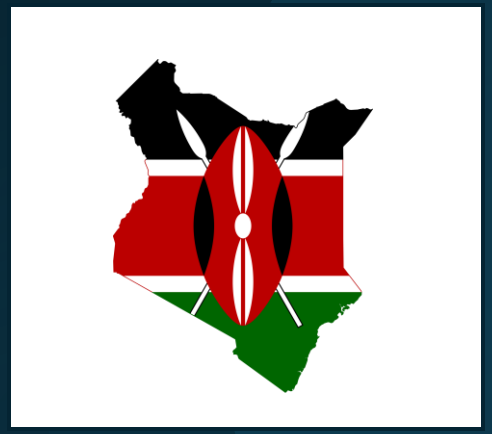





Digital Rights Alliance Africa

Baseline Monitoring Report

2025

Digital Rights Alliance Africa Baseline Monitoring Report 2025

This publication has been produced with financial support from Norway. The contents of this publication are the sole responsibility of Digital Rights Alliance Africa and can in no way be taken to reflect the views of the Government of Norway.

Table of Contents

Introduction

Overview of the Report

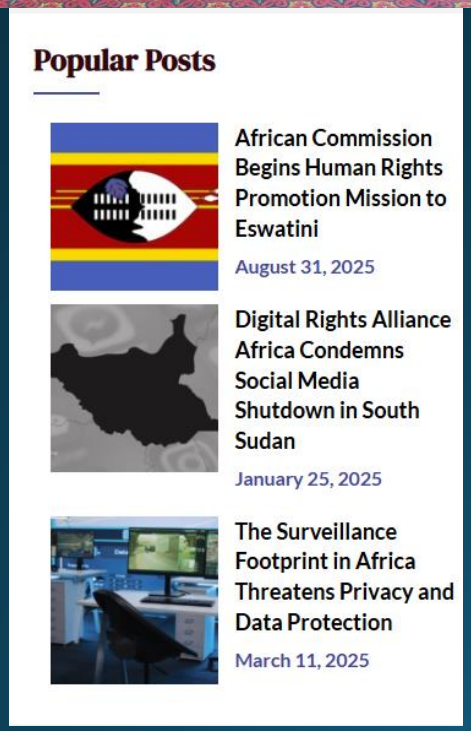
This baseline monitoring report is a collective effort by civil society members of the Digital Rights Alliance Africa to capture the state of the digital rights in their countries as it stands at the end of the 2025 calendar year. The goal is for members to assess the evolving legal and policy environment governing digital rights. The snapshot provided in this report will not only be used to promote evidence-based advocacy but also to guide the efforts of DRAA members in the coming years to ensure advocacy actions continue to address identified needs, to track if and how DRAA members' perceptions of the digital rights environment change over time, and to determine whether governments make progress towards improving online civic space.

Rather than providing an in-depth examination of all digital rights topics, the report focuses on issues related to legal frameworks and policies that impact meaningful internet access and privacy rights. DRAA members identified internet shutdowns, connectivity and affordability policies, cybercrime laws, digital identification frameworks, and data protection laws and enforcement as having the most relevance across the nine countries under review: Cameroon, Democratic Republic of Congo (DRC), Ethiopia, Kenya, South Africa, Tanzania, Togo, Uganda and Zambia.

The report provides the following takeaways:

- Despite constitutional protections, digital laws impermissibly restrict the rights to freedom of expression and privacy.
- Gaps in oversight and accountability by state actors and the private sector remain a key challenge.
- Digital Public Infrastructure and Artificial Intelligence are increasingly shaping the digital environment and inclusion in public decision making but with limited oversight and regulation.
- Civil society organizations are critical players in the digital civic space governance.

What is DRAA? Envisioning an Africa where digital rights are respected and protected.



The Digital Rights Alliance Africa (DRAA) is a pan-African, diverse coalition of formal civil society organizations (CSOs), human rights defenders (HRD), media practitioners, lawyers, and technologists that seek to champion digital civic space and counter threats to digital rights on the continent.

DRAA was established in 2023 by the International Center for Not-for-Profit Law (ICNL) and the Collaboration on International ICT Policy for East and Southern Africa (CIPESA).

As of 2025, DRAA members represent 13 countries. DRAA enables members to jointly leverage resources, learn from each others' experiences, and act collectively in ways that:

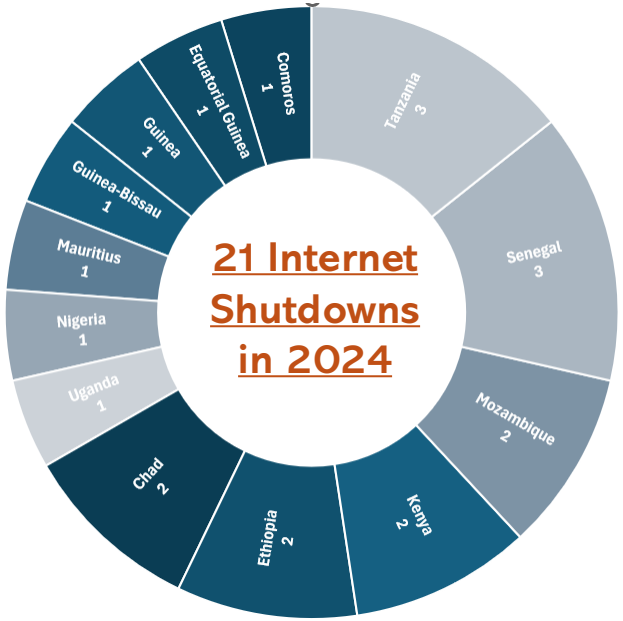
1. **Strengthen members' advocacy**, awareness creation, and strategic litigation to advance digital rights in Africa by building capacity and supporting research, monitoring, and resource creation.
2. **Collaborate to promote progressive frameworks** on digital rights at local and regional levels.
3. **Foster civil society engagement on digital rights norm settings** with technical standards and multilateral bodies at regional and international levels through awareness raising, capacity building and networking with stakeholders in the community of service.

The Digital Rights Environment in Africa

Public understanding of the human rights impacts of digital technologies is still nascent in Africa despite its growing relevance. The digital rights environment has been defined by governments disproportionately controlling online civic space while inadequately acting to stem abuses perpetrated by the private sector. This impunity has been facilitated by a lack of transparency, enabling internet shutdowns, invasive surveillance, and data protection violations to take place without independent oversight or redress. Meanwhile, digital innovation and use has far outpaced legal and policy developments, resulting in flawed and outdated regulations.

