USAID
FROM THE AMERICAN PEOPLE

# DIGITAL REGULATION AND THREATS TO DEMOCRACY

## HOW DIGITAL LAWS OFTEN FAIL TO PROTECT DIGITAL RIGHTS IN SUB-SAHARAN AFRICA



DigitalFrontiers
SCALING DIGITAL DEVELOPMENT

DAI
Shaping a more livable world.

# TABLE OF CONTENTS

**Abbreviations** ..... **3**

**1. Introduction** ..... **4**

Purpose ..... 5

Recommendations in Brief ..... 5

**2. Defining Digital Rights and Digital Threats to Democracy** ..... **7**

**3. International Commitments to Digital Rights** ..... **9**

**4. Regional Commitments to Digital Rights in SSA** ..... **12**

**5. Limitations in the Effectiveness and Implementation of Regional Digital Rights Agreements** ..... **14**

Inconsistent progress across the continent ..... 14

Adoption does not translate into enforcement ..... 14

Weak institutional structure and capacity ..... 15

Regulatory Agencies ..... 15

Courts ..... 15

**6. Digital Regulation as a Tool for Digital Repression in SSA** ..... **16**

Internet shutdowns ..... 17

Surveillance ..... 19

Limited judicial supervision ..... 19

Role of private companies in surveillance ..... 19

Legal limits on encryption ..... 20

"Safe Cities" surveillance systems ..... 21

Censorship ..... 21

**7. Channels for Advocacy and Reform in SSA** ..... **23**

**8. Recommendations** ..... **26**

**Recommendation 1:** Assess existing and new national digital regulation through the lens of human rights ..... 26

**Recommendation 2:** Leverage multi-stakeholder collaboration, especially through multilateral and regional bodies, to build out rights-respecting digital regulation in SSA ..... 27

**Recommendation 3:** Provide technical assistance to SSA country governments to effectively implement regional agreements at the country level ..... 28

**Recommendation 4:** Engage private sector stakeholders as advocates for rights-respecting regulation and technology development ..... 29

**Recommendation 5:** Support the work of local and international CSOs ..... 29

**Annex 1: Examples of Successful Strategic Litigation** ..... **31**

In Southern Africa ..... 31

In West Africa ..... 31

In East Africa ..... 32

**Annex 2: References** ..... **33**

## ABBREVIATIONS

| | |
|---|---|
| **ACHPR** | African Commission on Human and Peoples' Rights |
| **AfCFTA** | African Continental Free Trade Area |
| **AU** | African Union |
| **CBPR** | Cross-Border Privacy Rules |
| **CIPESA** | Collaboration on International ICT Policy on East and South Africa |
| **COP** | Child Online Protection Charter |
| **CSO** | Civil Society Organization |
| **DCCP** | Digital Connectivity and Cybersecurity Partnership |
| **DPA** | Data Protection Agency |
| **EACJ** | East African Court of Justice |
| **ECOWAS** | Economic Community of West African States |
| **GDPR** | General Data Protection Regulation of the EU |
| **GNI** | Global Network Initiative |
| **GSMA** | Global System for Mobile Communications Association |
| **HRC** | United Nations Human Rights Council |
| **ICCPR** | International Covenant on Civil and Political Rights |
| **KICTANet** | Kenya ICT Action Network |
| **MISA** | Media Institute for Southern Africa |
| **NADPA** | Network of African Data Protection Authorities |
| **OTT** | Over the Top Tax |
| **RECS** | Regional Economic Communities |
| **RICA** | Related Information Act |
| **SADC** | South African Development Community |
| **SSA** | Sub-Saharan Africa |
| **UDHR** | Universal Declaration of Human Rights |
| **UNGP** | UN Guiding Principles on Business and Human Rights |
| **USAID** | United States Agency for International Development |

# 1. Introduction

The potential for digital development to accelerate progress toward development objectives is an emerging priority for USAID. National level digital regulations, policies, and legislation—such as cybersecurity, privacy, and data protection laws—are required to shape and grow thriving digital ecosystems. Governments can also use and manipulate these laws and policies to stifle digital rights, including the right to privacy, freedom of expression, freedom of association and assembly, and access to information.

The current legal and regulatory landscape presents an opportunity to both protect and exploit users of digital technology. Several international multilateral bodies have drafted frameworks that can be used to guide national legislation. The Universal Declaration of Human Rights contains principles to guide the protection of rights online and offline. In 2022, the US led the multilateral Declaration for the Future of the Internet which outlines a vision for an "Internet that is open, free, global, interoperable, reliable, and secure" and that respects human rights.[1] African regional bodies such as the African Union (AU) have demonstrated a commitment to digital rights, and have adopted instruments to guide member states in creating a legal and regulatory enabling environment for digital growth. Many national governments throughout Africa have signed and ratified these international, regional, and sub-regional agreements and instruments.

These emerging international and regional declarations and commitments acknowledge the importance of protecting digital rights, but the reality at the national level is sobering. Although a number of governments have signed on to international and regional treaties and guidelines specific to digital technology, these declarations are non-binding, and member states are not required to ratify their aspirational norms and principles. These national level institutions are often limited in their ability to regulate global private sector technology companies and platforms, many of which operate out of the United States, Europe, and Asia. Institutions in charge of implementation, such as parliaments and courts, may not have the specialized knowledge or resources to address the evolving set of issues related to the governance of digital technologies. Many government officials increasingly rely on the ambiguous language of cyber crime and data protection laws and policies to strengthen their power, infringe on privacy, detain activists, impose internet restrictions, and weaken free media and independent journalists. A bill that addresses national security or law enforcement may also allow the use of surveillance technologies. Without proper restrictions, the same laws may be used to target political opponents and stifle freedom of speech and assembly.

1 "A Declaration for the Future of the Internet," The White House, n.d., https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf.

This guide highlights both positive and negative trends and areas of concern in the evolving field of regulation of digital technologies. It is intended to help USAID staff and implementers understand how these kinds of laws can negatively affect digital rights, as well as how USAID can support the development of digital laws and regulations that protect digital rights while capturing the positive benefits of technology. USAID recognizes that the regulation of digital technology and its applications is a complex task that does not have broad consensus from the range of actors involved. It will require civil society, legal professionals, and governments to successfully adopt and enforce rules and regulations that align the development, use, and governance of technology with democratic values and respect for human rights.

## PURPOSE

USAID's Conflict, Peacebuilding and Governance division in the Africa Bureau (AFR/SD/CPG) commissioned a Landscape Assessment to inform USAID staff and partners about the links between digital development and digital threats to democracy in sub-Saharan Africa (SSA) and to examine strategies to counter its rise. This report builds on the landscape assessment, exploring how digital policy, laws, and regulations often fail to protect digital rights in SSA.

This report offers insights for USAID staff, Missions, and implementers based in SSA who may be advising governments on legislative development and implementation. It is intended to show USAID staff and implementers how laws can negatively affect digital rights, how the current governing environment (or lack thereof) has eroded democracy, and how USAID can support the adoption and implementation of laws and regulations that protect digital rights. It provides an overview of the following topics: (i) definitions of digital rights and digital threats to democracy; (ii) regional commitments to digital rights in SSA; (iii) limitations in the effectiveness and execution of regional digital rights agreements; (iv) digital regulation as a tool for digital repression in SSA; (v) channels for advocacy and reform in SSA; and (vi) recommendations for USAID.

## RECOMMENDATIONS IN BRIEF

This report and its recommendations focus on how USAID can support rights respecting policy, particularly during the process of developing, modifying, or institutionalizing digital policy with host countries or multilateral partners.

1. **Assess existing and new national digital regulation through the lens of human rights.**

   While there are some instances of digital regulation being replicated from one country to another (the European Union's General Data Protection Regulation [GDPR] has guided the creation of similar regulations across SSA), there is no universally accepted model for digital regulation that is invulnerable to authoritarian misuse and manipulation. In order to understand which digital rights restrictions are permissible under international human rights law, USAID can assess local digital regulation through the lens of international human rights law, considering the legality, legitimacy, proportionality, and necessity of digital rights restrictions (further described in the expanded recommendations on page 26) and taking into account the country context. This understanding can serve as a guardrail to ensure that digital laws that undermine democracy and encroach on human rights do not receive USAID support and funding.

2. **Leverage multi-stakeholder collaboration—especially through multilateral and regional bodies—to build out rights-respecting digital regulation in SSA.**

   Several SSA countries borrow from and often directly mirror existing regulation from the European Union—for example, GDPR, as mentioned above[2]—to quickly fill regulatory vacuums related to data protection and cybersecurity. USAID can support countries in meaningfully tailoring these models to their local country contexts, rather than copying and pasting them without consideration for local political economy, social norms, and other contextual dynamics. USAID can play a role in coordinating the efforts of various international donors, ensuring that the advice provided to SSA governments is consistent and coherent.

3. **Provide technical assistance to SSA country governments to effectively implement regional agreements at the country-level**

   SSA countries have signed onto regional agreements at the country level, such as those drafted by the African Union, but implementation of those agreements has been ineffective. This is often due to a lack of institutional capacity, financial resources, and fragmented implementation. USAID and its partners can provide technical assistance and resources directly to governments to build their capacity to execute these agreements.

4. **Engage private sector stakeholders as advocates for rights-respecting regulation and technology development.**

   USAID can support private sector entities in acquiring the necessary understanding, capacity, and resources to effectively implement improved human rights practices, expand their corporate social responsibility, and contribute to rights-respecting digital regulation and technology development that is beneficial to their business interests. USAID can also work with private sector stakeholders to take advantage of the strong relationship between industry and government decision-makers, and to push for digital regulation and laws that support digital rights and are beneficial to the business interests of industry actors.

5. **Support the work of local and international CSOs**

   CSOs throughout SSA and internationally are leading the efforts to advocate against digital threats to democracy in SSA. USAID can support these efforts through funding and capacity-building, and by creating opportunities for learning across different countries in SSA. USAID can also support CSOs engaging in awareness-raising on digital rights and hygiene, emphasizing easy steps people can take to protect their privacy and data.

More details on these recommendations can be found at the end of this paper.

2 "What is GDPR, the EU's new data protection law?" GDPR EU, n.d., https://gdpr.eu/what-is-gdpr/.

# 2. Defining Digital Rights and Digital Threats to Democracy

Understanding how legislation and regulation can affect digital rights or enable digital repression requires clear definitions for these concepts and how they are related.

**Digital rights** are human rights applied in the digital realm. This note focuses on four types of digital rights: the right to privacy, freedom of expression, access to information, and freedom of association and assembly in the digital realm.[3] The table below defines these rights in detail:

| | |
|---|---|
| **PRIVACY** | "The right of an individual or group to maintain control over, and the confidentiality of, information about themselves, especially when that intrusion results from undue or illegal gathering and use of data about that individual or group."[4]<br><br>Privacy is instrumental in securing other human rights, including the rights to freedom of speech, opinion, affiliation, and assembly. Without privacy, it is often not practical or safe to organize political opposition, or otherwise develop alternatives to existing policies, dominant narratives, or experienced injustice. |
| **FREEDOM OF EXPRESSION** | "The right to express and receive opinions, ideas and information. Expression and exchanges of views increasingly take place online, including through social media platforms, websites, and search engines."[5]<br><br>Several international legal frameworks, guiding principles, and some national laws acknowledge internet access as either a human right or as an implicit aspect of the right to freedom of expression. |
| **ACCESS TO INFORMATION** | "The right to seek, receive, and impart information held by public bodies."[6] This includes governments and affiliated institutions. Several international legal frameworks and guiding principles have established that the right of access to information extends to the internet. |
| **FREEDOM OF ASSOCIATION AND ASSEMBLY** | "[A]lthough an assembly has generally been understood as a physical gathering of people, human rights protections, including for freedom of assembly, may apply to analogous interactions taking place online… International law protects the rights to freedom of peaceful assembly and of association, whether exercised in person, through technologies of today, or through technologies that will be invented in the future."[7] |

3 "Ensuring the protection of human rights in the digital era," United Nations Office of the Secretary-General's Envoy on Technology, n.d., http://www.un.org/techenvoy/content/digital-human-rights.

4 "USAID Digital Strategy," USAID, n.d., https://www.usaid.gov/digital-development/usaid-digital-strategy.

5 "Freedom of expression online: Communications and Digital Committee report," UK Parliament House of Lords Library, October 19, 2022, https://lordslibrary.parliament.uk/freedom-of-expression-online-communications-and-digital-committee-report/#heading-1.

