29] and laws such as the Domestic Violence Act require reform as they have a limited scope of addressing OGBV. Given the above, Zimbabwe is moderately compliant with the Declaration, as it has an existing CDPA, regulations, and has signed the Hanoi Convention on cybersecurity. However, TGFBV persists, and some laws still require refor

Privacy and Surveillance

The CDPA established the Cyber Security and Monitoring of Interceptions of Communications Centre as a unit in the Office of the President. The guiding policy undermines the centre's independence. The Centre is housed in the Office of the President and suggests a potential to target vulnerable groups, including activists, opposition actors and journalists, through targeted surveillance. This is problematic as it is likely to infringe on the rights to free expression and result in both state censorship and self-censorship. Section 6 of the Interception of Communication Act Section 6 (a,b and c) mandates the Minister to issue a warrant to authorised persons if there are reasonable grounds for the Minister to believe that the gathering of information concerning an actual threat to national security or to any compelling national economic interest is necessary or the gathering of information concerning a potential threat to public safety or national security is necessary. The above provisions are overly broad and expose individuals to the invasion of their private communications. The provisions give the Minister excessive power to issue warrants without judicial or parliamentary oversight. This could lead to targeted surveillance of journalists and activists. This directly affects compliance with Principle 41 as policies introduced to address national security weaken the protection of private communications, thereby opening the door for arbitrary interference.

In March 2025, 95 demonstrators were arrested and charged with promoting "public violence" and disrupting peace.[30] Some protesters were identified through social media and WhatsApp, raising concerns about surveillance of protesters, monitoring of social media and the use of technology in policing. Such policing initiatives restrict free expression online, leading to self-censorship and heightened fear of participating in online discussions, thereby undermining digital democracy.

Digital IDs and Smart City Developments

In 2024, the Department of Immigration introduced an Online Border Management System (OBMS) that utilises fingerprint and iris recognition technology to facilitate automated self-service immi

23. Veritas 'https://www.veritaszim.net/node/146 (Accessed 12 November 2024).
24. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000395151 (Accessed 12 February 2026)
25. Paradigm Initiative. Click That Hurt. https://paradigmhq.org/wp-content/uploads/2025/12/Clicks-That-Hurt-Report.pdf?x72143 (Accessed 17 February 2026)
26. BBC https://www.bbc.com/news/articles/czx4g9ejjj9o (Accessed 20 November 2025)

gration clearance and verify travellers' identities against a national immigration database.[31] However, there has been no deliberate effort to unpack how individuals' data will be used, stored, and shared to prevent its misuse. The Senate Hansard highlights that the Ministry of Home Affairs is working towards digital IDs and digital birth certificates.[32] There is currently no record of the government conducting data protection impact assessments to identify potential risks and biases emanating from the use of the OBMS and implementation of any Digital ID programmes. In May 2025, Zimbabwe also introduced online applications for e-visas, resident and work permits and electronic travel clearances.[33] Without impact assessments, the capabilities of digital ID and biometric systems to capture detailed data on individuals' activities and behaviours raise surveillance concerns and may infringe the right to privacy. The Government of Zimbabwe should conduct privacy impact assessments before implementing any biometric technologies. These assessments will determine how each technology affects privacy rights and other fundamental freedoms.

AI and Emerging Technologies

Since 2024, the Zimbabwean government has been developing a national artificial intelligence (AI) strategy to regulate the use of AI and related technologies across various sectors. The Minister of Information Communication Technology, Postal and Courier Services, Tatenda Mavetera[34] highlighted this initiative. The policy aims to create a governance framework that ensures ethical use, security, and the promotion of IoT and AI technologies in the country. Zimbabwe approved[35] the National AI Strategy in October 2025; however, as of the time of writing (December 2025), the strategy was not yet publicly available via government websites, although a copy shared during public consultations was circulating. The strategy, seen by PIN, mentions human rights, ethics and human-centred AI, referenced as Ubuntu AI, providing a strong anchor for the AI strategy. The strategy also mentions grievance and redress mechanisms, as well as risk management and mitigation strategies, which are key to safeguarding human rights. However, the strategy falls short because it fails to draw clear red lines, which are necessary to prevent universally unacceptable risks.