2024 Internet Penetration Rate at 38%

up 13% percentage points since 2019



21 Internet Shutdowns in 2024

2 Internet Shutdowns in 2025 During Election Periods

Cameroon
Tanzania

2025 study suspects Mozambique purchased Predator spyware

Other Cytrox customers have included Angola, Botswana, DRC, Egypt & Madagascar

Acknowledgement of DRAA Contributors

The following organizations contributed to collecting data, writing, and reviewing this report:

Bingwa Civic Tech Lab

Bloggers of Zambia

Centre for Artificial Intelligence Ethics and Governance in Africa

Collaboration on International ICT Policy for East and Southern Africa

International Center for Not-for-Profit Law

International Federation of Women Lawyers Cameroon

Jeunes Verts

Nubian Rights Forum

Methodology

1

2

3

Prior to data collection, DRAA members met virtually to discuss various digital rights topics and the issues most relevant in their countries. ICNL consolidated the ideas and shared a survey asking members to rank them in order of priority. Three topics emerged as the most pertinent, and members agreed that monitoring developments in these areas should be a long-term goal of the Alliance.

- Tracking overall legal and policy developments that impact digital rights.
- Tracking the enactment and enforcement of data protection laws.
- Tracking barriers to meaningful internet access due to policy action or inaction.

After identifying the priority topics, research was conducted to map existing monitoring projects and research activities of other digital rights coalitions and organizations in Africa. It was determined that the perspectives of domestic CSOs were missing from the ecosystem. Thus, ICNL and CIPESA sought to design a monitoring tool that not only captured the current environment but asked members to pinpoint the gaps in policies and government enforcement, their vision of what success and progress on digital rights is in their countries, and the local CSO initiatives that are seeking to advance those goals. A form was created that would capture baseline data and the form was presented to DRAA members for review and feedback.

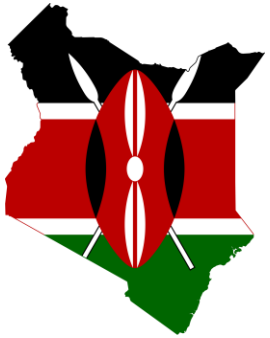
Once DRAA members validated the data collection form, they completed it by relying on internal expertise and desk research, with ICNL and CIPESA providing support as needed. The submitted data was compiled and analyzed by ICNL and fact checked by CIPESA. DRAA contributors were asked for their input when clarity or additional information was needed. ICNL and CIPESA occasionally supplemented submissions with additional desk research on Africa-wide issues or if country-level data required more context. The report was then shared with the contributors for review.

Countries That Were Reviewed

CAMEROON (CM)

DEMOCRATIC REPUBLIC OF CONGO (DRC)

ETHIOPIA (ET)



KENYA (KE)

SOUTH AFRICA (SA)

TANZANIA (TZ)

TOGO (TG)

UGANDA (UG)

ZAMBIA (ZM)

Regional Norms on Digital Rights

Updates

Overview

African standards on digital rights have been expanding over the years with a mix of regional treaties, declarations, and soft-law principles developed mainly by the African Union and the African Commission on Human and Peoples' rights as well as regional networks of digital advocates. These frameworks aim to protect human rights in the digital age—covering privacy, freedom of expression, access to information, and data protection, which guidance member states should comply with. However, state practice continues to show adverse impact on these rights due to new and existing restrictive laws used by authorities against CSOs/HRDs and political opposition.

African Charter on Human and Peoples' Rights (1981) guarantees freedom of expression and the right to receive information(Article 9) and freedom of assembly and association (Article 10). While privacy is not expressly mentioned in the Charter, the right is interpreted under broader rights. In its resolutions 473 (2021) and 573 (2023), the ACHPR has emphasized that the growing deployment of interception technologies, and surveillance tools, without sufficient safeguards, create systemic risks for privacy and other fundamental rights

African Union Convention on Cyber Security and Personal Data Protection (2014) (i.e., the Malabo Convention) provides for principles on personal data protection (e.g., consent, legitimacy, security) and cybercrime regulation.

Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) is a soft-law framework that contains strong digital rights provisions; Principle 5 recognizes that the same rights that people have offline should be protected online. It covers internet access as a fundamental enabler of rights, protection against unlawful surveillance, net neutrality principles, and limits on internet shutdowns

African Declaration on Internet Rights and Freedoms is a civil society–driven framework that emphasizes open and accessible internet, freedom from censorship, digital inclusion and gender equality, and transparency in governance

Recent African Union Updates

The Convention on Ending Violence Against Women and Girls (Feb. 2025) acknowledges that violence against women and girls manifests in cyberspace and calls on States to enact and enforce laws to address such threats.

The Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade (Feb. 2024) acknowledges that advanced technologies can foster innovation and deepen economic cooperation, encourages the ethical adoption and use of such technologies, and calls on African States to establish predictable and harmonized standards to enable digital trade.

The African Digital Compact (Aug. 2024) is the common position on digital transformation by the continent's ministers to harness digital technologies to drive sustainable development across Africa, bridge digital divides, and protect digital rights, in line with the UN's Global Digital Compact.

The Continental AI Strategy (Aug. 2024), endorsed by the AU's Executive Council, establishes Africa's commitment to an Africa-centric and ethical approach to AI development and use and calls for unified national approaches among AU Member States to navigate the complexities of AI-driven change. AAEA Principles and Guidelines for the Use of Digital and Social Media in Elections, 2023 to guide digital campaigns and check state sponsored disinformation

The Interoperability Framework for Digital Identification (Dec. 2023) provides for a continental standard on the interoperability of digital IDs and proofs of identity issued by AU Member States.

The Digital Transformation Strategy (May 2020) continues to guide the AU's vision until 2030.

Recent ACHPR Updates

Similar to the African Union, the African Commission on Human and Peoples' Rights (ACHPR) is taking steps towards strengthening digital norms across the Continent but with a focus on protecting civic freedoms. The ACHPR has largely focused on:

Artificial Intelligence and other emerging technologies: The ACHPR Resolution on AI and draft AI Study encourage key policy interventions to harness potential of AI in line with Agenda 2063 and the sustainable development goals. Mindful of its risks (data bias, AI divide), these documents emphasize risk mitigation, good governance, inclusion and diversity, human rights, gender equality, dignity, and safety. They call for coordination with stakeholders, including civil society. Despite the ACHPR's efforts and the growing use of AI technologies by States, normative guidance has been too general to be actionable and there has been little efforts to address human rights risks during AI deployment in practice.

Combating arbitrary surveillance practices: The ACHPR Guidelines on Association and Assembly (2017) requires States to respect the right to privacy for CSOs and protect CSOs from undue surveillance and provide redress. Other efforts by the ACHPR to address the rise of the surveillance ecosystem has been ACHPR Resolution 573 (2023) on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa and Principle 41 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa, calling on States not to engage in untargeted communication surveillance and to provide adequate safeguards for the right to privacy.