6 "Access to Information Laws," UNESCO, n.d., https://www.unesco.org/en/access-information-laws.

7 "Rights to freedom of peaceful assembly and of association: report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association," U.N. Digital Library, 2019, https://digitallibrary.un.org/record/3822961?ln=en&v=pdf.

USAID defines **digital threats to democracy** as "The use of digital tools and technology by the government, the private sector, or individuals to violate human rights. These include digital repression tactics such as surveillance, censorship, social manipulation and disinformation, internet shutdowns, and digitally-enabled targeted persecution, including the imposition of criminal penalties for online discourse, as noted in the 2022 Democratizing Digital Landscape Assessment."[8] The table below defines the tactics of digital repression in detail.

| | |
|---|---|
| **CENSORSHIP** | The suppression of free speech by governments or private institutions based on the assumption that said speech is objectionable or offensive. In addition to hard forms of censorship (handed down officially through laws and regulations), soft forms of censorship exist (applied through financial and/or reputational pressure).[9] |
| **SURVEILLANCE** | Observing, listening, monitoring or recording by a state, its agents, or other actors to track citizen's movements, activities, conversations, communications or correspondence, including the recording of metadata.[10] |
| **DIGITALLY-ENABLED TARGETED PERSECUTION** | The use of digital tools by governments to silence outspoken critics and groups. With much of today's political speech and activism occurring online, individuals are creating digital trails for governments to follow through the use of geolocated devices, digital payments, and social media posts detailing location-specific information, all of which can be used by governments to find and arrest citizens.[11] |
| **DISINFORMATION** | Disinformation is false information that is deliberately created or disseminated with the express purpose of causing harm. Producers of disinformation typically have political, financial, psychological, or social motivations.[12] |
| **INTERNET SHUTDOWNS** | An intentional disruption of the Internet or electronic communications that renders them inaccessible or unusable. They are often used to control the flow of information and can be partial shutdowns of certain websites or platforms, or a complete internet shutdown.[13] |

8 "Democratizing Digital How to Guide for Social Media Analytics," USAID Digital Frontiers, April 2024, https://www.digitalfrontiersdai.com/resources/democratizing-digital-how-to-guide-for-social-media-analytics/.

9 "USAID Digital Strategy, USAID, n.d., https://www.usaid.gov/digital-development/usaid-digital-strategy.

10 Tony Roberts, Abrar Mohamed Ali, Mohamed Farahat, et al., "Surveillance Law in Africa," Institute of Development Studies, 2021, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y.

11 "Digitized Autocracy Literature Review," USAID, August 2021, https://pdf.usaid.gov/pdf_docs/PA00XV9R.pdf.

12 Clair Wardle, "Information Disorder: The Essential Glossary," Harvard Kennedy School, The Shorenstein Center, July 2018, https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf; "Disinformation Primer," USAID, January 1, 2023, https://www.usaid.gov/democracy/documents/disinformation-primer.

13 "Internet shutdowns and elections handbook," Access Now, n.d., https://www.accessnow.org/guide/Internet-shutdowns-and-elections-handbook/.

# 3. International Commitments to Digital Rights

Many national level laws across SSA are rooted in widely recognized legal standards established by international organizations such as the United Nations. The rights to freedom of expression and access to information are cornerstones of modern human rights law. These rights are expanding to include internet-based freedom of expression and access to information, as well as the right to universal internet access.

## FREEDOM OF EXPRESSION ON THE INTERNET

**Universal Declaration of Human Rights (UDHR):** Article 19 of the UDHR—the foundation for modern human rights law—establishes that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[14] The UN General Assembly adopted the UDHR through a resolution, and states are not strictly bound by it. However, since its ratification in 1948, many of its articles are viewed as having gained legal authority as customary international law.

UN Committee on Civil and Political Rights General Comment no. 34: In 2011, the UN's Human Rights Committee provided new comments on Article 19 of the UDHR, stating that it "include[s] all forms of audio-visual as well as electronic and Internet-based modes of expression."[15] The internet is considered a form of expression, as Article 19 paragraph 2 protects all forms of expression and the means of their dissemination.[16]

**International Covenant on Civil and Political Rights (ICCPR):** Article 19 of the ICCPR establishes that "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[17] The ICCPR was adopted by the UN General Assembly in 1966 and entered into force in 1976.

**UN Guiding Principles on Business and Human Rights**: Governments are urged under the 2011 Guiding Principles[18] to support the protection of human rights in the business sector, including freedom of expression online and right to internet access.

14 "Universal Declaration of Human Rights," United Nations 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

15 "International Covenant on Civil and Political Rights," United Nations, September 12, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

16 "General comment No.34 on Article 19: Freedoms of opinion and expression," OHCHR, July 29, 2011, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no34-article-19-freedoms-opinion-and.

17 "International Covenant on Civil and Political Rights," OHCHR, December 16, 1966, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

18 "Guiding Principles on Business and Human Rights," OHCHR, 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

### BOX (CONTINUED): Freedom of expression on the internet

**2018 resolution of the UN Human Rights Council**: This resolution reaffirmed the importance of building trust in the internet and digital technologies with regard to freedom of expression, privacy, and other human rights, so the internet can act as an enabler for innovation, with full cooperation between governments, civil society organizations, the private sector, academia, and the technical community.[19]

## RIGHT TO INTERNET ACCESS

**The International Telecommunications Union's Constitution:** Article 33 refers to the right of the public to use international telecommunication services and stipulates the duty of governments to guarantee the exercise of this right. The internet is recognized as an international telecommunication service.[20]

**2011 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression:** This report highlights the need to adopt effective measures to achieve universal internet access. It also explicitly connects internet access to the right of freedom of expression, stating "The internet, as a medium by which the right to freedom of expression can be exercised, can only serve its purpose if States assume their commitment to develop effective policies to attain universal access to the internet."[21]

## INTERNET SHUTDOWNS AS A VIOLATION OF INTERNATIONAL HUMAN RIGHTS LAW

**UN Human Rights Council's "The promotion, protection and enjoyment of human rights on the Internet" resolution:** This 2016 resolution established that network shutdowns and other deliberate internet access limitations violated international human rights law.[22] It mandated a report that will look at the internet shutdowns trends, analyze their causes, their legal implications, and their impact on human rights.[23]

**UN Human Rights Committee General Comment No. 34:** The UN Human Rights Committee has stated that any limitations on online communication must be necessary and proportionate to accomplish a legitimate goal.[24]

Several African countries have played a role in proposing and discussing UN Human Rights Council (HRC)[25] resolutions related to digital issues. The 2021 Resolution on the right to privacy in the digital age was sponsored by Botswana, Mali, and South Africa, while Nigeria and Tunisia were among the sponsors of the 2021 Resolution on the promotion, protection, and enjoyment of human rights on the internet. Ghana, Namibia, Nigeria, and South Africa have made valuable contributions to HRC discussions on digital and human rights.[26]

---

19 "The promotion, protection and enjoyment of human rights on the Internet, "United Nations Digital Library, 2016, https://digitallibrary.un.org/record/845728?v=pdf.

20 "Constitution of the International Telecommunication Union," ITU, n.d., https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf.

21 "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," United Nations General Assembly Human Rights Council, May 16, 2011, para 60, https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf.

22 The promotion, protection and enjoyment of human rights on the Internet. UN.

23 "The promotion, protection and enjoyment of human rights on the Internet: resolution," United Nations Digital Library, accessed March 25, 2022, https://digitallibrary.un.org/record/3937534.

24 "UN Human Rights Committee: General Comment No. 34," Open Society Justice Initiative, July 21, 2011, https://www.justiceinitiative.org/publications/un-human-rights-committee-general-comment-no-34.

25 "Promotion and protection of human rights around the globe," UN Human Rights Council, n.d., https://www.ohchr.org/en/hrbodies/hrc/home.

26 Sorina Teleanu, Jovan Kurbalija "Stronger digital voices from Africa: Building African digital foreign policy and diplomacy," DiPLO, 2022, https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/.

## African lawmakers and policymakers are applying models and standards from the EU and other regions.

As countries in Africa and other developing countries rapidly digitize, they are experiencing increasing pressure to quickly adopt digital-focused laws, regulations, and policies. As of September 2021, a majority of African countries had passed some form of digital-focused regulation.[27] In many cases, these countries look to existing international models and standards to help them accelerate this process. The EU's General Data Protection Regulation (GDPR), adopted in 2016, has provided a model for other countries to follow. Several African countries, including Kenya, Rwanda, and South Africa have implemented data protection laws similar to the GDPR.[28] As the US International Trade Commission notes, "Before 2016 (the year GDPR was enacted), only 16 of 55 [African] nations had adopted specific data protection laws. As of August 2020, that number had risen to 31 countries."[29] The Privacy and Personal Data Protection in Africa Report by the African Declaration on Internet Rights and Freedoms Coalition in 2021 notes that: "inter-regional laws, such as the European Union's General Data Protection Regulation (GDPR), are more effective in shaping national legislation than instruments and conventions developed in Africa." The EU and other European donors have been pushing for alignment to these policies in Africa, particularly as they and other donors increasingly prioritize investments in digital public infrastructure such as digital ID, payments, and data-sharing systems.

The EU's new AI Act contains references to data protection, and could become another model for replication across Africa, especially since European donors like GIZ are already supporting the development of AI frameworks and policies in Africa. The AU has developed a Continental Strategy on AI, and European and multilateral donors are supporting individual SSA countries like Rwanda, Benin, Egypt, Morocco, Mauritius, Tunisia, Sierra Leone, and Senegal in developing national AI governance and strategy documents.[30]

Six SSA countries—Cabo Verde, Cameroon, Ghana, Mauritius, Nigeria, and Senegal—are parties to the Budapest Convention on Cybercrime, and eight other SSA countries and the African Union Commission maintain observer status.[31] The Malabo Convention (2014) aligns with the Budapest Convention (2001), and individual countries like Ghana and Mauritania are putting in place cybersecurity policy instruments that draw from both conventions.[32] The Malabo Convention also draws from other European standards, including the GDPR.[33]

27 Olumide Abimbola, Faten Aggad, Bhaso Ndzendze, "What is Africa's Digital Agenda?" Africa Policy Research Institute (APRI), n.d., https://afripoli.org/uploads/publications/Africas_Digital_Agenda_final.pdf.

28 "Digital rights in Africa: A brief national overview," DiPLO, n.d., https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-rights-in-africa-national-overview/.

29 Brian Daigle, "Data Protection Laws in Africa: A Pan African Survey and Noted Trends," United States International Trade Commission Journal of International Commerce and Economics, February 2021, https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf.

30 Melody Musoni, "Envisioning Africa's AI governance landscape in 2024," European Centre for Development Policy Management, January 2024, https://ecdpm.org/application/files/7017/0651/8711/Envisioning-Africas-AI-Governance-Landscape-in-2024-ECDPM-Briefing-Note-177-2024.pdf.

31 "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY," Council of Europe, n.d., https://www.coe.int/en/web/cybercrime/parties-observers.

32 "Security Policymaking: Implications of the Entry Into Force of the Malabo Convention for Digital Financial Systems in Africa," Carnegie Endowment for International Peace, July 10, 2023, https://carnegieendowment.org/2023/07/10/continental-cyber-security-policymaking-implications-of-entry-into-force-of-malabo-convention-for-digital-financial-systems-in-africa-event-8146.

33 Yohannes Eneyew Ayalew ,"The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?," June 15, 2023, https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/.

# 4. Regional Commitments to Digital Rights in SSA

African regional bodies have demonstrated a commitment to freedom of expression, freedom of association and assembly, access to information, and the right to privacy in the digital realm, and have adopted a variety of non-binding instruments to guide member states on these topics. The African Union (AU) and the African Commission on Human and Peoples' Rights (ACHPR) have spearheaded various instruments and initiatives that address concerns surrounding the safeguarding of human rights and liberties in the digital realm. (See Table 1 below.)

A key accomplishment of Africa's civil society in its fight for protecting digital rights was the drafting and passage of the African Declaration on Internet Rights and Freedoms at the African Internet Governance Forum in 2014. It calls on governments to ensure that access to the internet is "available and affordable to all persons in Africa without discrimination on any ground."[34] The declaration outlines 13 principles for the digital space, which range from safeguarding privacy and protecting data to freedom of expression and embracing cultural and linguistic diversity. The declaration also calls for legal, regulatory, and policy frameworks that align with global standards and best practices, urging African governments to ratify and implement relevant international and regional human rights treaties concerning internet rights protection. Civil society groups are encouraged to report abuses of internet rights and freedoms to international human rights bodies. As of 2023, the Declaration has received nearly 400 endorsements from organizations in 47 African countries.