In 2025, UNESCO published an Artificial Intelligence Readiness Assessment Report for Zimbabwe[36], which recommended that the multidisciplinary AI Ethics Think Tank, established in February 2025, oversee the implementation of the UNESCO Recommendation on the Ethics of AI. The think tank will develop and enforce ethical guidelines to ensure AI deployment aligns with Zimbabwe's priorities and create procedures for ongoing participation and engagement from key stakeholders.

Zimbabwe is mildly compliant with the Declaration as it currently provides for automated decision-making in the CDPA. However, this does not amount to a comprehensive AI governance framework. As of December 2025, Zimbabwe's national AI Policy or strategy was not yet available despite public announcements that it was now in its final stages.

Digital Inclusion of persons with disabilities

Zimbabwe gazetted the Persons with Disabilities Bill (The Bill)[37] on February 9 2024, and the Act[38] on November 21 2025, replacing the Disabled Persons Act of 1992. The Act, in Section 47 (e), establishes a fund to subsidise assistive devices and technology for persons with disabilities. However, the fund is not yet

27. Sunday Mail 'Zim rolls out unmanned borders' (2024) https://www.sundaymail.co.zw/zim-rolls-out-unmanned-borders (Accssed 2 November 2024).
28. ParlZim https://www.parlzim.gov.zw/download/senate-hansard-23-october-2025-vol-34-no-92/ (Accessed 1 November 2025)
29. Zimbabwe Department of Immigration https://www.zimimmigration.gov.zw/ (Accessed 12 November 2025)
30. Zimbabwe Broadcasting Corporation 'Government to launch AI Policy' (2024) https://www.zbcnews.co.zw/government-to-launch-ai-policy/ (Accessed 6 November 2024).
31. https://www.parlzim.gov.zw/download/national-assembly-hansard-27-november-2025-vol-52-no-10/
32. UNESCO https://unesdoc.unesco.org/ark:/48223/pf0000394wastraining685 (Accessed 15 November 2025)

operationalised, as the Act has not yet come into force and will come into operation on a date to be fixed by the President by notice in the Government Gazette. This is an implementation gap that limits the immediate enforceability of policies.

The Act also mandates the "availability of information intended for the general public in accessible formats and technologies appropriate to different kinds of impairments in a timely manner and without additional cost." So far, government websites such as the Ministries of ICT and of Education do not have accessibility built in. In May 2025, POTRAZ collaborated with the Internet Society Zimbabwe Chapter to train persons with disabilities from Mashonaland West on cybersecurity.[39] Further trainings of 100 persons with disabilities were conducted in Matabeleland South Province, focusing on digital skills.[40] While this demonstrates inclusion, there is no project data indicating wide coverage across all underserved communities. To ensure sustainability, reports showing impact beyond the training should also be made available to the public domain for assessment.

Universal Service Fund

Zimbabwe has existing legislation on the Universal Service Fund (USF), established by Section 73 of the Postal and Telecommunications Act, 2000 (Chapter 12:05). Annually, the Fund has implemented projects to support persons with disabilities and ICT support to various communities. However, universal coverage has not yet been achieved as infrastructure challenges, including access to electricity, contribute to the lack of internet access in some parts of the country. As of May 2025, the power utility has a backlog of 467,470 client connections due to high connection costs, leaving communities unconnected and unable to access the Internet.[41] Holders of licences in terms of the Act, including telecommunications operators, pay licence fees that finance or assist in financing the extension of postal and telecommunication services to underserved areas and community centres within or outside such areas. The mechanism is not transparently administered, as limited information is available on the contributions made by the telecommunications companies. The POTRAZ website is not adequately updated to reflect the administration and collection of funds. This lack of proactive disclosure by the regulatory authority directly affects Principle 29(3) of the Declaration.

The Treasury committed[42] to mobilising a total of ZiG594 million (approximately US$22 758 620) through the Universal Services Fund, citing that the money will be allocated towards the construction of base stations and digital services centres, the deployment of tele-medicine at health centres, and the training of people with disabilities in the provinces in the use of ICT services. Of the ZiG594 million committed for digital inclusion initiatives, available budget data indicates that ZiG54.3 million (approximately US$2 080 459) was disbursed through the Universal Services Fund during the first half of 2025, with the remainder reflecting budgetary allocations and planned expenditure rather than fully realised disbursements. In the 2025 Mid-Term Budget Review, the Finance Minister indicated that ZiG436.9 million (US$ 16 681 939) and ZiG54.3 million (US$ 207 331) were spent from the Budget and the Universal Services Fund, respectively, towards digital infrastructure for various projects during the first half of the year. This is concerning as it reflects weak oversight over budgeted funds, as only 9% of the committed funds were disbursed. As a result, policy commitments did not translate into actual impact, weakening USF's governance in the country. The level of investment in USF falls short of what is required to fully support USF projects, creating a gap in achieving meaningful connectivity and inclusion across the country. Access to electricity remains a major stumbling block to in-