Data Protection: In line with the Malabo Convention, ACHPR Res 620 (2024) focuses on promoting data access for advancing human rights and sustainable development in the digital age. However, data protection frameworks continue to include overly broad, loopholes, largely drawn from European standards without sufficient adaptation to African realities.

Internet shutdowns: The topic of internet shutdowns has not been forcefully addressed by the ACHPR since it adopted the African Commission Declaration on Freedom of Expression in 2019. Rather, it is the regional courts, particularly ECOWAS, leading jurisprudence and filling the accountability gap when violations occur.

Regional Human Rights Courts Updates

Regional courts have largely ruled against digital rights repression by States, citing the right to freedom of expression in the African Charter on Human and Peoples' Rights and the ICCPR as the basis for addressing issues ranging from surveillance to internet shutdowns to cybercrime laws. In 2025, three cases have crossed the docket of regional courts:

The Community Court of Justice of the Economic Community of West African States (ECOWAS) – 2025 Decision

In 2023, Senegal ordered a full internet shutdown when protests erupted against the arrest and conviction of a prominent opposition political figure. In *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) & Anor v Republic of Senegal*, the ECOWAS Court found that the shutdown violated the rights to freedom of expression, freedom of peaceful assembly, and access to information. The Court affirmed that the restriction was not provided by law, did not seem to respond to a legitimate interest, and could not be considered proportionate given that the entire internet was rendered inaccessible.

The African Court on Human and Peoples' Rights (AfCHPR) – Pending

Following comments on a news broadcast that criticized policies of the Tunisian Government, lawyer and advocate Sonia Dahmani was arrested for spreading false information under Decree 54. Her case is now pending review at the AfCHPR, which could lead to a landmark decision addressing a digital rights restriction in Northern Africa.

The East African Court of Justice (EACJ) – Pending

Seguya Hillary Innocent v Attorney General of Uganda (Ref. 21 of 2020) seeks to challenge the High Court of Uganda's ruling that the Government's blocking of social media platforms, rendering them inaccessible, in 2019 was lawful. The High Court ruled against petitioner challenging the Government's action, dismissing the case with costs. The case is currently under review.

Analysis of Regional Trends

AU instruments emphasize (i) the importance of access to the internet in the digital age; (ii) the need to create independent oversight and comprehensive governance frameworks on digital rights; and (iii) the importance of participation by CSOs in the development of policies and regulatory frameworks - which includes digital literacy and capacity building.

Domestication of regional standards remains a key priority, but State practice is still inconsistent and less harmonized.

- Several States are consulting on **new AI strategies**, but these are skewed at the technical level and pose heightened risks due to the lack of human rights due diligence.
- **Surveillance frameworks** grant excessive powers to security agencies to take arbitrary measures justified as 'national security.
- **Internet shutdowns** are becoming commonplace in recent election cycles in the name of protecting national security without credible evidence or independent oversight.
- **Data protection frameworks** are being adopted in a rush to align with EU GDPR and implementation is affecting CSOs with limited capacity to comply.

Civic Space Online

Overview

Civic Space Freedoms Online

Online civic space mirrors the notion of civic space in traditional spheres. The same key rights are applicable:

- **Freedom of Expression**
- **Privacy**
- **Peaceful Assembly**
- **Association**

Both international and African regional human rights frameworks recognize that limitations to these rights may be legitimately imposed in order to protect national security, public safety and order, public health or morals, and the reputation, rights and freedoms of others. However, to comply with human rights standards, these limitations must be provided for by law and be genuinely "necessary", which means – among other things – that they should respond to a pressing public need and be proportionate to their stated aim. These factors are encapsulated in the Three-Part Test, meaning a restriction to online civic freedoms is only permissible if all the following factors are met:

The restriction must be provided by law. It is not enough for a restriction to be written into law, it must be written clearly and accessibly, with enough precision to prevent undue discretion by authorities.

The restriction must pursue a legitimate purpose. (national security, public safety/order, public health/morals, and the reputation, rights, and freedoms of others).

The restriction must be necessary, and the least restrictive means to achieve the purported aim. Laws or actions that are broad and that attempt to restrict a wide range of behavior are not considered narrowly tailored to prevent the alleged harm.

The burden lies with the State to show that laws and regulations pass this three-part test.

Constitutions Protect Civic Space (with limitations)

In all countries under review, the Constitution protects the rights that bolster online civic space; three caveats, however, prevent the full realization of the constitutional protections:

1. The language of provisions may not align with human rights law. Rather than reflect the three-part test, in accordance with the International Covenant on Civil and Political Rights and the African Charter, they may only include the "provided by law" standard without referencing the legitimacy and proportionality standards.

2. Within the Constitution itself, there may be conflicting articles that undermine a civic space right, such as broad emergency powers or authorities to restrict rights for purposes other than the legitimate purposes listed in the ICCPR and the African Charter.

3. Implementing laws and regulations may not align with the civic space guarantees of the constitution, setting forth vague prohibitions that can be arbitrarily enforced or creating disproportionate restrictions that are not narrowly tailored to achieve the intended aim.

Article 31: Everyone has the right to privacy and to the confidentiality of correspondence, telecommunications, and any other form of communication. This right may only be infringed in cases **provided for by law.**

Article 25: Enables the President to derogate from civic space rights in times of emergency. Articles 30 and 32 give the President broad authority to declare that a state of **emergency or threatened emergency** exists, with no limits as to the nature, scope, or powers granted.

Section 26 of the Computer Misuse Act includes **restrictions on speech** that are vague and penalties that are likely disproportionate. In 2024, the Act was used to prosecute Tik Tok users for otherwise protected speech.

Perceptions

Governments have shown increased interest in leveraging digital tools and participating in digital transformation initiatives. Some countries, like Tanzania, have invested heavily in expanding internet connectivity. Yet, apart from South Africa, the perception among DRAA members is that their States' protection of digital rights is poor. This reflects broader civic space trends. For example, between 2015 and 2025, all the DRAA countries reviewed in the report experienced **a decline in its "Freedom in the World" score**, except for South Africa and Ethiopia. The biggest declines are in Tanzania (58 to 28), Togo (48 to 37), and Cameroon (24 to 15).

While these Freedom House scores only show a partial picture, they can help validate civil society's perspectives and align with DRAA's analysis of the trends in Africa:

- Despite existing normative frameworks on digital rights, **domestication and enforcement by States is relatively slow** with a tendency towards foregoing transparency and independent oversight as a means to evade accountability.
- States use **broad national security justifications** to tighten control of online spaces through extralegal or disproportionate enforcement and by enacting vaguely worded cybercrime, disinformation, fake news, and criminal defamation laws.
- Online repression is **heightened during protests and elections** which shows measures deliberately aimed at controlling online spaces to undermine democratic participation, accountability and entrench digital authoritarianism.
- The **private sector plays a key role in fueling digital abuses** by states and yet civil society faces barriers to engage with the companies on these concerns.