**TABLE 1: SSA Regional Initiatives in Safeguarding Digital Rights[35]**

| INITIATIVE | DESCRIPTION |
|---|---|
| Economic Community of West African States (ECOWAS) Act on Personal Data Protection (2010) | Requires member states to establish national legal frameworks to safeguard data and privacy, and to create data protection authorities. An ICT accessibility policy endorsed in 2018 urges member states to guarantee digital access for everyone, including persons with disabilities.[36,37] |
| Southern African Development Community (SADC) model law on data protection (2012) | A model law on data protection was adopted by SADC in 2012, outlining rights and obligations related to protecting personal data. It was developed with support from the EU and the International Telecommunications Union, among others.[38] |

34 "African Declaration on Internet Rights and Freedoms, Principle 2," African Internet Rights, n.d., https://africaninternetrights.org/.

35 National-level ratifications, proclamations, policies, laws, regulations, agencies, coordination committees, etc. can change rapidly. For up-to-date information, see the following resources: https://dataprotection.africa/; https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-rights-africa-continental-regional-policies-initiatives/; https://www.africandigitalrightsnetwork.org/.

36 "Draft ECOWAS ICT Accessibility Policy (2018) v1post Burkina Faso and Gambia Workshop," ICT Policy Africa, 6, September 25, 2019, https://ictpolicyafrica.org/en/document/0kgv8x4u0pd?page=6.

37 "African Bodies: ECOWAS Act on Personal Data Protection," One Trust Data Guidance, November 2021, https://www.dataguidance.com/opinion/african-bodies-ecowas-act-personal-data-protection.

38 "Southern African Development Community (SADC) Model Law," ITU, 2013, https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.

## TABLE 1 (CONTINUED): SSA Regional Initiatives in Safeguarding Digital Rights

| INITIATIVE | DESCRIPTION |
|---|---|
| African Union Convention on Cybersecurity and Personal Data Protection (the Malabo Convention, 2014) | Signatories "commit [themselves] to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and to punish any violation of privacy without prejudice to the principle of free flow of personal data."[39] Fourteen out of 55 states in the AU have signed the Convention, and only 13 have ratified it. It entered into force in June 2024, nine years after it was adopted.[40] |
| Network of African Data Protection Authorities (NADPA) (2016) | Promotes cooperation and sharing of experiences among privacy and data protection authorities from 19 countries. The network also supports states in preparing legislation on privacy and data protection, establishing data protection agencies (DPAs), and implementing relevant African legal instruments. It collaborates with African and international bodies and associations, such as the Global Privacy Assembly and the Global Privacy Enforcement Network.[41] |
| ACHPR Resolution on the Right to Freedom of Information and Expression on the Internet (2016) | Calls on countries to guarantee, respect, and protect citizens' right to freedom of information and expression through access to Internet services. |
| African Union Declaration on Internet Governance (2017) | Upheld the AU's commitment "to establish a global, transparent and inclusive framework of Internet governance based on openness principles, including…respect and protection of private life" and "Ensuring, to all, the right for using Internet in a manner that respects privacy, without prejudice to the necessary limitations prescribed by the requirements of public safety, the fight against cybercrime, violent extremism, and terrorism." |
| ACHPR Guidelines on Freedom of Association and Assembly in Africa (2017) | According to these Guidelines, "[t]he right to assembly may be exercised in a number of ways, including…through the use of online platforms, or in any other way people choose"[42] |
| ACHPR Guidelines on Access to Information and Elections in Africa (2017) | Notes that regulatory bodies should refrain from shutting down the Internet during electoral processes. In exceptional cases where shutdowns may be permissible under international law, such limitations must be authorized by law, serve a legitimate aim, and be necessary and proportional in a democratic society. |
| ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) | Lays out a set of principles related to Internet access, freedom of expression online, the right to anonymity, and the right to privacy and data protection in the digital space. |
| ACHPR Resolution on Internet Shutdowns and Elections in Africa (2024) | Directs countries to "take the necessary legislative and other measures to ensure open and secure Internet access before, during, and after elections, including ensuring that telecommunications and Internet service providers take adequate steps to provide unrestricted and uninterrupted access" |

39 "African Union Convention on Cyber Security and Personal Date Protection," African Union, June 27, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

40 Yohannes Eneyew Ayalew, "The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?," EJIL: Talk! June 15, 2023, https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/.

41 "Digital rights in Africa: A brief national overview," DiPLO, n,d, https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-rights-in-africa-national-overview/.

42 "Guidelines on Freedom of Association and Assembly in Africa," African Commission on Human and Peoples' Rights, September 21, 2017, https://achpr.au.int/index.php/en/soft-law/guidelines-freedom-association-and-assembly-africa.

# 5. Limitations in the Effectiveness and Implementation of Regional Digital Rights Agreements

## INCONSISTENT PROGRESS ACROSS THE CONTINENT

The international and regional commitments referred to above represent a step in the right direction of protecting digital rights on the continent, but the effectiveness and execution of these instruments has been severely limited. International and regional adoption of policies and laws have not successfully pressured governments to pass progressive privacy legislation, and progress to date has been inconsistent across SSA countries. Despite Kenya's regional and international commitments, Kenyan law does not adequately protect children's privacy rights. Ethiopia, on the other hand, has not yet joined any of the continent's data protection agreements, but it has taken the initiative to publish a Draft Personal Data Protection Proclamation. Thirty-six of the 54 African nations had data protection laws in place as of 2023.[43]

## ADOPTION DOES NOT TRANSLATE INTO ENFORCEMENT

Some SSA governments adopt regional treaties and guidelines, but they do not always bring national laws into compliance or adequately implement them. The high-profile declarations adopted by the AU are non-binding, and AU member states are not required to implement them. In 2014 and 2015, the ACHPR adopted guidelines that reaffirm its commitment to freedom of expression and access to information. Numerous international observers believe that some SSA governments accepted these regional treaties in response to international pressure, rather than out of a genuine desire to pursue such policies at home.[44] The Malabo Convention has only been ratified by 15 African countries, indicating that there is no continent-wide consensus on data protection and cybersecurity issues.

43 "Africa Privacy Report 2023/2024," Lawyers Hub: Tech for Justice, January 2023, https://www.lawyershub.org/Digital%20Resources/Africa%20Privacy%20Report%202023-24/Africa%20Privacy%20Report%202023-2024.pdf.

44 Africa Privacy Report.

## WEAK INSTITUTIONAL STRUCTURE AND CAPACITY

### Regulatory Agencies

Despite the growing number of SSA countries with formal data privacy laws, institutions in charge of regulating data governance have not changed to meet the evolving needs of the digital realm. Fifteen SSA countries with data protection laws have data protection agencies (DPAs) in place to enforce these laws. However, the full efficacy of these DPAS is constrained by fragmented implementation and their inadequate financial and human resources, lack of institutional capacity,[45] and power and information asymmetry between digital platforms and resource-constrained SSA countries.[46] As of 2023, DPAs in six African countries had issued only six major data privacy fines.[47] The situation is further exacerbated by a lack of capacity among judges and lawyers.

### Courts

Many judges are not trained in these relatively new laws and how they should be applied in order to protect human rights in the digital space, and many lawyers do not have as much experience in prosecuting and defending strategic litigation cases related to human rights in the digital space.[48]

45 Tomiwa Ilori, "Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions," African Internet Rights, n.d., https://africaninternetrights.org/sites/default/files/Tomiwa%20Ilori_AfDec_Data%20protection%20in%20Africa%20and%20the%20COVID-19%20pandemic_Final%20paper.pdf.

46 Adedeji Adeniran, "Developing an effective data governance framework to deliver African digital potentials," Brookings, March 21, 2022, https://www.brookings.edu/blog/africa-in-focus/2022/03/21/developing-an-effective-data-governance-framework-to-deliver-african-digital-potentials/amp/.

47 Africa Privacy Report.

48 "Data & Digital Rights in Nigeria: Assessing the activities, issues and opportunities," Luminate Group, n.d., https://luminategroup.com/storage/1361/Data-%26-Digital-Rights-in-Nigeria-Report-%5BFINAL%5D.pdf.

# 6. Digital Regulation as a Tool for Digital Repression in SSA

A more concerning trend at the country level besides a lack of resources is that many SSA countries are using digital laws and regulations to infringe on digital rights. Government officials increasingly rely on the ambiguous language of cybercrime and data protection laws and policies to strengthen their power, detain activists, impose internet restrictions, and weaken free media and independent journalists. These measures often violate the right to privacy, freedom of expression, freedom of association and assembly, and access to information online, even though they are legitimized through laws and regulations.[49] The key aim of these laws is to suppress dissent and differing opinions, limiting open online discourse. Digital policies, laws, and regulations are prone to abuse in contexts where incumbent or authoritarian governments seek to rule by law, using a range of quasi-legal tactics to justify closing political space. Oppressive measures in the digital realm are often justified as necessary to combat terrorism, organized crime, and secessionist violence.

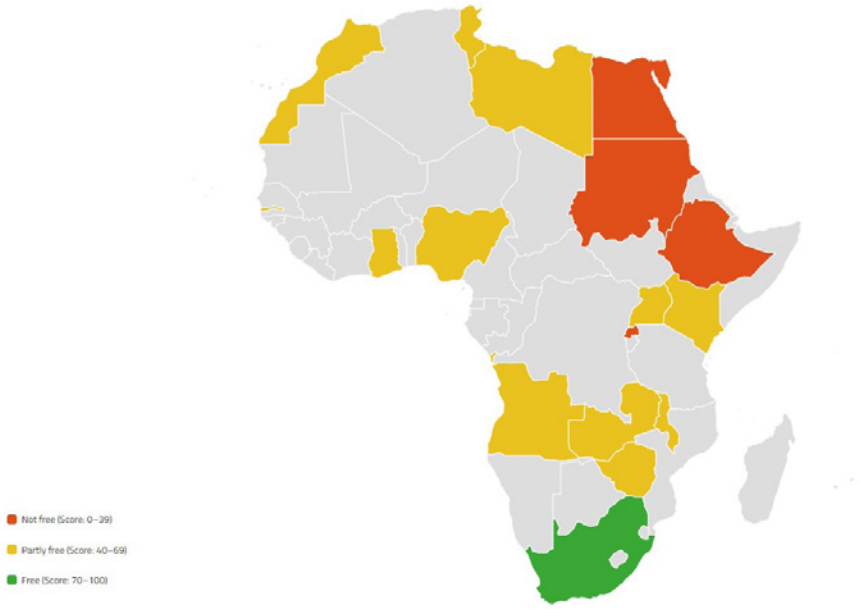
Studies have shown that increased interference with digital rights in SSA occurs predominantly in countries with inadequate oversight mechanisms. This has led to data breaches, personal data misuse, unlawful and indiscriminate interception of online communications, and unauthorized data retention policies led by government authorities, as well as internet shutdowns and silencing of journalists and political opponents.[50] Women, including female politicians and journalists, are often disproportionately affected in repressive environments and there are few laws to protect them online. Furthermore, legally restrictive environments often serve to repress and silence CSOs who are key advocates for the protection of digital rights. Without proper safeguards, data protection, cybersecurity, and digital surveillance laws can enable digital repression by imposing overly broad restrictions on human rights in the digital realm.

49 Nathaniel Allen, Catherine Lena Kelly, "Deluge of Digital Repression Threatens African Security," Africa Center for Strategic Studies, January 4, 2022, https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/.

50 Murray Hunter, Admire Mare, "A Patchwork For Privacy: Mapping communication surveillance laws In southern Africa," Media Policy and Democracy Project, June 5, 2020, https://archive.org/details/patchwork-for-privacy-communication-surveillance-in-southern-africa. Also see note 2.

As a result, internet freedoms in SSA are severely limited, broadly speaking. Freedom House's Freedom on the Net report[51] assesses various factors such as barriers to internet access, content restrictions (filtering, blocking, and other censorship methods), and violations of user rights (legal protections and restrictions on freedom of expression, privacy and surveillance, and consequences for online speech and activities). See Figure 1 for the results of the 2022 report, which includes 17 African countries. The 2023 study by the Agence Francaise de Developpement (AFD) on digital freedoms in French-speaking African countries listed only Seychelles and Mauritius out of 26 countries as "free."[52]

**FIGURE 1: Internet freedom in Africa**




*Source: DiploFoundation (2023), available at: https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-rights-in-africa-national-overview/.*

Trends highlight three key tactics of digital repression in SSA: internet shutdowns, surveillance, and censorship.