33. Persons with Disabilities Bill https://www.veritaszim.net/sites/veritas_d/files/Persons%20with%20Disabilities%20Bill%20H.B.%202%2C%202023%20.pdf (Accessed 10 March 2025)
34. Veritas https://www.veritaszim.net/node/7733 (Accessed onthe the implementation 11 November 2025)
35. Internet Society https://isoc.org.zw/wp/digital-skills-literacy-workshops-persons-with-disabilities-kariba/ (Accessed 21 November 2025)
36. Nkomwa Trust https://nkomwaftrust.org/potraz-nkomwa-foundation-trust-train-100-mat-south-pwds-in-digital-skills/ (Accessed 14 November 2025)
37. World Bank. Zimbabwe Energy Compact Mission. https://thedocs.worldbank.org/en/doc/0c714e463c-17130c6415ac2ffeafff6d-0010012025/original/Zimbabwe-National-Energy-Compact-Mission-300.pdf (Accesed on February 10, 2026)
38. Zim Treasury https://zimtreasury.co.zw/wp-content/uploads/2024/11/2025-INFRASTRUCTURE-Development-Programme.pdf (Accessed 08 November 2025)

ternet access. In the Mid-Term Review, the Treasury reported[43] that the Universal Services Fund allocated ZiG54.3 million to the E-Learning Programme, the USF Shared Sites Programme, the E-Government Programme, and the refurbishment of Community Information Centres (CICs). The Tower Relocation Programme, which aims to extend telecommunications services to 166 underserved and unserved areas, received ZiG13.5 million (US$ 515 463). This funded the relocation of towers to eight sites across four out of 10 provinces. ZiG5 million (US$ 190 912) was allocated to establishing and refurbishing Community Information Centres (CICs), to provide ICT access to marginalised communities, especially in areas lacking essential ICT infrastructure or where services are unavailable or unaffordable, thereby bridging the digital divide. At the regulatory authority level, project-level reports are not available as there is no transparency or proactive disclosure of income and expenditure on the USF. The Regulator's website has information from the first three phases of the project in 2015,[44] a direct disregard of Principle 29(3).

Children's Rights Online

Zimbabwe's Cyber and Data Protection Act (2021) protects and safeguards children's rights online. Part three of the Act addresses offences against children and procedural law, criminalising the production, dissemination, possession or access to child sexual abuse material. This aligns with international best practices that criminalise cyber grooming, accessing such material, and exposing children to pornographic content. In October 2025, Zimbabwe joined 72 other countries in signing[45] the Convention against Cybercrime, reinforcing its call for the protection of the rights of children in line with Article 34 of the UNCRC.

The Government of Zimbabwe is a state party to and has ratified the United Convention on the Rights of the Child (UNCRC), the African Charter on the Rights and Welfare of the Child (ACRWC), and the United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography OPSC). However, gaps remain as Zimbabwe has not yet enacted specific legislation to safeguard children's rights online. At the national level, Section 81 of Zimbabwe's Constitution provides for children's rights. Zimbabwe also has in place the Children's Amendment Act No 8 of 2023,[46] which in Section 2(i) introduces definitions of "child grooming" and "child sexual abuse material," in line with international standards. However, this Amended Act does not fully address digital developments or provide accessible, child-friendly mechanisms for reporting harm, removing harmful content, and seeking justice. In 2015, POTRAZ, inspired by the ITU Guidelines, developed child online protection guidelines to raise awareness of the issue and lay the foundation for protecting children's rights. The guidelines are not binding. In 2025, the Ministry of ICT launched a nationwide consultation survey for children and adults and conducted public consultations to gather input from children and interested stakeholders for the development of a National Child Online Protection Policy. There is no public information on whether the policy has been drafted.