The perception ratings follow a 1 to 5 scale. DRAA members from Tanzania and Ethiopia chose not to provide ratings.

	Freedom of Expression	Privacy	Peaceful Assembly	Association	Example
 DRC	2	1	2	2	On Oct. 1, the National Police arrested activist Jedidia Mabela after he criticized local corruption and called for greater transparency. The arrest took place without a warrant, and he was convicted the following day on charges of "spreading false rumors" and "defamation" in violation of Articles 199 and 74 of the Penal Code.
 CM	1	1	1	2	Over the pre and post Oct. election, the Minister of Territorial Administration repeatedly warned Cameroonians not to post, share, or like anything online that criticizes the government. Activists have been arbitrarily arrested after posting protected speech, such as criticism of government actions.
 KE	3	1	1	3	Suspicions that authorities surveilled protesters were confirmed in Sept. 2025 during court proceedings against a university student who posted criticism about the president in 2024. A police officer called as a witness said that call triangulation and tracing at Safaricom was performed without a court order.
 SA	4	4	4	4	No specific online civic space violation was reported in 2025, but the country's rapid deployment of digital technologies that can be used for mass surveillance, such as cameras equipped with facial recognition, without strong legal safeguards create risks for abuse.

	Freedom of Expression	Privacy	Peaceful Assembly	Association	Example
 TG	2	2	1	1	In June 2025, authorities ordered the blocking of popular platforms (e.g., Facebook, WhatsApp, YouTube, Signal) during protests. Technical analysis revealed domain blocking through intentional interference, causing connection and timeout failures. The shutdown restricted access to nearly 3.5 million people.
 UG	2	2	2	2	Many grave human rights violations occurred in 2025 during the campaign period in the lead up to the January 2026 general election. Among the violations included arrests of social media influencers, such as university student and TikTok'er Elson Tumwine for "offensive communication" and "computer misuse," vague provisions in Uganda's cyber laws.
 ZM	3	2	2	3	In 2025, former Parliamentarian Munir Zulu was sentenced on several counts for a social-media posts criticizing the President and other government leaders under provisions in the Penal Code that criminalize sedition and defamation. The provisions are vague, prohibiting speech that should otherwise be protected under the Constitution and the ICCPR.

Examples of Civil Society Initiatives

HRNJ-Uganda has built capacity of journalists as far as digital securit is concerned.

Center for Advancement of Rights and Democracy and the **Ethiopian Human Rights Council Organization** have worked to gather documentation on digital rights violations, conduct public awareness, engage in strategic advocacy, and provide digital literacy resources to communities

Since 2022, **Bloggers of Zambia** has convened the **CSO Coalition on Digital Rights** to coordinate collective advocacy. Bloggers also raises awareness on data governance and works with underserved communities in rural areas to provide digital literacy and ICT governance training ICT. **Internet Society Zambia Chapter** runs capacity-building programs for individuals, civil society, and technical communities understand data rights and responsible data practices.

La Différence's Pamoja Network enables residents of Idjwi island in Lake Kivu to access the internet. **Bingwa Civic Tech Lab** promotes digital and civic Literacy through its Digital & Gender Inclusion Labs. **Rudi International** supports youth impacted by conflict through the Elimu Technology Center.

Moxii Africa trains youth in digital and media literacy via Web Rangers and the Advanced Media Literacy Program, campaigns for universal free internet access and zero-rating, and builds media accountability resources such as NewsDiffs. **Moxii** also submits evidence of data protection abuses by platforms to regulators and promotes ethical data practices for media consumption and creation.

Nubian Rights Forum is litigating to ensure that all digitized services are accessible and affordable to ethnic minorities who live in remote areas. Meanwhile, ma Kenyan organizations are involved in litigation, advocacy, and community sensitization to encourage accountability regarding data protection.

Libra Law Office raises awareness of digital rights and conducts trainings for CSOs. **Paradigm Initiative** conducts digital rights and data protection advocacy. They also have a platform to report violations. **My Data Cameroon** organizes webinars to facilitate multistakeholder and build capacity on data protection best practices.

DataSecur Consulting, and ESTETIC, Togo Data Lab, and the **Internet Society Togo** offer trainings on data privacy and responsible data governance. **Festival De Datos** fosters multistakeholder consultations on data for environmental protection and health. **Internet Society Togo** also runs nationwide programs to promote community WiFi, connectivity in schools, and digital safety and digital literacy.

Cybercrime Laws

Impact on Civic Space

Cybercrime Laws

Cybercrime across Africa has been on the rise.
The Continent has lost about 4 billion USD annually to cyber fraud. According to the 2025 Interpol Cyberthreat Assessment Report:

- **2/3** of countries throughout Africa reported that cybercrimes accounted for at least 10% of all crimes, with countries in Western and Eastern Africa reporting that cybercrime accounted for at least 30% of all crimes.
- **#1** most common cybercrime was reported to be online scams and phishing. Banking fraud, digital sextortion, and ransomware attacks were also considered to be major law enforcement concerns.
- **75%** of countries reported that they lack the legal frameworks and prosecution capacity to fully address the threats.

So, aren't cybercrime laws necessary? There is no denying that cybercrimes pose threats to public safety, individual rights, and national security that require robust legal responses. However, laws do not comply with a country's human rights obligations when they include 1) overly vague categorization of crimes that unduly restrict legitimate speech, 2) restrictions on important privacy protecting tools (e.g., encryption and virtual private networks) that can help the public mitigate individual risks when using the internet, and 3) disproportionate authorities to conduct digital surveillance without independent judicial oversight or other safeguards to prevent abuse. Such provisions undermine the interests and rights that the governments are seeking to protect.

The following tables outline the legislation in each country under review and explains the civic space impacts and whether the law has been challenged to date. Eight of the 9 countries have standalone legislation. DRC does not but addresses cybercrime in other legislation. Civil society in all 9 countries reported that their countries' cybercrime laws threaten the rights to privacy and freedom of expression. In three countries, Kenya, Uganda, and Zambia, there are ongoing legal challenges to the laws.

Cybercrime Laws

Country	Cybercrime Law	Impacts on Rights	Legal Challenges
 DRC	**No standalone law.** The Digital Code (No. 23-010) and the Telecommunications Act (No. 20-017) address cybercrimes.	**Freedom of Expression**: Many vague prohibitions of online speech **Privacy**: protections for personal data; authorization of surveillance without a warrant	No known legal challenges.
 CM	Law No. 2010/012 on Cybersecurity and Cybercriminality adopted in Dec. 2010	**Freedom of expression**: overly broad restrictions on content, intermediary liability **Privacy**: interception of electronic communication without judicial review; mandatory data retention by ISPs, access to encrypted data and private keys	No known legal challenges.
 KE	Computer Misuse and Cybercrimes Act adopted in May 2018	**Freedom of Expression**: overly broad restrictions on content **Privacy**: disproportionate surveillance powers	The Constitutional Court has suspended sections until further review, stalling passage of proposed amendments. Litigation is ongoing.