## INTERNET SHUTDOWNS

SSA governments often violate digital rights by implementing full and partial internet shutdowns.[53] The ACHPR stated in 2016 that internet shutdowns were not permissible under international human rights law even during armed conflict,[54] and yet more than 30 African countries have cut off their internet connections over the past two decades.[55] According to Access Now, Africa had at least 25 internet shutdowns in 2019 and 18 in 2020.[56]

51 "Freedom on the Net," Freedom House, n.d., https://freedomhouse.org/report/freedom-net.

52 "Digital Freedoms in French-Speaking African Countries," Agence Française de Développement (AFD), May 2023, https://www.afd.fr/en/ressources/digital-freedoms-french-speaking-african-countries.

53 "Government Internet Shutdowns Have Cost $53 Billion Since 2019," Top 10 VPN, n.d., https://www.top10vpn.com/cost-of-Internet-shutdowns/.

54 "362: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa – ACHPR/Res.362," OAS, 2016, https://www.achpr.org/sessions/resolutions?id=374.

55 Tomiwa Ilori, "Life interrupted. Centering the social impacts of network disruptions in advocacy in Africa," Global Network Initiative, 2021, https://globalnetworkinitiative.org/wp-content/uploads/2021/03/Life-Interrupted-Report.pdf. "Internet Shutdowns in Africa: Addressing the Human Rights Responsibilities of Telecommunication Companies," Business & Human Rights Resource Centre, March 2022, https://www.business-humanrights.org/documents/37422/2022_Africa_Internet_Shutdowns_Briefing.pdf.

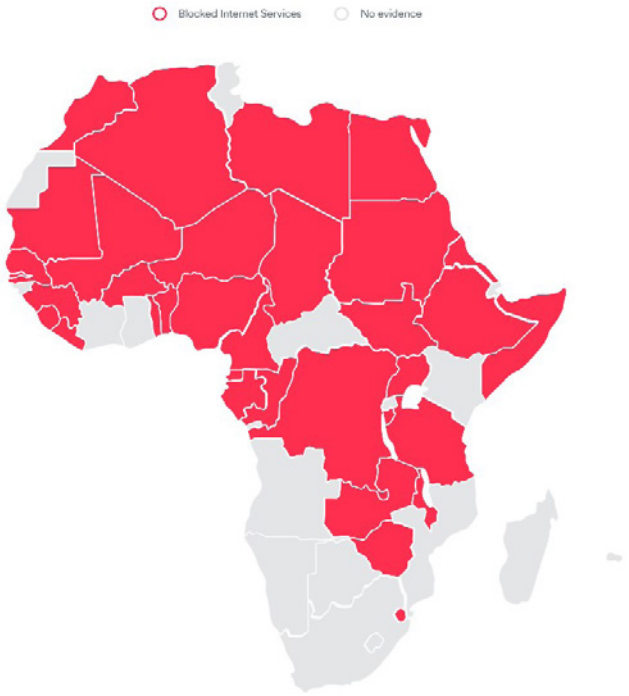
56 "Targeted, Cut Off, and Left in the Dark: The #KeepItOn report on Internet shutdowns in 2019," KeepItOn, 2019, https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.

### Case Study: Ethiopia

Internet users in Ethiopia are officially entitled to some fundamental freedoms, but these rights are frequently violated. Ethiopia's Council of Ministers imposed a six-month official state of emergency in Tigray in November 2020, cutting off Tigray's access to ICT infrastructure.[57] Its internet connectivity was partially restored 2.5 years later, beginning in February 2023,[58] making it one of the longest internet shutdowns in the world.[59]

Surfshark, an online platform that tracks internet shutdowns worldwide, shows that 53 percent of all internet shutdowns worldwide since 2015 have occurred in Africa.[60] (See Figure 2 below.) These shutdowns often occur around high profile or controversial political events. Internet shutdowns have occurred around contentious elections in Uganda, Niger, the Republic of the Congo, and Guinea, while civil unrest in Togo, Eswatini, Senegal, Burkina Faso, and Sudan has also prompted shutdowns.

**FIGURE 2: Where has the internet been restricted in Africa since 2015?**




*Source: https://surfshark.com/research/Internet-censorship*

57 "Freedom on the Net: Ethiopia," Freedom House, 2021, https://freedomhouse.org/country/ethiopia/freedom-net/2021.

58 "After years in the dark, Tigray is slowly coming back online," Access Now, March 17, 2023, https://www.accessnow.org/tigray-shutdown-slowly-coming-back-online/.

59 Fred Harter, "Record number of countries enforced Internet shutdowns in 2022 – report," The Guardian, February 28, 2023, https://www.theguardian.com/global-development/2023/feb/28/Internet-shutdowns-record-number-countries-2022-report.

60 "Internet shutdown tracker," Surfshark, n.d., https://surfshark.com/research/Internet-censorship.

## SURVEILLANCE

A frequent digital repression tactic used in many SSA countries is surveillance. Justifications for surveillance in many SSA countries are extremely broad, including national security, crime investigation, prevention of terrorism, and acts that endanger public peace and order. Many offenses are undefined or poorly defined, allowing state authorities to surveil critics and opponents through a broad interpretation of the law.[61] Under these laws, online criticism on nearly any subject may constitute an offense if the authorities consider it a threat to the national interest or to public safety.

### Limited judicial supervision

Laws that impose digital surveillance measures are not subject to judicial supervision in many SSA countries. These countries typically have few independent oversight bodies that monitor law enforcement's use of digital surveillance. Investigating authorities often do not issue public reports on activities related to digital surveillance.[62] In certain SSA countries, digital surveillance operations are exclusively carried out and monitored by entities within the executive branch, bypassing parliaments and courts. Security agencies in Nigeria can gain legal access to a database of internet and mobile subscribers without judicial checks and balances.[63] In Lesotho, the minister responsible for the National Security Services can issue interception warrants; in Niger, interception is requested by the President. In South Sudan, this role falls under the purview of the Director General of the National Security Service, while in The Gambia it resides with the Minister of Interior. In Togo, the Prime Minister and the ministers responsible for defense, economy and finance, justice, and civil protection can activate digital surveillance.[64] Individuals subjected to government-sponsored digital surveillance are not notified about it or afforded the right to appeal.

61 Evelyn Lirri, "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa," CIPESA, August 16, 2022, https://cipesa.org/2022/08/privacy-imperilled-analysis-of-surveillance-encryption-and-data-localisation-laws-in-africa/.

62 "Surveillance Law in Africa: a Review of Six Countries," Institute of Development Studies, October 2021, https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/16893. Tony Roberts, "Surveillance laws are failing to protect privacy rights: what we found in six African countries," The Conversation, October 21, 2021, https://theconversation.com/surveillance-laws-are-failing-to-protect-privacy-rights-what-we-found-in-six-african-countries-170373.

63 Surveillance Law in Africa. IDS.

64 Evelyn Lirri. Privacy Imperiled.

## Role of private companies in surveillance

Governments increasingly rely on private companies for surveillance technology. According to 2020 research from the University of Toronto's Citizen Lab, government agencies in Kenya, Nigeria, Zambia, and Zimbabwe have purchased spyware from Circles[65] whose technologies allow users to monitor calls, texts, and cellphone geolocation.[66] Certain governments in SSA have asked technology companies operating locally for access to the metadata of specific individuals.[67] Tanzania has made continuous appeals to tech companies like Vodacom for metadata,[68] and similar requests for data have been made by governments in Chad and Rwanda.[69] According to Freedom House, the Nigerian government set aside 2.2 billion naira ( USD 6.6 million) in their 2018 budget for a "Social Media Mining Suite," and has instructed the military to monitor online activity for any content that may be considered anti-government. This has led to an increase in arrests for internet-related offenses in the country. Nigerian human rights and democracy activist Ibrahim Garba Wala was given a 12-year prison sentence in April 2019 for criminal defamation, public incitement, and unlawful assembly on charges related to Facebook posts in which he alleged corruption in the National Hajj Commission. According to reports, Israeli firms Verint and WebIntPro have provided similar surveillance software to Angola and Kenya.[70]

Some cyber crime laws require internet service providers to retain users' data, including phone calls, text messages, browsing history, and app usage, for up to 180 days, and allow law enforcement access to this data without adequate human rights protections. The lack of legal precision and safeguards allows government authorities to circumvent these laws. This is often exacerbated by a weak civil society sector and inadequate judicial checks and balances on law enforcement agencies.[71]

## Legal limits on encryption

Some SSA countries have laws that limit the use of encryption. Citizens use encryption to maintain their right to privacy while protecting their data. This right is under threat in a number of SSA nations where regulations have been put in place that force encryption service providers to register, prohibit specific encryption methods, and demand that service providers turn over decrypted data.[72] In the Democratic Republic of the Congo, the Central African Republic, Niger, Benin, Ivory Coast, Togo, and Burkina Faso, authorization may be required if encryption is used for purposes other than authentication and integrity management. Failure to acquire authorization can result in a significant fine, imprisonment, or both.[73] Service providers in Mali, Tanzania, and Malawi must disclose the use of specific encryption software. [74]

---

65 Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, et al, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles," University of Toronto, The Citizen Lab, December 1, 2020, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

66 Bill Marczak. Running in Circles.

67 Abdi Latif Dahir, "Tanzania's government is casting itself as the nation's sole custodian of data," Quartz Africa, September 13, 2018, https://qz.com/africa/1389147/tanzanias-magufuli-bans-data-publication-without-government-ok/.

68 Alex Boniface Makulilo, "Analysis of the regime of systematic government access to private sector data in Tanzania." Information & Communications Technology Law 29, no. 2, 250-278, March 28, 2020, https://www.tandfonline.com/doi/abs/10.1080/13600834.2020.1741156.

69 "Privacy and data protection in the Digital Era: Challenges and Trends in Africa," CIPESA, September 2018, https://cipesa.org/?wpfb_dl=278.

70 Adrian Shahbaz, Allie Funk "Social Media Surveillance," Freedom House, 2019, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance.

71 Juliet Nanfuka, "Data Privacy Still A Neglected Digital Right in Africa," CIPESA, January 27, 2022, https://cipesa.org/2022/01/data-privacy-still-a-neglected-digital-right-in-africa.

72 Juliet Nanfuka. Data Privacy.

73 Juliet Nanfuka. Data Privacy.

74 Juliet Nanfuka. Data Privacy.

### Case Study: How Broad justifications for Digital Surveillance in the Controversial Southern African Development Community (SADC) Model Law on Cyber Crime Can Impinge Upon the Right to Privacy

In response to a 2008 African Union framework to harmonize telecommunications and ICT policies across the continent, SADC launched a model law on cyber crime for its member states in 2012 and adopted it in 2013. Several studies note that aspects of the model law violate the fundamental right to privacy. Section 25 addresses issues related to the search and seizure of electronic equipment believed to have been used to commit a crime or to contain evidence of the commission of a crime. Critics are concerned that warrants issued for computer searches under Section 25 are so broad that law enforcement can use a single warrant to search all devices connected to a network.

Prior to the approval of the SADC Model Law in 2013, SADC member states such as Mauritius and Botswana already had national cybercrime legislation in place, in some cases based on international cybercrime treaties and laws. These earlier laws are generally less likely to violate the right to privacy, in comparison to national cybercrime laws modeled on the controversial SADC Model Law.

## "Safe Cities" surveillance systems

"Safe Cities"[75] surveillance systems often encroach on digital human rights. In Botswana, Kenya, Nigeria, Uganda, Zambia, and Zimbabwe, government authorities have made substantial investments in state-run video surveillance systems popularly known as "Safe Cities." These initiatives are concerning because their provisions for collection and processing of personal data lack adequate regulatory safeguards.[76] In 2019, Kampala police invested USD 126 million in CCTV facial recognition surveillance equipment from Huawei to allegedly combat an escalating crime problem. Opposition and civil society leaders have noted that, in reality, this technology is used to track down political opponents. A third-party investigation revealed that Ugandan intelligence agents were decrypting the encrypted communications of Bobi Wine, a popular singer and member of the opposition. This concern appears to have merit.[77]

75 Bulelani Jili, "The Spread of Surveillance Technology in Africa Stirs Security Concerns," Africa Center for Strategic Studies, December 11, 2020, https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/. "U.S.-China Relations in 2020: Enduring Problems and Emerging Challenges," Hearing on U.S.-China Relations in 2020: Enduring Problems and Emerging Challenges, U.S.-China Economic and Security Review Commission, September 9, 2020, https://www.uscc.gov/hearings/us-china-relations-2020-enduring-problems-and-emerging-challenges. The Safe Cities concept uses a variety of networked tracking devices, video cameras, software, and cloud storage systems to tap public and private platforms more cohesively and improve public services including policing and traffic management and streamlining administrative services. Visibility is supposedly increased for police officers by providing them with access to this network of systems, allowing them to quickly track down and address criminal activity.

