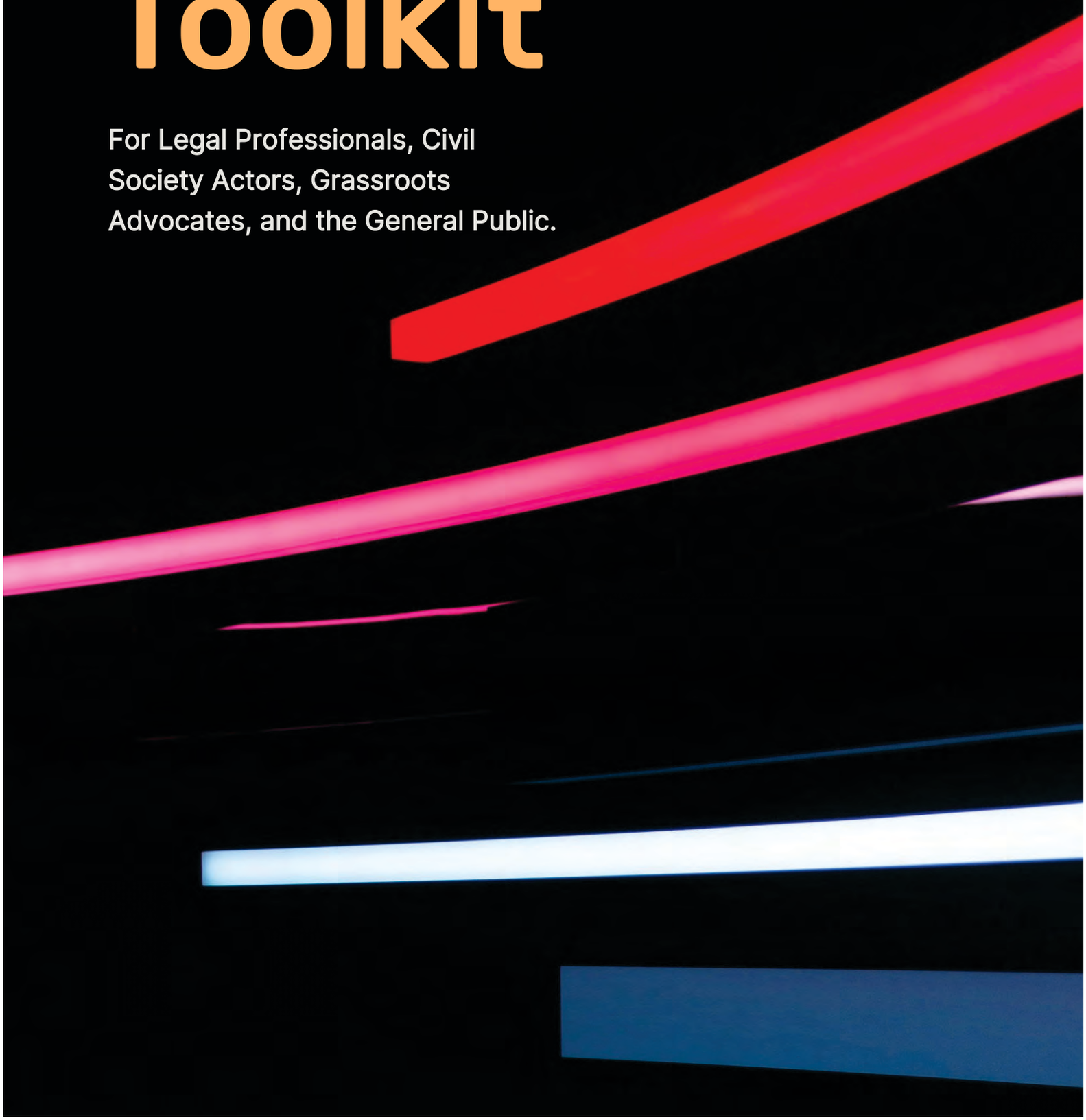
digicivic INITIATIVE

Luminate
Building Strong Societies

Digital Rights Toolkit

For Legal Professionals, Civil Society Actors, Grassroots Advocates, and the General Public.



Digital Rights Toolkit

For Legal Professionals, Civil Society Actors, Grassroots Advocates, and the General Public.