Cybercrime Laws

Country	Cybercrime Law	Impacts on Rights	Legal Challenges
 ET	Computer Crimes Proclamation No. 958 adopted Jul. 2016	**Freedom of Expression**: overly broad restrictions on content, such as "incitement of fear" online **Privacy:** disproportionate powers authorizing search, seizure, and surveillance	No known legal challenges.
 SA	Cybercrimes Act 19 adopted in Jun. 2021	**Freedom of expression**: concern that prohibition on "incitement" may be overbroad **Privacy**: warrant requirements undermined by disproportionate exceptions; data retention mandates for content providers	No known legal challenges.
 TG	Law No. 2018-026 on cybersecurity and the fight against cybercrime adopted Dec. 2018	**Privacy**: disproportionate surveillance powers with minimal safeguards **Freedom of Expression**: vague restrictions, such as to protect morality, enable censorship	2020 ECOWAS decision called on Togo to ensure all laws align with human rights obligations to guarantee non-recurrence of the 2017 internet shutdown.

Cybercrime Laws

Country	Cybercrime Law	Impacts on Rights	Legal Challenges
 UG	Computer Misuse Act adopted in April 2011 and amended in Sept. 2022	**Freedom of expression**: overly broad restrictions on content, disproportionate penalties, and no whistleblower exceptions to unauthorized access **Privacy:** Increased data protections for children	The Constitutional Court has declared Section 25 (offensive communications) to be unconstitutional.
 TZ	The Cybercrimes Act No. 14 adopted in Sept. 2015	**Freedom of Expression:** vague prohibitions on online content, such as "false information" **Privacy:** disproportionate surveillance powers without sufficient judicial oversight	There have been several challenges since 2015, but the courts have consistently upheld the law.
 ZM	The Cyber Crimes Act No. 4 adopted in Apr. 2025	**Freedom of Expression:** vague prohibitions on online content, such as "false information" **Privacy:** vague provisions could criminalize the use of encryption and virtual private networks	Petition challenging the Act on constitutional grounds was filed in Nov. 2025.

Looking Forward: UN Cybercrime Convention

In 2024, the UN General Assembly adopted the Convention on Cybercrime. Once at least 40 State signatories ratify the treaty through their domestic processes, the Convention will go into effect. Although the aim of the Convention is to strengthen global cooperation in combating cybercrime, experts have warned that it undermines international human rights law and creates standards that facilitate a "race to the bottom" regarding privacy rights protections. Among its obligations, Parties to the Convention will be required to:

- Put into law the prohibition of cyber-dependent crimes and cyber-enabled crimes, including but not limited to, a certain crimes outlined in the Convention.
- Assist other States parties in criminal investigations when evidence or suspects of "serious crimes" are located within their territory (even if the nation's jurisdiction does not criminalize the same offense).
- Designate authorities to assist other Parties 24/7, creating a global network for cybercrime prevention.

From Africa, 22 States signed the Convention so far, five of which are examined in this report: **DRC, South Africa, Tanzania, Uganda**, and **Togo**. In all five States, domestic ratification requires additional procedural steps, so DRAA members can use this time to foster multistakeholder discussions on the implications of ratification domestically by engaging CSOs, legislators, and relevant officials to explain how the Convention will impact domestic legal obligations, human rights, and sovereignty.

Digital ID Laws

& Impact on Civic Space

Digital ID Laws: Overview

The right to legal identity (ID) is recognized under Article 16 of the ICCPR and Article 22 of the ACHPR. However, a 2022 study by the World Bank's Identification for Development (ID4D) Initiative found that roughly 850 million people globally do not have a national ID. Given that legal ID is often required to access services and exercise civic rights, such as voting, the UN has included "legal identity for all" as one of the sustainable development goals to achieve "peace, justice, and strong institutions." To address the gap, governments in Africa, with funds from the World Bank and other financial institutions, are leapfrogging forward as part of their digital transformation initiatives. The result has been the adoption of advanced digital ID systems that are equipped with biometrics intended to replace traditional ID and enable individuals to efficiently register online and use their biometric data when accessing services.

Civil society has raised three concerns with these programs.

1. When ID systems are **mandatory**, individuals who cannot access the internet, or who face other barriers, are precluded from services that require a digital form of ID. If the law also requires digital ID for **SIM card registration** (how most Africans use 4G/LTE networks), this creates a cycle of exclusion.

2. When ID systems require **biometric data**, the system must be able to withstand data breaches because a person's face and fingerprint cannot be altered if the system is hacked. A government rushing to adopt a digital ID system without robust cybersecurity capabilities puts the entire nation's sensitive personal data at risk.

3. When ID systems are deployed in countries with **weak legal systems**, the centralization of biometric data is susceptible to misuse by law enforcement if warrant requirements, oversight, and other safeguards are not in place.

Digital ID Laws: Snapshot from DRAA Countries

	 DRC	 CM	 ET	 KE	 SA	 TZ	 TG	 UG	 ZM
New Legal Framework?	Decree No. 22/07	Decree No. 2025/059	Proclamation 1284/2023	✗	✗	✗	Law No. 2020-009	Registration of Persons Act, 2015	✗
Implemented?	✗	✓	✓	Maisha Namba (on hold)	MyMzansi (in progress)	Jamii Namba (in progress)	✓	✓	INRIS System (in progress)
Mandatory Registration?	✓	✓	✗	✗	✗	✓	✗	✓	✓
Biometric Data?	✓	✓	✓	✓	✓	✓	✓	✗	✓
Is digital ID required to register a SIM?	✓	✓	?	✗	✗	✓	✓	✓	✓

Digital ID Laws: Legal Challenges

In Uganda, Section 66 of the 2015 digital ID law mandates use of national ID cards, including for purchasing SIM cards. However, by 2021, only 12 percent of Ugandans had acquired the new ID. Furthermore, civil society has expressed concern that the ID system centralizes highly personal information, including biometric data in a context without strong cybersecurity capabilities and data protection enforcement.

In April 2022, three Ugandan CSOs brought a legal challenge in April 2022 arguing that Sec. 66 violates the right to health, right to social security, and rights to equality and nondiscrimination, but the petitioners lost the case in a High Court ruling in June 2025.