76 Juliet Nanfuka, "Data Privacy Still A Neglected Digital Right in Africa," CIPESA, January 27, 2022, https://cipesa.org/2022/01/data-privacy-still-a-neglected-digital-right-in-africa/.

77 Bulelani Jili. The Spread of Surveillance.

## CENSORSHIP

The final digital repression tactic used in SSA is censorship that infringes on both freedom of expression and access to information. SSA governments increasingly misuse laws on national security, public order, public morality, data protection, digital surveillance, and cybersecurity and anti-terrorism to restrict freedom of expression. Government officials are more frequently relying on ambiguous language about national security concerns, mis- and disinformation, online hate speech, and combating fraud in cybercrime and data protection laws and policies to strengthen their power, detain activists, and weaken free media and independent journalists. These measures impinge upon human rights and contravene international criteria for legitimate restrictions on digital rights, even though such restrictions have been legitimized through laws and regulations.[78] Governments can intentionally label genuine political critique as disinformation, enabling authorities to frame prosecution as a defense of free speech.[79]

### Case Study: Kenya

Despite Kenya's vibrant digital ecosystem, its Computer Misuse and Cybercrimes Act of 2018 effectively restricts free speech online.[80] The Act outlaws the dissemination of fraudulent publications, which include false, misleading, or fabricated facts or misinformation with the goal that the data be evaluated or acted upon, as well as the dissemination of false material that is intended to cause fear, disorder, or violence, or that is likely to discredit a person.[81] The Government of Kenya has arrested several bloggers for violating this law. A 23-year-old student named Elijah Kitonyo was arrested in 2020 for tweeting that the government was misleading the public about the COVID-19 situation in the country.[82] In the same year, blogger Robert Alai was detained and charged under the Act for disseminating false and disturbing information on Twitter, claiming that two individuals in Mombasa had died from COVID-19.[83] These two arrests exemplify the regional trend of using cybersecurity laws to persecute outspoken citizens and activists.

Some countries in SSA are effectively censoring citizens' right to freedom of expression and information by implementing laws and policies that limit internet usage, such as taxes on social media usage. African governments in countries such as Kenya, Nigeria, and Uganda have started taxing social media, e-commerce, and mobile money usage as a means of increasing state revenues, in response to the growing popularity of digital services such as WhatsApp. These rules effectively reduce internet usage, infringing on freedom of expression and access to information. SSA governments have also tightened information control by blocking specific online platforms that do not comply with their directives.

78 Nathaniel Allen, Catherine Lena Kelly, "Deluge of Digital Repression Threatens African Security," Africa Center for Strategic Studies, January 4, 2022, https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/.

79 James Lynch, "Middle East and North Africa Iron net: Digital repression in the Middle East and North Africa," European Council on Foreign Relations, June 29,2022, https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/.

80 The Computer Misuse and Cybercrimes Act of 2018," National Computer and Cybercrime Coordination Committee, May 30, 2018, https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act/.

81 The Computer Misuse and Cybercrimes Act of2018.

82 Amina Wako, "Coronavirus: Detectives arrest man spreading falsehoods," Nation Media Group, March 24, 2020, https://www.nation.co.ke/news/DCI-arrests-man-over-COVID-19-tweet/1056-5492720-bgpj5kz/index.html.

83 Siago Cece, "Blogger Alai to be charged over 'alarming coronavirus post'," Nation Media Group, March 24, 2020, https://www.nation.co.ke/kenya/news/blogger-alai-to-be-charged-over-alarming-coronavirus-post--280580.

### Case Study: Uganda

In 2018, Uganda imposed a 200-shilling (USD 0.05) daily tax on the use of "over the top" (OTT) mobile communication apps, such as social media, messaging apps, and dating apps.[84] As a result, Uganda lost five million internet memberships within the first year of the OTT tax implementation[85] and the number of Twitter users decreased by 13 percent.[86] The tax was later replaced with a 12 percent levy on internet data,[87] which is expected to have similar effects.[88]

84 "Taxing Social Media in Africa," Internet Health Report, 2019, https://Internethealthreport.org/2019/taxing-social-media-in-africa/.

85 Taxing Social Media.

86 "African governments hope digital taxes will fill a budget hole," The Economist, October 13, 2022, https://www.economist.com/middle-east-and-africa/2022/10/13/african-governments-hope-digital-taxes-will-fill-a -budget-hole.

87 Edrine Wanyama, "Advancing Collaborations in Strategic Litigation for Digital Rights in East Africa," CIPESA, January 28, 2020, https://cipesa.org/2020/01/advancing-collaborations-in-strategic-litigation-for-digital-rights-in-east-africa/. Dunia Mekonnen Tegegn, "Advancing Strategic Litigation on Internet Shutdowns cases in Africa: Promises and Pitfalls," CIPESA, n.d., https://cipesa.org/?wpfb_dl=462.

88 "Uganda introduces 12% Internet data levy, critics say move will stifle online access," Reuters, April 30, 2021, https://www.reuters.com/world/africa/uganda-introduces-12-Internet-data-levy-critics-say-move-will-stifle-online-2021-04-30/.

# 7. Channels for Advocacy and Reform in SSA

In SSA, stakeholders such as CSOs, academia, private sector companies, and the media are vital in the effort for reform because they can collaborate with or pressure their governments to maintain and protect digital rights. While the incentives for various actors may differ, together they can provide channels for advocacy and reform in SSA, especially to preserve digital rights.

Civil society can exercise vital checks and balances on digital threats to democracy in sub-Saharan Africa. Civil society has raised red flags in multiple countries about the roll-out of high-risk technologies, such as biometric registration, compulsory SIM registration, and CCTV surveillance.[89] Civil society played a key role in the passage of South Africa's recent Cybercrimes Act and the Protection of Personal Information (POPI) Act 2020,[90] which clearly defines the term "cyber crimes".[91] High profile civil society groups from across the continent protecting the right to online privacy include:

- Kenya ICT Action Network (KICTANet): A network of experts and civil society activists that convenes digital policy dialogues with government and security sector officials.[92] Their work has influenced the content of key cybersecurity laws and policies.[93]
- MISA Zambia and the Bloggers of Zambia: These organizations serve as watchdogs for digital rights protection.
- Unwanted Witness: A CSO created in 2012 in Uganda to promote online freedoms and safeguard digital rights. The organization's mission is to foster a safe and secure digital environment for Ugandans and to encourage the appropriate use of technology.[94]

89 Nathaniel Allen, Catherine Lena Kelly, "Deluge of Digital Repression Threatens African Security," Africa Center for Strategic Studies, January 4, 2022, https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/. Tony Roberts, Abrar Mohamed Ali, Mohamad Farahat, et al., "Surveillance Law in Africa: a review of six countries," Brighton: Institute of Development Studies, October 21, 2021, https://www.ids.ac.uk/publications/surveillance-law-in-africa-a-review-of-six-countries/.

90 Karen Allen, "South Africa Lays Down the Law on Cybercrime," Institute for Security Studies, June 9, 2021, https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.

91 Nathaniel Allen, Catherine Lena Kelly, "Deluge of Digital Repression Threatens African Security," Africa Center for Strategic Studies, January 4, 2022, https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/.

92 "Kictanet 2022 Annual Report," Kictanet, 2022, https://www.kictanet.or.ke/.

93 Nathaniel Allen. Deluge of Digital Repression.

94 "Unwanted Witness: About Us," Unwanted Witness, n.d., https://www.unwantedwitness.org/about/.

### Case Study: Nigeria

In 2021, the Government of Nigeria used the Cybercrimes Act as the basis for banning Twitter countrywide.[95] In 2022, several Nigerian NGOs submitted a case to the Community Court of Justice of the Economic Community of West African States (ECOWAS Court), contesting several sections of the Cybercrimes Act that they claimed were vaguely worded, unclear, and unlawful and stating that they violated Nigerians' right to freedom of expression and information.[96] As a result, ECOWAS ordered Nigeria to modify the Cybercrimes Act.

Strategic litigation has gained popularity as a way for citizens and civil society to push back against limitations on the fundamental human right to privacy in the digital environment. Strategic litigation can result in significant legal precedents by revealing inequities, publicizing human rights violations, and increasing awareness of and bringing about legislative, policy, and practice preforms. The case study below and Annex 1 offer examples of how strategic litigation has been used to protect digital rights across SSA.

### Case Study: Zambia

After the Zambia Information and Communications Technology Authority (ZICTA) disabled WhatsApp, Facebook, Twitter, and Messenger on the day of Zambia's 2021 general election, a Chapter One Foundation lawsuit led to an injunction. As a result, access to all platforms was restored after two days.[97] ZICTA stipulated in the court settlement and consent ruling on March 21, 2022, that it would refrain from acting in the future to obstruct internet access or flow outside of its legal authority or control and pledged to inform the general public of any internet shutdowns within 36 hours.[98] The Government of Zambia appears to have abandoned an August 2018 proposal to tax messaging apps like WhatsApp, Skype, and Messenger at 30 ngwee a day due to the vehement objections of civil society and social media users.[99]

95 "Information Minister and the Twitter Ban," LEGIST, Policy and Legal Advocacy Centre, June 29, 2021, https://placng.org/Legist/information-minister-and-the-twitter-ban/.

96 "ECOWAS Court orders Nigeria to align its Cybercrime Law with its international obligations," Media Foundation for West Africa, March 28, 2022, https://www.mfwa.org/ecowas-court-orders-nigeria-to-align-its-cybercrime-law-with-its-international-obligations/.

97 "Freedom on the Net 2021: Zambia," Freedom House, 2021. https://freedomhouse.org/country/zambia/freedom-net/2021.

98 "Zambia: Telecom regulator agrees to inform public of reason for any interruption in access to Internet within 36 hours of any such event in future," Business and Human Rights Resource Centre, 2022, https://www.business-humanrights.org/en/latest-news/zambia-telecom-regulator-enters-into-a-consentjudgement-on-Internet-shutdowns-agrees-to-inform-the-public-of-the-reason-for-any-interruption-in-accessto-Internet-within-36-hours-of-any-such-event-in-future/.

99 "Freedom on the Net 2021: Zambia, Freedom House, 2021, https://freedomhouse.org/country/zambia/freedom-net/2021.

International NGOs and pan-African CSOs are also fighting to protect digital rights in SSA. INGOs, including Human Rights Watch,[100] Article 19,[101] Amnesty International,[102] Freedom House,[103] and Access Now[104] have created strategies to promote and uphold freedom of expression online. Several CSOs, alliances, and think tanks based in Africa are also highly active in protecting and promoting digital rights, including The African Internet Rights Alliance,[105] the African Digital Rights Network,[106] Collaboration on International ICT Policy in East and Southern Africa (CIPESA),[107] OpenNet Africa,[108] the Association for Progressive Communications (APC),[109] Research ICT Africa,[110] and the Paradigm Initiative.[111] They also participate in international processes and initiatives, such as the Internet Governance Forum (IGF), the RightsCon conference, and the Human Rights Council (HRC). Their contributions to the Council and attendance at side events held during Council sessions bring high value to USAID and SSA governments aiming to strengthen their engagement in international processes related to digital rights.[112]

The private sector also has a role in advocating for and shaping digital laws and regulations, especially where digital rights violations can also have negative effects on their businesses. The telecommunications industry has supported digital policy and regulations. In countries like Nigeria, telecommunications industry associations have both the financial resources and the political connections needed to participate as digital policies, regulations, and laws are developed.[113] In Kenya, with support from the international telecommunications industry association GSMA, local telecommunications companies have worked with regulators to push Kenya to sign the Child Online Protection (COP) Charter, under which "Kenya's mobile industry will work together with the country's regulator to foster a culture of safe and responsible use of the Internet."[114] At a global level, telecommunications and internet providers partnered with the Global Network Initiative (GNI) to release a joint statement condemning internet shutdowns, citing their negative economic impacts.[115] In Pakistan, private sector-supported research has been used in litigation against internet shutdowns.[116]

100 Human Rights Watch, https://www.hrw.org/.

101 Article 19, https://www.article19.org/.

102 Amnesty International, https://www.amnesty.org/en/.

103 Freedom House, https://freedomhouse.org/.

104 Access Now, https://www.accessnow.org/.

105 African Internet Rights Alliance, https://aira.africa.

106 African Digital Rights Network, https://www.africandigitalrightsnetwork.org/.

107 Collaboration on International ICT Policy for East and Southern Africa (CIPESA), https://cipesa.org/.

108 OpenNet Africa, https://www.opennetafrica.org/.

109 Association for Progressive Communications (APC), https://www.apc.org/.

110 Research ICT Africa, https://researchictafrica.net/.

111 "Connecting African Youth with digital opportunities and ensuring digital rights for all," Paradigm Initiative, n.d., https://paradigmhq.org/.