TABLE OF CONTENT

1. Introduction & Purpose of the Toolkit
2. Understanding Digital Rights & Civic Space
3. Key Digital Rights Issues
4. Advocacy Foundations (Advocacy Cycle, Power Mapping, Evidence Building)
5. Tools for Advocacy (Litigation, Policy, Media, Grassroots Organizing)
6. Inclusive Policy Frameworks
7. Practical Advocacy Strategies (shutdowns, OGBV, repressive laws, etc.)
8. Case Studies
9. Tools and Resources
10. Conclusion & Next Steps

ACKNOWLEDGMENT

This Digital Rights Toolkits is published by Advocates for the Promotion of Digital Rights and Civic Interactions Initiative (Digicivic Initiative) with support from Luminate. Digicivic Initiative would like to thank Luminate for its financial support which made the publication and other activities within the project possible.

The development of this Digital Rights Toolkit would not have been possible without the commitment and contributions of numerous individuals and organizations dedicated to advancing digital rights across Africa. We express our profound gratitude to experts and advocates whose proficiency served as a foundation for this work.

We acknowledge the tireless efforts of civil society groups, legal practitioners, grassroots movements, and community-based organizations who continue to defend online freedoms despite significant challenges. Special appreciation goes to the reviewers, editors, and partners who provided valuable feedback during the drafting of this toolkit. Finally, we recognize the countless activists, journalists, and everyday citizens whose experiences and resilience inspire the ongoing fight for a safer, more accessible, and rights-respecting digital future.

CONTRIBUTORS

Solomon Okadara – Digital Rights Lawyers

National Data Protection Commission

National Human Rights Commission

Spaces for Change

Mbamalu Chibundo- Tomorrow Africa Minds

Accountability Lab

National Information Technology Development Agency (NITDA)

Ali Sabo- Centre for Information Technology and Development (CITAD)

Rita Anwiri Chindah

Mojirayo Ogunlana

Morisola Alaba-Akinlabi

Maxwell Ahunanyah

PREFACE

Digital technologies now shape nearly every aspect of civic, social, economic, and political life. They influence how people access information, participate in democratic processes, build communities, and exercise their fundamental rights. As Africa's digital landscape expands driven by increased connectivity, mobile innovation, and emerging technologies so too do the risks and inequalities that affect how individuals experience these rights. Internet shutdowns, unlawful surveillance, online gender-based violence, discriminatory data practices, harmful content regulation, and the exclusion of marginalized communities continue to narrow civic space and challenge the exercise of freedom of expression, privacy, association, and access to information.

This Digital Rights Toolkit has been developed in response to these evolving realities. It is designed as a practical and accessible resource for legal professionals, civil society organizations, journalists, policymakers, grassroots advocates, and members of the general public who seek to understand and engage with digital rights in meaningful ways. The toolkit simplifies complex concepts, clarifies legal frameworks, and provides real-world case studies, advocacy strategies, and tools for community engagement. It aims to strengthen digital literacy, improve evidence-based advocacy, and enable users to navigate the intersection of human rights and technology with confidence.

At its core, this toolkit is grounded in the belief that digital rights are human rights. It affirms that people should be free to communicate, organize, innovate, and participate in public life without fear of repression, discrimination, or technological harm. It also recognizes that an inclusive digital future is possible only when all groups, including women and girls, people with disabilities, rural communities, linguistic minorities, and young people, are able to access and benefit from digital spaces safely and equitably.

By equipping advocates with knowledge, strategies, and practical tools, this toolkit seeks to contribute to a broader movement committed to protecting and expanding civic space in the digital age. It invites users to challenge restrictive policies, advance rights-respecting governance, and promote a digital environment where freedom, dignity, and inclusion are upheld for all.

Mojirayo Ogunlana
Executive Director, Digicivic Initiative

GLOSSARY

Accessible Format - Making digital content usable for persons with disabilities.

Biometric Digital ID System: Systems using fingerprints, facial recognition, or DNA for identification—raising major privacy and inclusion concerns.

Circumvention: Efforts to bypass censorship or surveillance technologies, often through VPNs or proxy tools.

Consent: The individual's right to freely give specific, informed, clear, expression, in whatever form, to the collection, recording, storage, alteration, retrieval, use, disclosure, erasure, destruction, and sharing of their information or that of another individual, in whose stead they have lawful authority to act, by another, whether by automated or manual activity.

DDOS - Distributed denial of service attack is a malicious activity that involves the disruption of normal traffic to a server by flooding that server with internet traffic using multiple malware infected bots so that a system, such as an application or web, becomes unavailable to a legitimate end user.