On digital inclusion, Zimbabwe is moderately compliant with the Declaration's Principle 37 (3), as the country has an existing and functional USF, is adopting international treaties and updating policies on children's rights online. However, improving access for underserved communities, including persons with disabilities, should be a major priority to close the gaps in policy and practice.

39. Zim Treasury https://zimtreasury.co.zw/wp-content/uploads/2025/07/THE-2025-MID-TERM-BUDGET-AND-ECONOMIC-REVIEW.pdf (Accessed 5 November 2025)
40. POTRAZ https://www.potraz.gov.zw/?page_id=411 (Accessed 4 January2026)
41. United Nations Treaties. United Nations Convention on Cybercrime. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en (Accessed 2 February 2026)
42. Veriitas https://www.veritaszim.net/sites/veritas_d/files/Act%20No.%208%20of%202023%20Children%27s%20Amendment.pdf (Accessed on January 25 2025)

Conclusion

This report highlights both positive and negative developments. Zimbabwe's score of 36 demonstrates that the country is moderately compliant with the African Commission's Declaration. Policy and implementation gaps remain, as Zimbabwe has neither adopted legislation on emerging technologies and digital IDs, nor revised its traditional gender-based violence policies to address online gender-based violence. Despite comprehensive policies to improve digital access, at the implementation level, challenges persist in providing connectivity to underserved communities due to recurring infrastructure issues and limited transparency around USF projects. The existence of sedition laws, false news criminalisation and the arrests of journalists is a major setback in compliance with the Declaration Principles 22(2) and 20 (1) and (2). Despite existing challenges, Zimbabwe has opportunities to improve its oversight mechanisms to strengthen the DPA's focus and ensure parliamentary oversight of surveillance systems and the appointment of independent commissioners.

Recommendations

The Government should:

- Amend GBV-related laws, such as the Domestic Violence Act, to recognise, prevent and combat Tech-Facilitated GBV, in line with Resolution 522
- Sign and ratify the African Union Convention on Cyber Security and Personal Data Protection, to strengthen alignment with Principles 41 and 42 of the Declaration
- Conduct public consultations and human rights impact assessments before implementing surveillance initiatives.
- Repeal Sections 31 and 33 of the Criminal Law (Codification and Reform) Act that criminalise false news and sedition.
- POTRAZ should proactively disclose information on USF projects by keeping it up to date and making it readily available on government websites.
- Update the Children's Amendment Act 8 of 2023 to provide child-friendly reporting channels and provisions for the removal of harmful content.
- POTRAZ should promote regular proactive disclosures of information through official channels and publish regular reports on data breaches, enforcement of the CDPA, licensing and USF expenditure.

Civil Society Organisations should:

- Conduct public audits/assessments on the implementation of the CDPA
- Engage in litigation initiatives to address violations resulting from surveillance and arbitrary arrests.
- Conduct awareness campaigns on children's rights and the rights of persons with disabilities.
- Advocate for policy reform on false news criminalisation and sedition legislation

Media should:

- Investigate developments in the ICT sector to ensure policies protect and do not subject journalists to arbitrary arrests
- Collaborate with civil society organisations in educating the public on digital rights and inclusion.

The Private Sector should:

- Conduct human rights impact assessment and due diligence measures before deploying surveillance technologies, ensuring technology development and deployment are in line with the United Nations Guiding Principles on Business and Human Rights
- Conduct public consultations to engage citizens on the deployment of new technologies to ensure products are human rights compliant.
- Publish transparency reports on the use of surveillance technologies to ensure transparency and accountability, in line with global transparency standards.

The Score Index

Zimbabwe, 2025

1. Totally non-compliant. 2. Mildly compliant - which is a mild attempt at compliance with critical gaps. 3. Moderately compliant - where there are areas of improvement. 4. Considerably compliant - Minimal areas of reform. 5. Fully Compliant - No concerns

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Internet Shutdowns	P38(2)	4	4	Zimbabwe did not shut down the Internet in 2025. In 2019, after an internet shutdown, a court ruled that internet shutdowns are illegal. Since then, there has been internet shutdowns in 2022 and in 2023.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37	4	4	Policies such as the National Broadband Plan, the National ICT Policy, and NDS1, among others, exist. NDS2 is currently under development. However, universal, affordable, meaningful access to the Internet for all, including children and persons with disabilities, is still a work in progress.
False News Criminalisation	P22(2)	1	1	Under Section 31(a)(iii) of the Criminal Law (Codification and Reform) Act, it is an offence to publish or communicate a statement that is wholly or materially false with the intention of undermining public confidence in law enforcement