112 Sorina Teleanu, Jovan Kurbalija, "Stronger digital voices from Africa: Building African digital foreign policy and diplomacy," DiPLO, 2022, https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/.

113 Chux Daniels, Benedikt Erforth, Chloe Teevan, "Putting People at the Centre of Digital Policy Mechanisms for Citizen Engagement in Nigeria," Taylor and Francis Group, 2022, https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003274322-12/putting-people-centre-digital-policy-joe-abah-krista-baptista-connor-mackenzie-anand-varghese.

114 "First GSMA We Care Initiative Launches in Kenya, Focusing on Online Child Protection," GSMA, November 20, 2018, https://www.gsma.com/newsroom/press-release/first-gsma-we-care-initiative-launches-in-kenya-focusing-on-online-child-protection/.

115 "The Economic Impact of Disruptions to Internet Connectivity," Global Network Initiative, n.d., https://globalnetworkinitiative.org/%E2%80%8Bnew-report-reveals-the-economic-costs-of-Internet-shutdowns/.

116 David Sullivan, "Five Ways Telecommunications Companies Can Fight Internet Shutdowns," Lawfare News, August 23, 2020, https://www.lawfaremedia.org/article/five-ways-telecommunications-companies-can-fight-Internet-shutdowns.

# 8. Recommendations

## RECOMMENDATION 1: ASSESS EXISTING AND NEW NATIONAL DIGITAL REGULATION THROUGH THE LENS OF HUMAN RIGHTS

USAID can assess digital regulation through an international human rights law lens in order to understand which digital rights restrictions are permissible under international human rights law. This understanding can ensure that laws that support digital repression, undermine digital democracy, and encroach on human rights do not receive USAID support and funding.

When assessing local digital laws and regulations, USAID staff can use the UN's three-part test that considers the legality, legitimacy, proportionality and necessity of digital rights restrictions under data protection and cybersecurity and cybercrime laws.[117] International law allows for the restriction of digital rights (the right to privacy, freedom of expression, freedom of association and assembly, and access to information) both offline and online, but only under limited and specific circumstances, and in accordance with Article 19 of the ICCPR (freedom of expression and access to information) using the three-part test in the table below.

**TABLE 2: Three-part test for assessment of legitimacy of digital rights restrictions under international human rights law:**

| PRINCIPLE | EXPLANATION |
|---|---|
| **LEGALITY** | • ICT laws must clearly stipulate any restrictions on freedom of expression unambiguously. Citizens must be able to understand and comply with the laws, making them legitimate. Vague and overly broad provisions do not meet this standard.<br>• Laws and regulations should have strict limitations on access to and merging of government databases.<br>• Prohibiting the publication of material based solely on its criticism of the government or its political and social system goes against international law. The Human Rights Committee of the United Nations states that restrictions on digital rights should be specific to the content. Broad bans on certain sites and systems are not in line with international law.[118] |

117 Dr. Agnes Callamard, "Freedom of expression and advocacy of religious hatred that constitutes incitement to discrimination, hostility or violence," Article 19, n.d., https://www.ohchr.org/Documents/Issues/Expression/ICCPR/Seminar2008/PaperCallamard.doc. "Freedom of expression and ICTs: Overview of international standards," Article 19, 2013, https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf. Joyce Hakmeh, "Cybercrime Legislation in the GCC Countries," Chatham House, July 4, 2018, https://www.chathamhouse.org/2018/07/cybercrime-legislation-gcc-countries/international-law-and-freedom-expression-online. See also: UN General Assembly Resolution on the Right to Privacy in the Digital Age of 2014 , the 2014 Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, and the Report of the Office of the United Nations High Commissioner for Human Right to Privacy in the Digital Age.

118 "General Comment No. 34," International Covenant on Civil and Political Rights (ICCPR), September 12, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

**TABLE 2 (CONTINUED): Three-part test for assessment of legitimacy of digital rights restrictions under international human rights law:**

| PRINCIPLE | EXPLANATION |
|---|---|
| **LEGITIMACY** | • Limitations on digital rights should only be imposed for legitimate reasons such as protecting the rights and reputations of others, ensuring national security, maintaining public order, and promoting public health or morals.<br>• Digital surveillance in public areas should only be used for legitimate reasons such as safeguarding people's safety and protecting critical infrastructure. |
| **PROPORTIONALITY AND NECESSITY** | • Digital surveillance may be permissible, but states must demonstrate that measures are both necessary and proportionate. Prior approval from a competent judicial authority is necessary for proportionate digital surveillance. This means that the least intrusive surveillance methods shall be used.[119] |

USG offices and Missions that work with government representatives and fund the development and enactment of digital laws in any sector must understand which digital rights restrictions are permissible under international human rights law. This will ensure that digital laws that further digital repression, undermine digital democracy, and encroach on human rights do not receive USG support and funding. USAID and other donors and implementing partners can use this information to understand and track trends and spot warning flags in the use of data privacy and cybercrime legislation and policy to further digital repression and limit digital rights across sub-Saharan Africa.

## RECOMMENDATION 2: LEVERAGE MULTI-STAKEHOLDER COLLABORATION, ESPECIALLY THROUGH MULTILATERAL AND REGIONAL BODIES, TO BUILD OUT RIGHTS-RESPECTING DIGITAL REGULATION IN SSA

Several SSA countries borrow from and often directly mirror existing regulation from the European Union's General Data Protection Regulation (GDPR) to quickly fill regulatory vacuums related to data protection and cybersecurity. USAID can build on these trends to support the development of rights-respecting digital regulation on the continent. It can convene various stakeholders—including European Union and multilateral donors, as well as regional bodies like the AU, AfCFTA and Regional Economic Communities (RECS)—to support the adaptation of relevant digital regulation models for individual SSA countries. USAID can support and influence countries to meaningfully tailor these models to their local country contexts, rather than copy-pasting them without consideration for local political economy, social norms, and other dynamics. USAID can also coordinate the efforts of various international donors, ensuring that the advice provided to SSA governments is consistent and coherent.

119 "Regulation of Communications Surveillance and Access to Internet in Selected African States," International Commission of Jurists, 2021, https://www.kas.de/documents/275350/0/Report-on-Regulation-of-Communications-Surveillance-and-Access-to-Internet-in-Selected-African-States.pdf/66dbd47d-4d7d-2779-a595-a34e9f93cfbb?t=1639140695434.

Regional bodies like the AU can support adaptation and implementation of cross-border data-sharing models, like the Asia-Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules (CBPR) System, a "voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies."[120] This process will benefit from USAID's experience working on CBPR through the Digital Connectivity and Cybersecurity Partnership (DCCP).

USAID can embed high level advisors in regional bodies. USAID has supported the AfCFTA Secretariat on the recently-released AU Digital Protocol through a seconded technical advisor. Advisors can develop digital frameworks and models, establish strategic partnerships with international and regional organizations and experts, facilitate inclusive negotiations on new policies, provide capacity-building for various stakeholders, engage civil society, provide advice on new policies, and analyze existing policies for bottlenecks.

## RECOMMENDATION 3: PROVIDE TECHNICAL ASSISTANCE TO SSA COUNTRY GOVERNMENTS TO EFFECTIVELY IMPLEMENT REGIONAL AGREEMENTS AT THE COUNTRY LEVEL

SSA countries have signed onto regional agreements such as those drafted by the African Union, but at the country level, implementation of those agreements has been ineffective. This is often due to a lack of institutional capacity and financial resources, as well as fragmented implementation. USAID and its partners can provide technical assistance and resources directly to governments to build their capacity to execute these agreements.

Specific activities could include:

- **Capacity Strengthening:** Conducting workshops and training sessions to build the capacity of government officials to understand, implement, and monitor digital regulations in line with good international practices (see Recommendation 3). Workshops can focus on areas such as legal frameworks, policy development, and stakeholder engagement in implementing human rights-respecting data protection and cybersecurity and cyber crime laws. They should be tailored to meet the specific capacity needs of staff, based on their positions (i.e., policymakers, line ministries, regulatory bodies, etc.), current skills, and knowledge of the regulations. USAID can also work through organizations like Lawyers Without Borders to increase knowledge and capacity across judicial systems in key countries.
- **Technical Expertise:** Securing technical experts from partner organizations to work alongside government ministries and engage interested Members of Parliament on the topic. These experts could assist with the roll-out and implementation of digital regulations in line with good international practices, provide on-the-job training, and offer guidance on best practices.
- **Policy and Regulatory Support:** In partnership with AU, RECs, and other regional organizations, assist governments in developing and implementing policies and regulations that align with regional agreements on data protection and cybersecurity and cyber crime. This can involve conducting policy assessments, drafting new legislation, and providing guidance on regulatory frameworks.
- **Monitoring and Evaluation:** Supporting SSA governments in establishing monitoring and evaluation mechanisms to track progress in implementing digital regulations and their compliance with international human rights agreements in the digital environment. This can include developing indicators, collecting data, and analyzing results to inform decision-making, and sharing this information with relevant external stakeholders such as CSOs.

120 "The APEC Cross-Border Privacy Rules (CBPR) System," Cross Border Privacy Rules System, n.d., https://cbprs.org/about-cbprs/.

- **Resource Mobilization:** Assisting governments in mobilizing financial resources to support the implementation of human rights-respecting digital regulation. This could include identifying funding sources, developing funding proposals, and engaging with donors and financial institutions.

## RECOMMENDATION 4: ENGAGE PRIVATE SECTOR STAKEHOLDERS AS ADVOCATES FOR RIGHTS-RESPECTING REGULATION AND TECHNOLOGY DEVELOPMENT

USAID can organize capacity-building for the private sector on the implementation of the UN Guiding Principles on Business and Human Rights (UNGPs).[121] The UNGPs provide a framework for businesses to prevent and address adverse human rights impacts linked to their operations, products, or services. Many private sector entities, especially in developing countries, lack the understanding and resources to effectively implement these principles. USAID's capacity-building efforts can help bridge this gap by providing training, guidance, and resources to help businesses integrate human rights considerations into their operations, with a special focus on digital-focused businesses (e.g., information technology (IT) and software development companies, technology-driven startups). This can improve human rights practices, enhance corporate social responsibility, and contribute to more rights-respecting digital regulation and technology development. Suggested programs and activities include:

- **Workshops and training** sessions tailored to the needs of different industries and sectors, focusing on practical guidance for implementing the UNGPs. These sessions could include case studies, best practices, and tools for conducting human rights due diligence and stakeholder engagement.
- **Online resources** such as webinars and e-learning modules to reach a broader audience and provide ongoing support.
- **Multi-stakeholder forums** or roundtable discussions where different groups (private sector, government, academia, CSOs) can exchange ideas, share experiences, and identify common challenges and solutions related to human rights in the digital environment. These forums can also create collaborative ways for private sector stakeholders to advocate for rights-respecting digital regulation, especially during early stages of regulation design.

USAID can also work with private sector stakeholders—particularly the telecommunications industry—to build on the strong relationship between the industry and government decision-makers, and to push for digital regulation and laws that support digital rights and are beneficial to the business interests of industry actors. USAID can also work with the private sector to co-fund research and make the economic case for these kinds of regulatory regimes as relevant.

121 "Business and Human Rights," UNDP, n.d., https://www.undp.org/business-and-human-rights.