In Kenya, Maisha Namba is the country's second attempt to roll out digital ID. The first attempt, initiated in January 2019, was called Huduma Namba and was immediately met with legal challenges. By January 2020, Kenya's High Court issued an order effectively putting an end to the program. The Court cited 3 main reasons for its order: 1) the high privacy risks the system posed to sensitive biometric data, 2) concerns regarding exclusion of Kenyans who may not have the necessary documentation to register, and 3) the unconstitutionality of the government collecting DNA and GPS data as part of the ID system.

Following the November 2023 launch of the new Maisha Namba system, civil society again challenged its rollout, citing similar concerns about exclusion and privacy. In 2025, the High Court ordered the government to pause implementation while it reviews the constitutionality of the system.

Looking Forward: Digital Public Infrastructure

As part of the African Union's Digital Transformation Strategy (2020–2030), digital ID is part of the drive towards a connected and modern digital future for Africa. Within this vision, digital public infrastructure (DPI) is the foundation for interoperable systems and data exchange mechanisms that will fuel digital ID, financial services, and other governmental programs.

As governments in African move towards fulfilling commitments under the Strategy and the African Digital Compact, there is an opportunity for civil society to engage to call for **transparent, inclusive, participatory, secure, and privacy protecting DPI**. Such engagement can better ensure DPI does not become an opaque tool for surveillance and exclusion. The World Bank and donors have already committed billions of dollars to developing DPI in Africa. The projects span from expanding connectivity (a necessity to ensure all people can access DPI systems) to improving digital literacy to setting up digital ID frameworks.

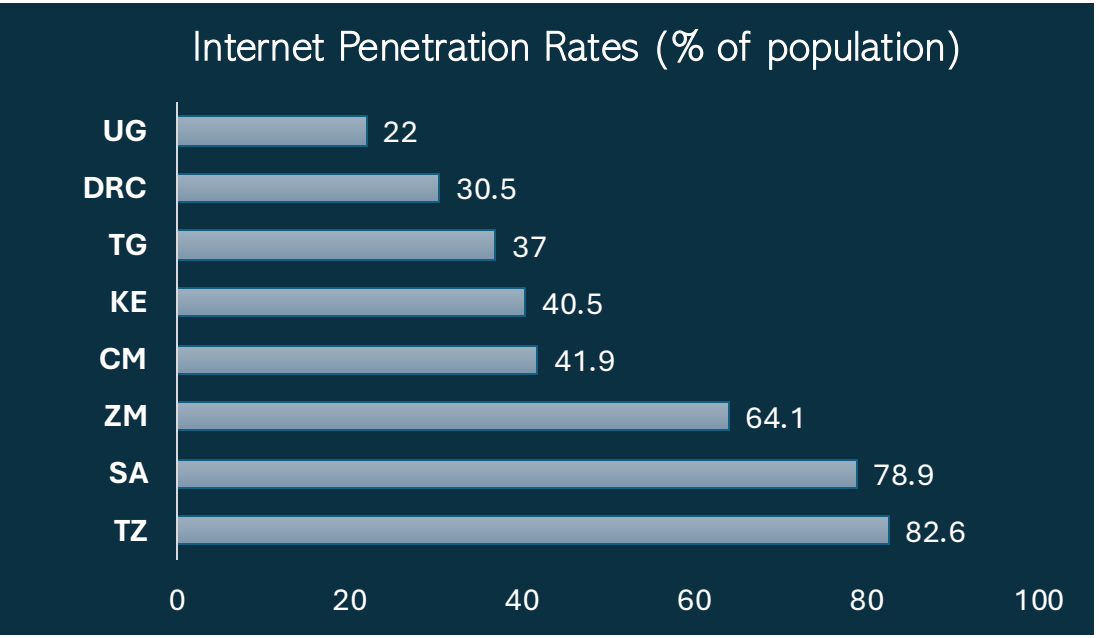
Examples of projects include:

- The Gates Foundation awarded over $75 million USD to organizations like Global Impact and the International Bank for Reconstruction and Development to support DPI-related projects in Africa in 2025.
- Since 2024, the World Bank has implemented the Digital ID for Inclusion and Services Project in Ethiopia, a $350,000 USD project to "to establish an inclusive and secure foundational digital ID system."
- The Estonian government has supported investments in Africa's DPI, like the Nam-X project in Namibia, an interoperable e-Government system modeled after Estonia's X-Road.

Deep Dive: Meaningful Internet Access

Shutdowns & Other Barriers to Access in DRAA Countries

Overview of DRAA Countries



Internet penetration rates as reported by DataReportal.

Internet penetration across Africa increased 13 percent between 2019 and 2024, the result of focused investments in internet infrastructure and last mile connectivity initiatives. Government efforts to expand connectivity varies, however, as demonstrated in the chart to the left. Moreover, the raw percentages do not reflect the principle of "meaningful internet access."

According to the International Telecommunication Union, meaningful access requires that **everyone has access "*to the Internet in optimal conditions, at an affordable cost, whenever and wherever needed*."** Within this definition there are six factors: quality of the connection; availability for use; affordability of use; availability and affordability of devices; digital literacy skills to navigate the internet; and security to ensure use is safe and secure.

DRAA members were asked to explain what the penetration rate alone cannot: is access to the internet meaningful? And what steps should their governments take to address the ITU's 6 factors for "meaningfulness"? Based on their responses, two points stand out: 1) governments must work closely with civil society and other stakeholders to achieve meaningful internet access for all and 2) the internet will never be meaningfully accessible if the government is authorized to arbitrarily disrupt access, in part or in full, without transparency or redress for the public.

Internet Shutdowns

Four DRAA countries experienced an intentional internet shutdown in 2025. All four were in the context of political unrest and conflict. In all countries but Togo, the internet has been fully restored. During the shutdowns, however, impacts were far reaching as described here.

Jun 26 - Present

Protests

Following street protests that began in the capital Lomé, three major telecommunications networks in Togo were disrupted, affecting social media and instant messaging applications and search engines.

Oct 29 – Nov 3

Post-Election Protests

The government ordered a total internet shutdown following post-election protests. According to UN human rights experts the shutdown " severely curtailed the ability of human rights defenders and journalists to carry out their work" while widespread arbitrary arrests and enforced disappearances were occurring.

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

Jan 25 - Feb 2

Conflict in Goma

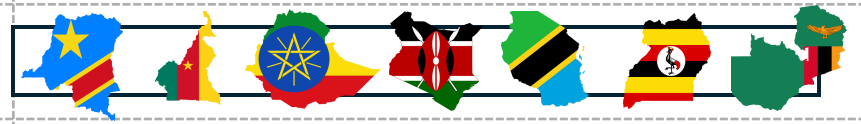
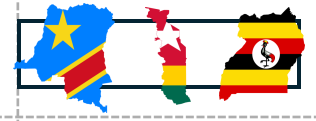
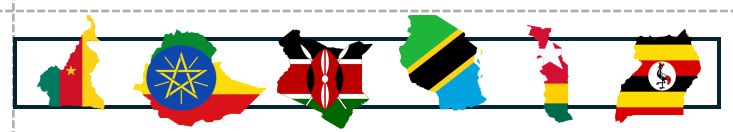
In response to the deteriorating security situation, authorities ordered a shutdown impacting millions of people. Access to information about unfolding events, what medical services were available for people wounded due to the conflict, and where to seek safety were all impacted.