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
				agencies or the state. Violators can face penalties of up to 20 years in prison for such offences.
Sedition Legislation	P22(2)	1	1	Under Section 33 of the Criminal Law (Codification and Reform) Act, it is an offence to undermine the authority of or insult the President. Violators can face penalties of up to 20 years in prison. Journalists and citizens were arrested in the period under review.
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20(1) & (2)	3	2	During the reporting period, journalists and citizens were arrested in violation of their rights to freedom of expression and access to information online.
Data Protection Legislation.	P42	3	4	Zimbabwe adopted the CDPA; however, the regulations do not require general data breach notification to data subjects. Despite the work underway, there are lingering concerns that the Data Protection Authority may not allocate sufficient time and resources to data protection, as the data protection mandate is an add-on to its primary mandate of regulating the telecommunications sector. Implementation of the CDPA and regulations began.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)	5	5	No cases were recorded. Meta and TikTok transparency reports for 2025 reflect that Zimbabwe did not make any content takedown requests. Google's transparency report has no information on Zimbabwe.
Invasion of Privacy of Communications	P41	2	2	The Cyber Security and Monitoring of Interceptions of Communications Centre is housed in the Office of the President and suggests the potential to target vulnerable groups through targeted surveillance. Section 6 of the Interception of Communication Act Section 6 (a,b and c) mandates the Minister to issue a warrant to authorised persons if there are reasonable grounds for the Minister to believe that the gathering of information concerning an actual threat to national security or to any compelling national economic interest is necessary or the gathering of information concerning a potential threat to public safety or national security is necessary. The above provisions expose individuals to invasion of their private communications.
Failure by the government to proactively disclose and disseminate information	P29(3)	3	3	Government websites often carry outdated information. Zimbabwe has an existing Freedom of Information Act. Improvements were shown in the public disclosure of information on the USF.

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
on digital technologies.				
AI and Emerging Technologies national strategies	P39(6)	2	2	Despite being announced as complete, Zimbabwe's AI Policy was not yet publicly available on official government platforms as at December 31 2025. However, the CDPA in section 4 (1) provides for automated decision-making.
Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online	P37(5)	3	3	Zimbabwe adopted the CDPA, which has provisions protecting children's rights online. Public consultations on the child online protection framework were conducted.
Digital Inclusion	P37(3)	3	3	There are laws in place to support digital inclusion through the Universal Service Fund. The score improved due to the availability of information on the USF and the funds allocated. Zimbabwe gazetted the Persons with Disabilities Act, which seeks to ensure access to technology for persons with disabilities. However, challenges persist as the rural-urban divide exists and limited infrastructure, coupled with electricity supply challenges, hinders progress towards achieving meaningful inclusion.
Total (out of 60):	2024: **34**		2025 **34**	

LONDA 2025 INDEX SCORES

Overall Country Performance Rating
1.Totally Non-Compliant (0)
2. Mildly Compliant (less than 30)
3. Moderately compliant. (30 and less than 45)
4. Considerably Compliant (45 and more)
5. Fully Compliant (score of 60)

NB: Compliance is with regards the ACHPR Declaration of Principles of Freedom of Expression and Access to information in Africa