## RECOMMENDATION 5: SUPPORT THE WORK OF LOCAL AND INTERNATIONAL CSOS

CSOs throughout SSA and internationally are leading the efforts to advocate against digital threats to democracy in the region. In many countries, legally restrictive environments also repress organizations that are advocating for the protection of digital rights. USAID can support civil society efforts through funding and capacity-building, and by creating opportunities for learning across different countries in SSA. Potential activities include:

- **Amplifying strategic communications**: USAID can amplify the voices of civil society around specific issues, including efforts to improve digital literacy so citizens know their rights and can advocate for reform. This can be done through collaborative communications efforts, strategic convenings or events, and in speeches from high level USAID officials.
- **Collaborating with and funding existing mechanisms**: USAID can galvanize support for funding mechanisms such as the African Digital Rights Fund, led by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA).[122] They can do this either through direct funding or by co-funding with other like-minded donors, such as the UK's FCDO or the European Union.
- **Using strategic litigation**: USAID can develop relationships with organizations—both local and international—that have successfully engaged, or are considering engaging, in strategic litigation efforts, including by identifying priority areas for legislative, regulatory, or policy reforms.
- **Providing capacity-building**: In many SSA countries, CSOs play the role of policy think tanks and watchdogs. USAID can provide capacity-building workshops and training, particularly on how to analyze available data and how to use this data to influence policy and advocate for digital rights protection.[123] USAID can also build capacity among CSOs to protect themselves from repressive regimes through trainings on topics such as resiliency and digital security.
- **Facilitate cross-CSO learning**: As USAID is working across SSA, it can use its networks and convening power to disseminate learnings from one context to another.

122 "About CIPESA," CIPESA, n.d. https://cipesa.org/about-us/about-cipesa/.

123 Relevant USAID-supported resources include: https://greaterInternetfreedom.org/digital-rights/; https://www.icnl.org/resources/civic-freedom-monitor; https://monitor.civicus.org/globalfindings_2023/; https://csosi.org/.

# Annex 1: Examples of Successful Strategic Litigation

### In Southern Africa:

- **Zimbabwe:** In 2019, Zimbabwe's High Court found that the government's mandatory internet shutdown exceeded its authority and ordered the government to restore internet service. After several protesters were killed in 2019 over rising petrol prices, Zimbabwe's government sent in the military and shut down the internet. Civil society organizations challenged the shutdown, and the High Court concluded that the government's decision to shut down the Internet during the protests was unlawful because it had gone beyond its mandate.
- **Zimbabwe:** The Zimbabwean police requested access to the records of Econet (a telecommunications company) subscribers in their pursuit of illegal foreign currency traders. The High Court of Zimbabwe quashed a warrant for these records in September 2020 due to privacy concerns. Civil society organizations also filed an application stating that police access to Econet's 11 million subscriber database would violate users' right to privacy.
- **South Africa:** The Amabhungane Centre for Investigative Journalism filed a case in 2017 challenging the constitutionality of the Related Information Act (RICA). The South African Constitutional Court found several provisions of RICA unconstitutional. It also found the state (the National Communication Centre) guilty of carrying out unlawful mass surveillance and foreign signal interception.

### In West Africa:

- **Togo:** The ECOWAS Court of Justice concluded in 2020 that the internet shutdown imposed by the Togolese government during 2017 protests was illegal. The court ordered the government to compensate the plaintiffs two million CFA and to ensure the application of freedom of expression protections.
- **The Gambia:** In Federation of African Journalists and Others v. The Gambia, the ECOWAS Court of Justice ruled in 2018 that The Gambia must promptly abolish or change or decriminalize its laws regarding fake news, sedition, criminal libel, and defamation to comply with its duties under international law. The judgment of the Gambia Press Union and Others v. Attorney General that followed the decision of the ECOWAS Court of Justice stated that the practice of applying criminal penalties for false news, sedition, criminal libel, and defamation has a chilling effect that may unreasonably restrict the ability of journalists to exercise their right to free expression and impose an excessive burden in violation of the right to free expression guaranteed by international law. The Gambian Supreme Court also declared the law on false news on the Internet to be unconstitutional.

### In East Africa:

- **Uganda:** The Ugandan Cyber Law Initiative, together with several individuals, filed an action in the Constitutional Court in 2018 against the Attorney General, the Uganda Communications Commission, and the Uganda Revenue Authority over the introduction of an Over the Top (OTT) media tax. The applicants sought the court's declaration that the new law was unconstitutional and infringed on economic rights, freedom of expression and information, freedom of assembly, and other political rights and freedoms. There has been no progress on the case, although the social media tax was replaced with a 12% levy on data.
- **Kenya:** In the Bloggers Association of Kenya (BAKE) v. Hon. Attorney General & Three Others in Kenya, BAKE argued that the Computer and Misuse Act of 2018 violated, endangered, and impinged upon the fundamental liberties guaranteed by Kenya's 2010 Constitution's Bill of Rights. In its petition, it referenced European Union case law due to the lack of precedent and case law on strategic litigation in Africa. After enacting a temporary order to suspend the statute, the High Court ultimately deemed the entire Act to be lawful and decided that the 26 sections challenged by BAKE were constitutional. This verdict represents a setback for the digital rights movement in Kenya. An earlier case—Coalition for Reform and Democracy (CORD) et al v Republic of Kenya et al—also sparked national debate in 2015. In this case, CORD (a coalition of political parties) went to the High Court to dispute the validity of the Security Laws (Amendment) Act, No. 19 of 2014, specifically around the publication or distribution of obscene, gory, or offensive material, for fear that it would apply to Kenyan citizens using social media. In its judgment, the court declined to suspend the whole Security Law (Amendment) Act of 2014 from coming into force, implementation, or operation, but granted conservatory orders halting several clauses.
- **Kenya:** The Katiba Institute—a CSO dedicated to seeing Kenya's constitution implemented—and legal scholar Yash Pal Ghai filed suit asking the High Court to declare the Huduma ID system's data collection and roll-out process unconstitutional. The Court held that the Data Protection Act of 2019 should apply retroactively to the government's roll-out of the system that began in 2020.

In addition to national level courts, regional institutional avenues for strategic litigation include the ECOWAS Community Court of Justice (ECOWAS Court), the East African Court of Justice (EACJ), the Southern African Development Community Tribunal (SADC Tribunal), and the African Commission on Human and Peoples Rights (ACHPR).

# Annex 2: References


*362: Resolution on the Right to Freedom of Information and Expression on the InternetInternet in Africa – ACHPR/Res.362,* OAS, 2016, (LIX)2016, https://www.achpr.org/sessions/resolutions?id=374.

Abimbola, Olumide, Faten Aggad, Bhaso Ndzendze, et al., *What is Africa's Digital Agenda"* Africa Policy Research Institute (APRI), n.d., https://afripoli.org/uploads/publications/Africas_Digital_Agenda_final.pdf.

*About CBPRS*, Cross Border Privacy Rules System, https://cbprs.org/about-cbprs/.

*About CIPESA*, CIPESA, https://cipesa.org/about-us/about-cipesa/.

Access Now, https://www.accessnow.org/.

*Access to Information Laws*, UNESCO, n.d., https://www.unesco.org/en/access-information-laws.

Adeniran, Adedeji, *Developing an effective data governance framework to deliver African digital potentials*, Brookings, March 21, 2022, https://www.brookings.edu/blog/africa-in-focus/2022/03/21/developing-an-effective-data-governance-framework-to-deliver-african-digital-potentials/amp/.

Africa Center for Strategic Studies, January 4, 2022, https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/.

*Africa Privacy Report 2023/2024,* Lawyers Hub: Tech for Justice, January 2023, https://www.lawyershub.org/Digital%20Resources/Africa%20Privacy%20Report%202023-24/Africa%20Privacy%20Report%202023-2024.pdf.

*African Bodies: ECOWAS Act on Personal Data Protection,* One Trust Data Guidance, November 2021, https://www.dataguidance.com/opinion/african-bodies-ecowas-act-personal-data-protection.

*African Declaration on Internet Rights and Freedoms Coalition (2021) Privacy and personal data protection in Africa. A rights-based survey of legislation in eight countries*, https://www.apc.org/en/pubs/privacy-and-personal-data-protection-africa-rights-based-survey-legislation-eight-countries.

*African Declaration on Internet Rights and Freedoms, Principle 2*, n.d., https://africaninternetInternetrights.org/.

African Digital Rights Network, https://www.africandigitalrightsnetwork.org/.

*African governments hope digital taxes will fill a budget hole,* The Economist, October 13, 2022, https://www.economist.com/middle-east-and-africa/2022/10/13/african-governments-hope-digital-taxes-will-fill-a-budget-hole.

African Internet Rights Alliance, https://aira.africa.

*African Union Convention on Cyber Security and Personal Date Protection*, African Union, June 27, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_ african_union_convention_on_cyber_ security_and_personal_data_protection_e.pdf .

*After years in the dark, Tigray is slowly coming back online*, Access Now, March 17, 2023, https://www.accessnow.org/tigray-shutdown-slowly-coming-back-online/.

Allen, Karen, *South Africa Lays Down the Law on Cybercrime*, Institute for Security Studies, June 9, 2021, https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime.

Allen, Nathaniel, Catherine Lena Kelly, *Deluge of Digital Repression Threatens African Security*, January 4, 2022, Africa Center for Strategic Studies, https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/.

Allen, Nathaniel, Matthew La Lime, *How Digital Espionage Tools Exacerbate Authoritarianism Across Africa*, Brookings Techstream, November 19, 2021, https://www.brookings.edu/articles/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/.

Amnesty International, https://www.amnesty.org/en/.

Article 19, https://www.article19.org/.

Association for Progressive Communications (APC), https://www.apc.org/.

Ayalew, Yohannes Eneyew, *The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?* EJIL: Talk!, June 15, 2023, https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/.

Ben-Hassine, Wafa, *Digital identity programs: what could go wrong? Our contribution at UNCTAD's E-Commerce Week*, Access Now, April 19, 2021, https://www.accessnow.org/digital-identity-programs-what-could-go-wrong-our-contribution-at-unctads-e-commerce-week/.

Ben-Hassine, Wafa, *Government Policy for the Internet Must Be Rights-Based and User-Centred,* UN Chronicle, n.d., https://www.un.org/en/chronicle/article/government-policy-internetInternet-must-be-rights-based-and-user-centred.

*Business and Human Rights*, UNDP, n.d., https://www.undp.org/business-and-human-rights.

Callamard, Dr. Agnes, *Freedom of expression and advocacy of religious hatred that constitutes incitement to discrimination, hostility or violence,* Article 19, n.d., https://www.ohchr.org/Documents/Issues/Expression/ICCPR/Seminar2008/PaperCallamard.do.

Cece, Siago, *Blogger Alai to be charged over 'alarming coronavirus post',* Nation Media Group, March 24, 2020, https://www.nation.co.ke/kenya/news/blogger-alai-to-be-charged-over-alarming-coronavirus-post--280580.

*Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa*, CIPESA, 2018, https://cipesa.org/?wpfb_dl=272.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA), https://cipesa.org/.

*Paradigm Initiative: Connecting African Youth with digital opportunities and ensuring digital rights for all,* Paradigm Initiative, n.d., https://paradigmhq.org/.

Dahir, Abdi Latif, *Tanzania's government is casting itself as the nation's sole custodian of data*, Quartz Africa, September 13, 2018, https://qz.com/africa/1389147/tanzanias-magufuli-bans-data-publication-without-government-ok/.

Daigle, Brian, *Data Protection Laws in Africa: A Pan-African Survey and Noted Trends,* United States International Trade Commission Journal of International Commerce and Economics, February 2021, https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf.

Daniels, Chux, Benedikt Erforth, Chloe Teevan, *Putting People at the Centre of Digital Policy Mechanisms for Citizen Engagement in Nigeria,* Taylor and Francis Group, 2022, https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003274322-12/putting-people-centre-digital-policy-joe-abah-krista-baptista-connor-mackenzie-anand-varghese.

*Data & Digital Rights in Nigeria: Assessing the activities, issues and opportunities,* Luminate Group, n.d., https://luminategroup.com/storage/1361/Data-%26-Digital-Rights-in-Nigeria-Report-%5BFINAL%5D.pdf.

*Data and Online Privacy Under Attack*, Southern Africa Digital Rights Issue Number 1, African Internet Rights, July 2022, https://africaninternetrights.org/en/resource/southern-africa-digital-rights-issue-number-1-data-and-online-privacy-under-attack.