Oct 23

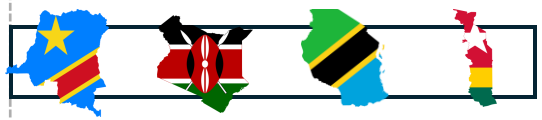
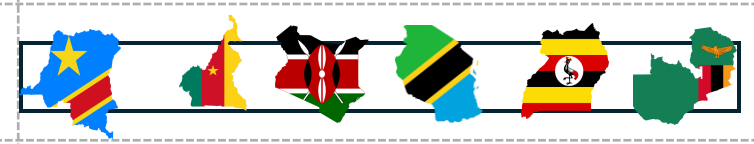
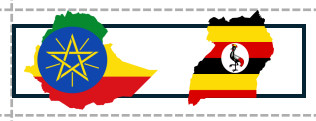
Unrest following the general election

During protests criticizing the electoral process, a shutdown impacted Yaoundé, Douala, and several other regions in the country. Due to a simultaneous lockdown imposed by armed groups, education, business operations, communication, and election campaigns were all suspended.

Barriers to Internet Access

Type of Barrier	Significant Barrier	Moderate Barrier
Lack of internet infrastructure in rural and remote areas.		
Affordability of devices to connect to the internet		
Affordability of broadband Internet		
Poor quality/reliability of internet connectivity		
Lack of internet resources in locally spoken languages		
Government shutdowns or blocking of social media and messaging apps		
Fear of the risks of cybercrime or surveillance of online activities		

Barriers to Internet Access

Type of Barrier	Significant Barrier	Moderate Barrier
Online threats targeting women, girls, and/or LGBTQ+ communities		
Accessibility of internet and devices for persons with disabilities		
Lack of knowledge about how to connect to or use internet		
Taxes on internet or social media usage		
Legal hurdles to buying/registering SIM cards		

Expanding Access: Government Efforts and CSO Recommendations

	What steps have the government taken?	What actions should the government take?
	In 2025, the government did not take tangible positive steps to improve access to the internet.	1) Invest in connectivity infrastructure. 2) Make universal service funds available to initiatives that improve connectivity in rural areas. 3) Create a favorable climate for private sector investment.
	In 2025, the government did not take tangible positive steps to improve access to the internet.	1) End orders to ISPs to disrupt internet access. 2) Increase access and affordability by repealing bandwidth taxes and providing subsidies to ISPs to expand networks. 3) Raise public awareness of digital rights and literacy.
	The government has taken some steps to liberalize the digital market; invest in infrastructure and digital literacy programs; promote affordability; seek additional resourcing from development partners; and encourage tech entrepreneurship.	1) Adopt rights-based approaches towards accessible and affordable digital infrastructure, especially in rural and remote areas. 2) Meaningfully engage civil and digital actors. 3) Address environmental sustainability as part of the digital agenda via indigenous financing schemes in climate affected communities.
	In 2025, the government did not take tangible positive steps to improve access to the internet (recent World Bank-funded initiatives are ongoing but not yet complete).	1) Ensure internet access in the whole country. 2) Improve Internet Infrastructure for easy accessibility. 3) Promote inclusion in digital transition.

Expanding Access: Government Efforts and CSO Recommendations

	What steps have the government taken?	What actions should the government take?
	The government has invested in the SA Connect program; shifted from analogue to digital TV broadcasting, thereby boosting network capacity; reallocated spectrum; and supported digital skills training in schools	1) Develop a national strategy around media and information literacy for children and adults. 2) Ensure free and accessible internet in all schools. 3) Expand zero-rating of public interest websites and essential online services.
	Togo has expanded fiber-optic and 4G/5G networks; connected rural areas with public Wi-Fi, invested $100 million in digital infrastructure; reduced device/broadband costs through partnerships; and launched large-scale digital skills training for youth and women.	1) Accelerate rural Infrastructure projects and expand fiber-optic and mobile networks to underserved rural and remote areas. 2) Subsidize devices and broadband for low-income households through targeted subsidies and voucher programs. 3) Scale free, inclusive digital literacy and skills training for youth, women, older adults, and persons with disabilities.
	The Ministry of ICT & National Guidance launched a Digital Transformation Roadmap (2023/24–2027/28), which explicitly prioritizes building digital infrastructure (broadband, data centers), promoting e-services, and investing in digital skills	1) Reduce the cost of internet. 2) Invest in nationwide fiber-optic coverage. 3) Incorporate digital literacy in the national curriculum.
	The Government has committed to the National Digital Inclusion Goal of 80% internet access by 2026, constructed new communication towers to enhance nationwide coverage, launched Zam-Free Wi-Fi, and promoted digital literacy.	1) Expand digital infrastructure and entrepreneurship 2) Review and revise laws and policy 3) Investment in digital skills and literacy

Looking Forward: USAFs

A universal service access fund (USAF) serves as a financial mechanism to increase telecommunications services by incentivizing companies to invest in underserved areas. USAFs have been used around the world to subsidize connectivity projects, such as the Rural Health Care Support program in the United States and the Digital Bharat Nidhi in India.

The International Telecommunications Union tracks USAFs globally and its tracker shows that there are 37 active USAFs in Africa. Examples of USAFs in DRAA countries include:

- **The Universal Service and Access Agency of South Africa**, which conducts annual audits and reports to the Department of Communications and Technologies with oversight by Parliament.
- **The Broadband Connectivity program in Zambia**, managed by the Information and Communications Technology Authority
- **The Digital Tanzania project** launched in 2017 to expand and upgrade cell towers.
- Other countries like Ethiopia and DRC area set to launch USAFs in coming years.

According to the United Nations, **USAFs face many challenges,** such as:

- Long delays in disbursing funds;
- Lack of coherent regulatory frameworks to facilitate disbursements;
- Lack of transparency, accountability, and inclusivity in design and management of projects;
- Lack of coordination across stakeholders;
- Uncertainty regarding sustainability of the projects when funding ends, a new government comes to power, or technologies evolve; and
- Lack of mechanisms to measure results

Civil society has an opportunity to track the implementation of these projects, call for inclusive and transparent processes, and consider how rights-based laws and regulations can support more effective and meaningful implementation of initiatives.