Deepfakes: This is a type of technology that uses a special kind of 'machine learning' called 'deep' learning to create convincing images, audios, and videos that have been doctored or edited to imitate an original.

Digital Activism - Use of digital tools and platforms to advocate for social and political change.

Digital Equality - refers to the fair and inclusive access, use, and benefits of digital technologies, such as the internet, digital devices, and online services, by all individuals and communities, regardless of their gender, age, location, income, ability, or social status.

Digital Freedom - The ability to access, create, and share information freely online without undue restriction.

Digital Identity - This is the information that represents personal identifiers of individuals, created, received and stored by a computer as a means of recognizing these agents for the purpose of identification.

Digital Infrastructure: The physical and virtual systems—networks, data centers, cables—that enable connectivity.

Digital Literacy - This refers to the ability to understand, use, create, interact, operate, and function in a digital environment where information and communication play critical roles through the efficient and increased use of digital technologies such as the internet, social media platforms, digital health services, etc.

Digital Piracy - Unauthorized reproduction or distribution of copyrighted digital materials.

Digital Rights - Digital Rights refers to a broad set of human rights that online users are entitled to. It is an extension of human rights in the digital space such as freedom to organize, assemble, join groups, be free from discrimination, own property, etc. in the online environment. These rights include the right to life, dignity, fair hearing, movement, property, and so much more. For the purpose of this toolkit and in relation to the civic space, the digital rights emphasised here are for privacy, freedom of expression, freedom of association and freedom of assembly.

Digital Rights Advocacy: Organized efforts to protect and advance digital freedoms and inclusion.

Digital Rights Management Information (DRMI): Systems that control access to or usage of digital works, often balancing intellectual property and user rights.

Digital Rights Trust Fund: Financial mechanism to support advocacy, research, and community-driven digital rights initiatives.

Disinformation: Disinformation is false information that is deliberately created, presented, and disseminated to deceive or mislead people, and which may cause public harm. It is created knowingly to manipulate opinions, cause confusion, or achieve political, social, or financial gain.

Domain Name System (DNS) - The system translating web addresses into IP addresses; essential to internet accessibility.

Domain Names - Digital identifiers for websites; disputes over them often touch on intellectual property and access.

DOS attack - Denial of service attack is a cyber-attack in which a malicious actor or perpetrator aims to shut down a machine or network, in order to render it inaccessible to its intended legitimate users by disrupting the device's normal operations or services.

Doxing or doxxing is the deliberate and malicious act of hunting, collecting, and publishing of specific identifiable information about an individual or organization in order to expose, exploit, extort, harass, or intimidate the targeted individual or organization .

Encryption: This is a process that is used for the protection of data. It is initiated to protect data from being stolen, changed, or compromised. This involves the encoding of data from plain text to unintelligent scribbles.

Encryption Standards: They are a set of algorithms and protocols that are designed to protect digital data by securing online communications and connections, with the principal aim of maintaining confidentiality and integrity. These standards can be symmetric and asymmetric. The symmetric employs the use of a single, shared key for both encryption and decryption, while asymmetric uses a pair of linked keys differently for encryption and decryption- usually, a public key for encryption and a private key for decryption.

Falsification: Alteration or misrepresentation of RMI or data to deceive or mislead.

Hate Speech: Any kind of communication in speech, writing, or behavior that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, color, descent, gender, or other identity factor. Hate speech targets individuals or groups and aims to incite discrimination.

Human Rights Enforcement: Ensuring digital rights are protected through courts, policy, and international mechanisms.

Inclusive Governance: Ensuring all stakeholders—especially marginalized tion, hostility, or violence.

Information Technologies- This is generally defined as the use of computers for the creation, storage, processing, management, transmission, retrieval or manipulation of any information.

Internet Freedom: This envisions an open and safe internet where rights and freedoms are respected and protected. It encompasses freedom of expression, assembly, association, access to information, freedom from censorship, arbitrary decisions, surveillance and net neutrality, etc.

Internet Intermediaries: (Network Operators, Infrastructure Providers, Caching Providers, Technical Providers, Content Services, Online Platforms)

Internet Service Providers (ISPs): Companies providing users access to the internet, critical to maintaining openness and access.

Interoperability - Ensuring digital systems and platforms can operate together seamlessly and inclusively.

IP address: Internet Protocol address is a unique number that identifies a specific digital device on the Internet and also provides information about the specific location of the network through which it is connecting.

Lawful Access: Government access to digital communications for security purposes, which must comply with due process and human rights standards.