*Democratizing Digital Landscape Assessment,* USAID Digital Frontiers, September 27, 2022, https://www.digitalfrontiersdai.com/resources/democratizing-digital-landscape-assessment/.

*Digital Freedoms in French-Speaking African Countries,* Agence Française de Développement (AFD), May 2023, https://www.afd.fr/en/ressources/digital-freedoms-french-speaking-african-countries.

*Digital rights in Africa: A brief national overview,* DiPLO, n,d., https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-rights-in-africa-national-overview/.

*Digitized Autocracy Literature Review,* USAID, August 2021, https://pdf.usaid.gov/pdf_docs/PA00XV9R.pdf.

*Draft ECOWAS ICT Accessibility Policy (2018) v1post Burkina Faso and Gambia Workshop*, ICT Policy Africa, 6, September 25, 2019, https://ictpolicyafrica.org/en/document/0kgv8x4u0pd?page=6.

*ECOWAS Court orders Nigeria to align its Cybercrime Law with its international obligations*, Media Foundation for West Africa, March 28, 2022, https://www.mfwa.org/ecowas-court-orders-nigeria-to-align-its-cybercrime-law-with-its-international-obligations/.

*Ensuring the protection of human rights in the digital era*, United Nations Office of the Secretary-General's Envoy on Technology, n.d., http://www.un.org/techenvoy/content/digital-human-rights.

*First GSMA We Care Initiative Launches in Kenya, Focusing on Online Child Protection*, GSMA, November 20, 2018, https://www.gsma.com/newsroom/press-release/first-gsma-we-care-initiative-launches-in-kenya-focusing-on-online-child-protection/.

Freedom House, https://freedomhouse.org/.

*Freedom of expression and ICTs: Overview of international standards*, Article 19, 2013, https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf.

*Freedom of expression online: Communications and Digital Committee report*, UK Parliament House of Lords Library, October 19, 2022, https://lordslibrary.parliament.uk/freedom-of-expression-online-communications-and-digital-committee-report/#heading-1.

*Freedom on the Net 2021: Zambia*, Freedom House, 2021. https://freedomhouse.org/country/zambia/freedom-net/2021.

*Freedom on the Net*, Freedom House, n.d., https://freedomhouse.org/report/freedom-net.

*Freedom on the Net: Ethiopia,* Freedom House, 2021, https://freedomhouse.org/country/ethiopia/freedom-net/2021.

*General comment No. 34*, International Covenant on Civil and Political Rights (ICCPR), September 12, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

*Government Internet Shutdowns Have Cost $53 Billion Since 2019*, Top 10 VPN, n.d., https://www.top10vpn.com/cost-of-internet-shutdowns/.

Hakmeh, Joyce, *Cybercrime Legislation in the GCC Countries,* Chatham House, July 4, 2018, https://www.chathamhouse.org/2018/07/cybercrime-legislation-gcc-countries/international-law-and-freedom-expression-online.

Harter, Fred, *Record number of countries enforced internet shutdowns in 2022 – report*, The Guardian, February 28, 2023, https://www.theguardian.com/global-development/2023/feb/28/internet-shutdowns-record-number-countries-2022-report.

https://www.kas.de/documents/275350/0/Report-on-Regulation-of-Communications-Surveillance-and-Access-to-InternetInternet-in-Selected-African-States.pdf/66dbd47d-4d7d-2779-a595-a34e9f93cfbb?t=1639140695434.

Human Rights Watch, https://www.hrw.org/.

Hunter, Murray, Admire Mare, *A Patchwork For Privacy: Mapping communication surveillance laws In southern Africa*, Media Policy and Democracy Project, June 5, 2020, https://archive.org/details/patchwork-for-privacy-communication-surveillance-in-southern-africa.

Ilori, Tomiwa, *Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions*, African Internet Rights, n.d., https://africaninternetrights.org/sites/default/files/Tomiwa%20Ilori_AfDec_Data%20protection%20in%20Africa%20and%20the%20COVID-19%20pandemic_Final%20paper.pdf.

Ilori, Tomiwa, *Life interrupted. Centering the social impacts of network disruptions in advocacy in Africa,* Global Network Initiative, 2021, https://globalnetworkinitiative.org/wp-content/uploads/2021/03/Life-Interrupted-Report.pdf.

*Implications of Zambia's Cyber Security and Cybercrimes Act 2021 on Digital Rights*, CIPESA, 2021, https://cipesa.org/?wpfb_dl=447.

*Information Minister and the Twitter Ban*, LEGIST, Policy and Legal Advocacy Centre, June 29, 2021, https://placng.org/Legist/information-minister-and-the-twitter-ban/.

*Internet shutdown tracker*, Surfshark, n.d., https://surfshark.com/research/internet-censorship.

*Internet shutdowns and elections handbook,* Access Now, n.d., https://www.accessnow.org/guide/internet-shutdowns-and-elections-handbook/.

Jili, Bulelani, *The Spread of Surveillance Technology in Africa Stirs Security Concerns*, Africa Center for Strategic Studies, December 11, 2020, https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/

Kelly, Catherine Lena, *Justice and Rule of Law Key to African Security*, Spotlight, Africa Center for Strategic Studies, May 25, 2021, https://africacenter.org/spotlight/justice-and-rule-of-law-key-to-african-security/.

*Kictanet 2022 Annual Report*, Kictanet, 2022, https://www.kictanet.or.ke/.

Lirri, Evelyn, *"Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa,"* CIPESA, August 16, 2022,https://cipesa.org/2022/08/privacy-imperilled-analysis-of-surveillance-encryption-and-data-localisation-laws-in-africa/

Lynch, James, *Middle East and North Africa Iron net: Digital repression in the Middle East and North Africa*, European Council on Foreign Relations, June 29,2022, https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/.

Makulilo, Alex Boniface, *Analysis of the regime of systematic government access to private sector data in Tanzania*, Information & Communications Technology Law 29, no. 2, 250-278, March 28, 2020, https://www.tandfonline.com/doi/abs/10.1080/13600834.2020.1741156

*Mapping and Analysis of Privacy Laws in Africa*, CIPESA, 2011, https://cipesa.org/?wpfb_dl=479.

Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, et al, *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*, University of Toronto, The Citizen Lab, December 1, 2020, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles.

*Mechanisms for Citizen Engagement in Nigeria*, Taylor and Francis Group, 2022, https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003274322-12/putting-people-centre-digital-policy-joe-abah-krista-baptista-connor-mackenzie-anand-varghese.

Mekonnen Tegegn, Dunia, *Advancing Strategic Litigation on Internet Shutdowns cases in Africa: Promises and Pitfalls*, CIPESA, n.d., https://cipesa.org/?wpfb_dl=462.

Musoni, Melody, *Envisioning Africa's AI governance landscape in 2024,* European Centre for Development Policy Management, January 2024, https://ecdpm.org/application/files/7017/0651/8711/Envisioning-Africas-AI-Governance-Landscape-in-2024-ECDPM-Briefing-Note-177-2024.pdf.

Nanfuka, Juliet, *Data Privacy Still A Neglected Digital Right in Africa*, CIPESA, January 27, 2022, https://cipesa.org/2022/01/data-privacy-still-a-neglected-digital-right-in-africa/.

*Online database of privacy laws in Africa*, https://www.privacytracker.africa/

OpenNet Africa, https://www.opennetafrica.org/.

*Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY,* Council of Europe, n.d., https://www.coe.int/en/web/cybercrime/parties-observers.

*Privacy and data protection in the Digital Era: Challenges and Trends in Africa*, CIPESA, September 2018, https://cipesa.org/?wpfb_dl=278.

*Promotion and protection of human rights around the globe*, UN Human Rights Council, n.d., https://www.ohchr.org/en/hrbodies/hrc/home.

*Regulation of Communications Surveillance and Access to Internet in Selected African States,* International Commission of Jurists, 2021, https://www.kas.de/documents/275350/0/Report-on-Regulation-of-Communications-Surveillance-and-Access-to-Internet-in-Selected-African-States.pdf/66dbd47d-4d7d-2779-a595-a34e9f93cfbb?version=1.0&t=1639140695434.

Research ICT Africa, https://researchictafrica.net/.

Roberts, Tony, *Surveillance laws are failing to protect privacy rights: what we found in six African countries*, The Conversation, October 21, 2021, https://theconversation.com/surveillance-laws-are-failing-to-protect-privacy-rights-what-we-found-in-six-african-countries-170373.

Roberts, Tony, Abrar Mohamed Ali, Mohamed Farahat, et al., *Surveillance Law in Africa*, Institute of Development Studies, 2021, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y.

*Security Policymaking: Implications of the Entry Into Force of the Malabo Convention for Digital Financial Systems in Africa*, Carnegie Endowment for International Peace, July 10, 2023, https://carnegieendowment.org/2023/07/10/continental-cyber-security-policymaking-implications-of-entry-into-force-of-malabo-convention-for-digital-financial-systems-in-africa-event-8146.

Shahbaz, Adrian, Allie Funk, *Social Media Surveillance*, Freedom House, 2019, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance.

*Shutdowns in Africa: Addressing the Human Rights Responsibilities of Telecommunication Companies*, Business & Human Rights Resource Centre, March 2022, https://www.business-humanrights.org/documents/37422/2022_Africa_InternetInternet_Shutdowns_Briefing.pdf

*Southern African Development Community (SADC) Model Law*, ITU, 2013, https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.

Sullivan, David, *Five Ways Telecommunications Companies Can Fight InternetInternet Shutdowns*, Lawfare News, August 23, 2020, https://www.lawfaremedia.org/article/five-ways-telecommunications-companies-can-fight-internetInternet-shutdowns.

*Surveillance Law in Africa: a Review of Six Countries*, Institute of Development Studies, October 2021, https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/16893.

*Targeted, Cut Off, and Left in the Dark: The #KeepItOn report on internetInternet shutdowns in 2019*, KeepItOn, 2019, https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.

*Taxing Social Media in Africa*, InternetHealth Report, 2019, https://internethealthreport.org/2019/taxing-social-media-in-africa/.

Teleanu, Sorina, Jovan Kurbalija, *Stronger digital voices from Africa: Building African digital foreign policy and diplomacy*, DiPLO, 2022, https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/.

*The Economic Impact of Disruptions to InternetInternet Connectivity*, Global Network Initiative, n.d., https://globalnetworkinitiative.org/%E2%80%8Bnew-report-reveals-the-economic-costs-of-internetInternet-shutdowns/.

*U.S.-China Relations in 2020: Enduring Problems and Emerging Challenges,* Hearing on U.S.-China Relations in 2020, U.S.-China Economic and Security Review Commission, September 9, 2020, https://www.uscc.gov/hearings/us-china-relations-2020-enduring-problems-and-emerging-challenges.

*Uganda introduces 12% internet data levy, critics say move will stifle online access*, Reuters, April 30, 2021, https://www.reuters.com/world/africa/uganda-introduces-12-internet-data-levy-critics-say-move-will-stifle-online-2021-04-30/.

*Unwanted Witness: About Us*, Unwanted Witness, n.d., https://www.unwantedwitness.org/about/.

*USAID Digital Strategy,* USAID, n.d., https://www.usaid.gov/digital-development/usaid-digital-strategy.

Wako, Amina, *Coronavirus: Detectives arrest man spreading falsehoods*, Nation Media Group, March 24, 2020, https://www.nation.co.ke/news/DCI-arrests-man-over-COVID-19-tweet/1056-5492720-bgpj5kz/index.html.

Wanyama, Edrine, *Advancing Collaborations in Strategic Litigation for Digital Rights in East Africa,* CIPESA, January 28, 2020, https://cipesa.org/2020/01/advancing-collaborations-in-strategic-litigation-for-digital-rights-in-east-africa/.

Wardle, Clair, *Information Disorder: The Essential Glossary*, Harvard Kennedy School, The Shorenstein Center, July 2018, https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf; *Disinformation Primer,* USAID, January 1, 2023, https://www.usaid.gov/democracy/documents/disinformation-primer.

*Zambia: Telecom regulator agrees to inform public of reason for any interruption in access to internet within 36 hours of any such event in future,* Business and Human Rights Resource Centre, 2022, https://www.business-humanrights.org/en/latest-news/zambia-telecom-regulator-enters-into-a-consentjudgement-on-internet-shutdowns-agrees-to-inform-the-public-of-the-reason-for-any-interruption-in-accessto-internet-within-36-hours-of-any-such-event-in-future/.



USAID
FROM THE AMERICAN PEOPLE