Deep Dive:
Data Protection Frameworks

Status of Enactment and Enforcement in DRAA Countries

Overview of DRAA Countries

In 1988, Human Rights Committee, in its General Comment interpreting the right to privacy under Article 17, stated that governments are not only obligated to refrain from unlawful and disproportionate restrictions on the right to privacy, but also to proactively protect the right to privacy by providing rights and remedies for the mishandling of personal data. Now, personal data protection laws are seen as a key enabler of civic space online.

Why does personal data protection matter? If people do not trust the safety and security of digital platforms and fear that their personal data will be mishandled or stolen without their consent or knowledge, they are less likely to use the internet to communicate and share ideas, participate in online communities and gatherings, or create accounts to receive news and information from online sources. For example, after the 2015 revelation that the company Cambridge Analytica scraped Facebook user data, engagement on Facebook deceased significantly. more broadly, global trends show that trust in the internet is in decline. While countries around the world have adopted data protection laws over the past ten years, laws alone are insufficient for people to trust that their privacy will be protected online. They must also know that that there is a data protection authority actively overseeing and implementing the law, that breaches and other violations will be handled promptly and transparently, and that the data protection authority is independent and will act fairly to adjudicate complaints.

Due to the scope of their enforcement powers, **the data protection authority's independence is crucial** to prevent abuse of power. Independence is strengthened when the executive does not direct the actions of the authority, members are appointed for a fixed term, removal of members is only based on cause, the authority is properly resourced, and transparency mechanisms enable public oversight. Moreover, the authority should be permitted to speak publicly on matters within its purview, hire its own staff, and manage its own budget.

The following table outlines the status of data protection frameworks in the nine countries under review and highlights the biggest barrier to the independence of the data protection authority. Often, implementing regulation and the realities of implementation determine the true extent of the authority's independence, but for this report, only the text of the law was examined.

Data Protection Law Enacted	✗	✓ Dec. 2024	✓ Jul. 2024	✓ Nov. 2019	✓	✓	✓ Oct. 2019	✓ May 2019	✓ Apr. 2021
Data Protection Authority Established	✗	✓ not operational	✓ not operational	✓	✓	✓	✓	✓	✓
Independence of the Authority		⚠ Section 53 provides for independence, but a presidential decree will determine its specific organization and function.	⚠ The Preamble provides for independence, but the Authority is managed by the Ministry of Innovation & Technology, an executive agency.	⚠ The Cabinet Secretary for Information, Communication and Technology has a role in the direction and operations of the Authority.	✓	⚠ It is unclear whether the President, who is responsible for appointing members of the authority, can also fire them without cause.	✓	⚠ The authority does not take direction from the Executive, but it is placed within the ICT Ministry and lacks clarity on other key issues.	⚠ The authority is not empowered to carry out essential functions and operates within and takes direction from the ICT Ministry.
Major Enforcement Actions Initiated	✗	✗	✗	✗	✓	✓	✗	✓	✗

Responses to Breaches in DRAA Countries

As the table shows, 8 of 9 countries represented in this report have standalone data protection laws. **DRC** is the only country without a standalone law, but other legal instruments, including the Telecommunications Act and the Digital Code, have data protection provisions. In 6 of the 9 countries, the data protection authority responsible for enforcing the law is operational. In countries with active data protection authorities, only three have instigated major enforcement actions. In **Zambia**, where the Office of the Data Protection Commissioner became fully operational in 2025, enforcement has so far been limited to ensuring compliance with the registration requirements. **Uganda**'s Personal Data Protection Office (PDPO) issued a major action in 2025 when it faced off with major tech giant, Google, over its handling of user data. In response to a petition filed by four Ugandans alleging that Google has unlawfully transferred their personal data out of the country, PDPO ordered Google to register as a data controller in Uganda and explain how it is complying with the cross-border data transfer rules in the Act. Google appealed but later dropped the case and agreed to register.

In theory, these types of enforcement actions should create a climate of accountability, leading to greater privacy guarantees for Africans. However, in practice, civil society still has a large role to play to oversee compliance and advocate for redress.

In **Kenya**, for example, the government rolled out its biometric-enabled digital ID system without an impact assessment or public consultations. Civil society filed a complaint alleging the system creates grave risks to personal data that could impact over 50 million Kenyans. Citing the data protection law, the High Court ordered a suspension of the system's implementation as it reviews the case.

In **Ethiopia**, a large breach in April 2025 would not have been remedied without civil society advocacy. After the names, photos, and bank details of account holders with the State-owned Commercial Bank of Ethiopia (CBE) were made public, the Bank claimed that the breach was due to a glitch in its system and not a hacking incident, denouncing public criticism of its policies and actions. It was not until an Ethiopian CSO pressured the Bank to take further action that it removed the data and provided remedies to its customers.

Looking Forward: Intersection with AI

In recent years, the world's attention has turned to the risks and opportunities of artificial intelligence (AI), a field of computer science that uses large datasets to train algorithms to identify patterns and perform a range of tasks.

Data is at the heart of AI. When AI systems are trained on personal data or are deployed to automatically make decisions about individuals, then personal data protection laws may apply. Thus, the governance of personal data and AI are interrelated and complementary. They both seek to improve transparency, fairness, and accountability in an increasingly digitized and automated world.

In 2024, the UN General Assembly adopted **the Global Digital Compact** (GDC), a framework that commits governments to making the digital space more inclusive, safe, open, and secure. The GDC establishes the Global Dialogue on AI scheduled to launch in Geneva. The **AU Digital Compact** also prioritizes strengthening AI governance and establishing oversight at national and regional levels to monitor AI developments.

The Dialogue creates an opportunity for advocacy. Although the Dialogue's format and intended outcomes are still unclear, the GDC commitments serve as a baseline to call for robust and rights-respecting data protection enforcement and AI governance, and domestic discussions before and after the Dialogue could be leveraged as catalysts for action.

Next Steps

DRAA's Plans for 2026 and Beyond

Following the publication of the report, DRAA members plan to create indicators to track changes and enforcement of cybercrime and digital ID laws, improvements or setbacks related to meaningful internet access, and developments in data protection enforcement. Additionally, members from countries that were not included in this initial report will undertake a similar baseline process and join future monitoring efforts. These countries currently include Lesotho, Liberia, Nigeria, and Zimbabwe, but could expand if members join from additional countries. The second iteration of the report will be released in early 2027.

Findings will be shared with continental policy actors including the African Commission on Human and Peoples' Rights, and Regional Economic Communities to inform their normative guidance and protection initiatives relating to restrictive cybercrime laws, regulation of DPI, etc.

DRAA members will use the report to frame their national advocacy, litigation and research initiatives. DRAA will also engage with development partners to tailor their support towards realizing the report's recommendations.

Visit our website: https://digitalrightsalliance.africa/