Lobbying - Targeted engagement with policymakers to influence legislation or regulation related to digital rights.

Malware - It's a software or code written by bad actors to maliciously access information from applications and services. There are mainly two types, the spyware, which is a type of malware that is used to monitor and spy on victims. This is also a type of surveillance technique used by state and non-state actors; and the Ransomware, which is a malware that encrypts information or data on victims' systems, in this type of attack, the hacker will demand a ransome in order to decrypt the information.

Mass Surveillance: Widespread monitoring of digital activity, often violating privacy and freedom of expression.

Misinformation - Misinformation refers to false or misleading information that is shared, regardless of intent to deceive. The person sharing misinformation believes it to be true, there is no deliberate intent to cause harm.

New Actors: Emerging stakeholders such as tech startups, data brokers, and digital influencers shaping the digital landscape.

NonProfit Basis for Research - Ensuring open and ethical use of data for public-interest research.

Online Content Regulation: State or platform-based efforts to moderate or remove harmful content, often a point of tension with free expression.

Online Harms: Behaviors or content online that cause psychological, social, or physical harm, such as cyberbullying or hate speech.

Personal data - means any information relating to a living natural person who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual.

Privacy of Beneficiary Person/PWD: Protection of data belonging to individuals benefiting from aid or services, especially vulnerable groups.

Privacy Rights: The right to control personal data and communications against unlawful surveillance or misuse. It encompasses the legal and moral entitlements of individuals to live free from arbitrary interference in their personal, family, and private affairs, and to exercise control over personal information and personal autonomy. These rights recognize that every individual is entitled to a sphere of personal life that is protected from intrusion by the state, organizations, or other individuals, except where such interference is lawful, necessary, and proportionate.

Private Censorship: Content control or removal by private platforms that may suppress legitimate speech.

Right of Way - Legal frameworks allowing installation of digital infrastructure across public or private land.

Rights Management Information (RMI): Metadata identifying ownership and usage rights for digital content.

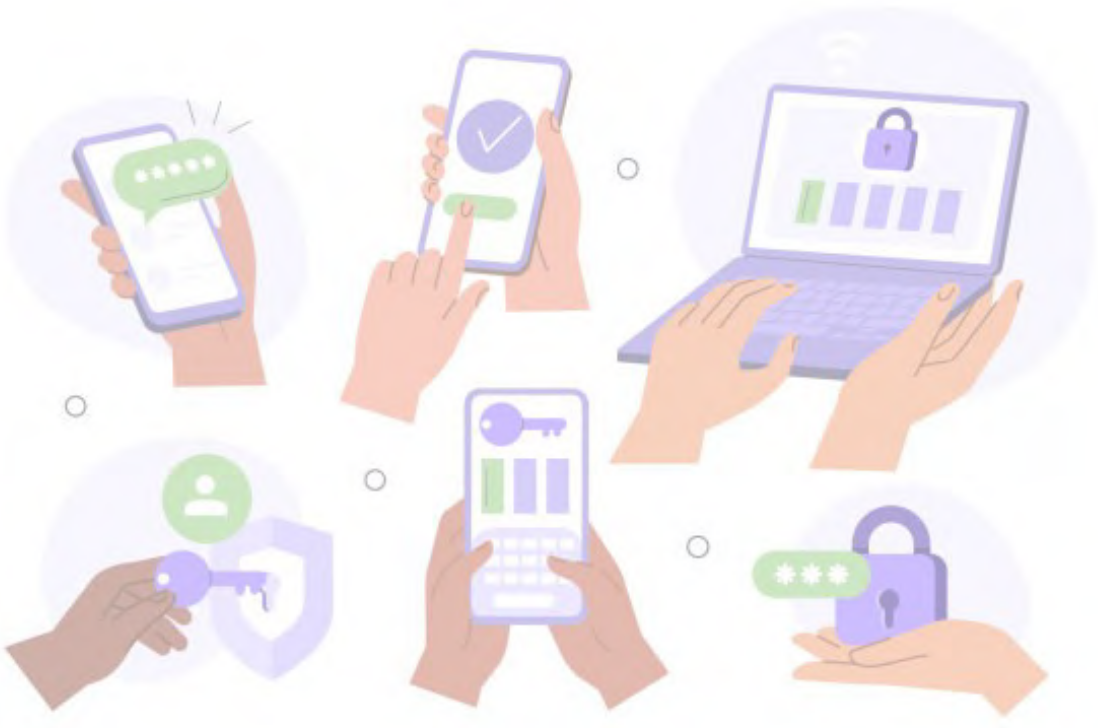
SDG of Digital Rights (ESG and Digital Rights) - Aligning digital policies with Sustainable Development Goals and Environmental, Social, and Governance principles to promote ethical and sustainable technology.