Country	Internet Shutdowns		Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet		False news criminalisation		Sedition legislation		Arbitrary arrests and harassment of the media, HRDs and citizens		Data protection legislation		States interfere and require the removal of online content by internet intermediaries		Invasion of privacy		Failure by the government to proactively disclose and disseminate information digital technologies		AI and emerging technologies		Adoption of specific child laws, policies and measures promoting children's digital safety and privacy online		Digital Inclusion		2024 Score	Difference Green +ve Red -ve Black Constant	2025 Score	2024 Ranking	2025 Ranking
	2024	2025	2024	2025	2024	2025	2024	2025	2024	2025	2024	2025	2024	2025	2024	2025	2024	2025	2024	2025	2024	2025	2024	2025					
South Africa	5	5	3	3	4	4	5	5	3	3	4	5	5	5	3	3	3	4	2	3	3	3	3	4	43	4	47	1	1
Ghana	5	5	4	4	1	1	3	3	2	2	5	5	4	4	5	5	3	3	3	4	3	3	4	4	42	1	43	2	2
Namibia	5	5	2	4	4	4	5	5	4	3	2	2	4	4	4	4	3	3	2	2	2	2	2	4	39	3	42	4	3
Senegal	1	4	3	3	1	1	3	3	3	1	4	4	2	3	4	4	4	4	3	3	4	4	4	4	36	2	38	5	4
Egypt	4	4	4	5	1	1	1	1	1	2	3	4	2	2	1	1	3	4	5	5	3	4	4	5	32	6	38	13	4
Zambia	5	5	4	3	3	3	2	2	2	2	4	4	4	4	3	2	4	3	4	3	2	3	3	3	40	-3	37	3	6
Kenya	2	2	4	3	1	2	3	3	1	2	5	5	3	2	2	2	4	3	3	5	3	5	3	3	34	3	37	9	6
Rwanda	5	5	4	4	3	3	2	3	1	1	4	3	2	3	1	1	3	3	5	4	3	3	3	3	36	0	36	5	8
Malawi	5	5	4	4	1	1	3	4	2	2	3	3	4	5	2	1	4	3	1	2	3	3	3	3	35	1	36	8	8
Nigeria	3	3	4	4	3	2	1	1	1	1	4	4	4	3	3	3	2	3	4	4	3	3	4	4	36	-1	35	5	10
Lesotho	4	4	4	4	3	3	1	1	1	1	4	4	3	4	3	3	2	2	2	3	1	3	3	3	31	4	35	15	10
Botswana	5	5	3	4	1	2	1	1	2	3	3	4	2	2	2	3	3	4	2	2	1	1	3	4	28	7	35	20	10
Tunisia	5	5	3	3	1	1	1	1	1	1	3	3	4	4	2	2	3	3	3	3	4	4	4	4	34	0	34	9	13
Zimbabwe	4	4	4	4	1	1	1	1	3	2	3	4	5	5	2	2	3	3	2	2	3	3	3	3	34	0	34	9	13
The Gambia	5	5	4	4	1	1	1	1	1	1	2	3	5	5	4	4	2	2	1	2	4	4	1	2	31	3	34	15	13
Benin	4	4	3	3	1	1	1	1	3	3	4	4	3	3	3	3	3	3	3	3	3	2	2	3	3	33	0	33	12	16
Sierra Leone		5		3		2		5		2		3		3		2		3		2		1		2	0	-	33		16
Somalia	3	4	2	3	2	2	2	2	2	2	4	4	2	3	2	2	3	3	2	3	1	1	2	3	27	5	32	22	18
Cote d'Ivoire		4		2		3		3		2		4		1		2		2		4		2		3	0	-	32		18
CAR	5	5	2	2	2	2	2	2	3	3	4	3	3	3	4	4	2	2	1	1	1	1	2	2	31	-1	30	15	20
Angola	4	2	3	3	2	2	2	2	2	2	4	4	2	2	3	3	3	3	2	2	2	2	2	2	31	-2	29	15	21
Togo	4	3	3	3	2	1	3	2	1	1	4	4	2	2	1	1	3	3	2	3	2	2	2	3	29	-1	28	19	22
Cameroon	3	1	3	2	2	3	2	3	2	1	4	3	3	3	3	2	2	1	2	3	4	3	2	2	32	-5	27	13	23
Uganda	3	2	2	2	1	1	1	3	1	1	4	3	2	2	2	3	3	2	3	2	3	2	3	3	28	-2	26	20	24
Tanzania	2	1	2	3	1	1	1	1	1	1	3	4	2	2	2	2	4	3	2	2	3	3	4	3	27	-1	26	22	24
Ethiopia	1	4	2	2	1	1	2	2	1	1	3	3	2	2	1	1	1	1	2	3	3	3	2	3	21	5	26	26	24
Mozambique	1	1	3	3	2	2	2	2	1	1	1	2	4	4	1	1	2	2	1	1	3	3	2	2	23	1	24	25	27
DRC	3	1	3	3	1	1	1	1	1	1	3	3	3	1	2	2	2	2	2	2	3	2	2	2	26	-5	21	24	28
Sudan	2	1	2	3	2	2	2	2	1	1	2	2	2	2	1	1	2	1	1	1	2	2	2	2	21	-1	20	26	29