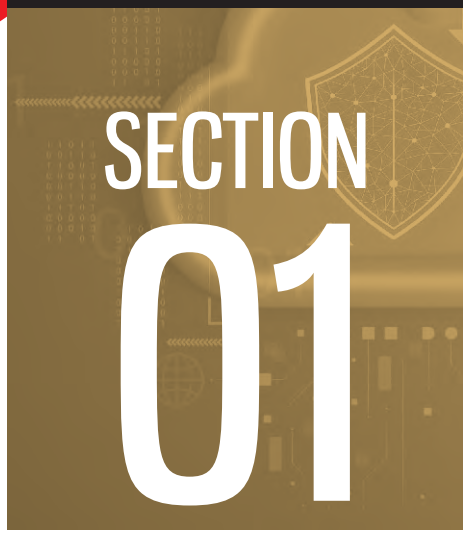
Security and Digital Inclusion: Building secure digital ecosystems that are open, accessible, and inclusive for all.

Surveillance Tech: Technologies used to monitor citizens; advocacy focuses on transparency and safeguards.

Take Down Notice of Content: Legal or administrative orders to remove content, often under copyright or other rights violations.

Throttling is the intentional act of internet service providers (ISP) or network administrators to slow down the performance of an internet reception, not really for technical reasons, but usually to manage network congestion during peak hours, enforce data caps, or limit the usage of certain applications.





INTRODUCTION

1.1 Purpose of the Toolkit

This toolkit is designed as a practical resource for individuals and organizations seeking to strengthen digital rights advocacy and advance inclusive digital policy frameworks in Africa. It builds on the digital rights and civic space and adapts its principles to empower diverse actors such as lawyers, civil society organizations, grassroots movements, and everyday citizens to effectively engage in the protection and promotion of digital rights.

The aim is not only to explain what digital rights are, but also to provide actionable tools including advocacy strategies, litigation approaches, case studies, and templates to help stakeholders influence law, policy, and practice in ways that expand civic space online and offline.

1.2 Why Digital Rights Matter

Digital rights matter because they safeguard not only access to technology but also the freedom to choose information sources and the right to privacy, which are essential for genuine civic participation and personal autonomy. In an increasingly digital world, individuals must have the freedom to seek, receive, and share information from diverse and independent sources without fear of censorship or manipulation. Equally, protecting privacy ensures that personal data is not exploited, surveilled, or misused, allowing people to express themselves freely and participate safely in public life. When digital rights are upheld, technology becomes a tool for empowerment, accountability, and inclusion strengthening democracy and protecting human dignity in the digital age.

However, these opportunities are accompanied by new challenges:

- **Internet shutdowns during elections and protests**.

Internet shutdowns during critical periods such as elections and protests silence political participation and restrict access to vital information. They undermine democratic processes, enable abuses to go unreported, and violate international human rights standards.

- **Repressive laws that criminalize online speech.**

This refers to where governments continue to use overly broad or vague legislation to punish dissent and silence critical voices online. Such laws gag free expression, weaken civic space, and discourage legitimate public debate.

- **Mass surveillance without adequate safeguards.**

Widespread, unchecked surveillance allows governments and private actors to track individuals' activities without transparency or accountability. This creates fear, self-censorship, and an environment where privacy and personal autonomy are severely undermined.

- **Anonymous Communication**

Efforts to restrict anonymous communication deprive individuals of a critical protection mechanism especially activists, whistleblowers, journalists, and marginalized groups. Limiting anonymity exposes users to retaliation, harassment, and surveillance.

- **Online Gender Based violence**

Women and gender-diverse persons face disproportionate harassment, doxxing, threats, and digital abuse that silence their voices and restrict participation in public life. OGBV fosters trauma, exclusion, and further embeds gender inequality in digital spaces.

- **Digital exclusion**

Rural communities, persons with disabilities, elderly persons, and low-income groups are systematically left behind due to limited connectivity, affordability challenges, and inaccessible technologies. This exclusion widens social inequities and prevents full participation in political, economic, and civic life

- **Doxxing Campaign**

Doxxing exposes personal or sensitive information without consent, placing individuals at risk of harassment, intimidation, physical harm, and reputational damage. It violates privacy rights and is frequently used to silence activists, journalists, and minority groups.

- **Platform Throttling**

Platform throttling deliberately slows down access to specific websites or services, impairing communication and limiting access to real-time information. This subtle form of censorship restricts civic participation while avoiding direct legal scrutiny.

- **Misinterpretation of available laws as they apply to the Internet Space**

Poor knowledge of digital ecosystems leads authorities and institutions to wrongly apply offline laws to online contexts, often in ways that violate rights. These misinterpretations create unpredictable enforcement environments that harm free expression and innovation.

- **Disinformation, Misinformation**

False or misleading content spreads rapidly online, manipulating public opinion, distorting democratic processes, and fueling conflict. Efforts to address these harms are often misused to suppress dissent or justify restrictive regulations.

- **Regulatory and Financial Restrictions**

Burdensome registration rules, funding limitations, and compliance requirements weaken civil society and independent media working on digital rights. These constraints restrict advocacy, reduce transparency, and silence accountability actors.

- **Use of deepfakes and synthetic media**

Deepfakes and synthetic media are increasingly deployed to sow confusion, incite tribal or religious tensions, manipulate politics, and provoke xenophobic or racist narratives. Their realism makes it difficult for users to distinguish truth from fabrication, undermining trust in the information ecosystem.

- **Litigating Digital Rights**

Digital rights litigation is complex, resource-intensive, and often hindered by outdated legal frameworks and limited judicial capacity. Despite these challenges, strategic litigation remains a crucial tool for establishing precedent and strengthening human rights protections online.

- **Using Emerging Tech to control information ecosystems**

Governments and powerful actors use emerging technologies such as AI-driven moderation, automated surveillance, and algorithmic ranking to shape, suppress, or manipulate public discourse. These tools centralize power, reduce transparency, and can be weaponized to undermine civic freedoms.

- **Sexually explicit content involving a child**

The creation, sharing, or possession of sexually explicit content involving a child constitutes a severe violation of children's rights and safety. Online circulation of such content fuels

exploitation, traumatizes victims, and demands robust prevention, reporting, and prosecution mechanisms.

Digital rights advocacy ensures that technology enhances rather than erodes human rights and civic freedoms, but it often competes with the global order and foreign interference by challenging the power dynamics embedded in global technology governance. The global digital landscape is largely shaped by a few powerful states and multinational tech corporations that control data flows, digital infrastructure, and online platforms. Advocating for digital rights, therefore, means confronting these centralized structures to demand transparency, accountability, equitable access, and respect for human rights across borders. This advocacy questions the dominance of profit-driven and surveillance-oriented models that prioritize control and commercial interests over privacy, freedom of expression, and inclusion seeking instead a fairer digital order where global rules and technologies serve people, not power.

1.3 Measurable Outcomes for Users?

This toolkit is intended for:

- **Legal professionals**: to deepen their knowledge of digital rights and litigation strategies and the ability to litigate digital rights cases.
- **Civil society organizations**: providing insight to develop policy briefs and campaign strategies-to strengthen advocacy and policy engagement.
- **Grassroots advocates**: to organize community awareness campaigns that connect community voices with national and international advocacy.
- **The public**: to enable them to become informed digital citizens, exercising and defending their digital citizenship rights.

1.4 Challenges and the Need for the Toolkit

The expansion of digital technologies has reshaped civic space, yet it has also generated complex challenges that many individuals and institutions are ill-equipped to navigate. Across Africa, rights violations such as internet shutdowns, unlawful surveillance, arbitrary content takedowns, personal data exploitation, disinformation, deepfake manipulation, and algorithmic discrimination have become increasingly common. Many legal and advocacy actors have inadequate accessible, Africa-centered resources that demystify these issues and illustrate their connection to international human rights standards.

Furthermore, critical gaps persist in understanding data retention limits, lawful processing of personal data, cross-border data flows, and security safeguards. Communities face growing concerns over digital authenticity in the era of synthetic media, the misuse of online platforms by minority actors for harmful purposes, the spread of plagiarized or manipulated content, and the

marginalization of vulnerable groups, including the elderly and visually impaired, who require targeted protections and accessible digital formats. These challenges threaten democratic participation, weaken accountability, and erode trust in digital systems.

1.5 How This Toolkit Addresses These Challenges

This toolkit directly responds to these challenges by providing a comprehensive, simplified, and actionable guide to understanding and advocating for digital rights in a rapidly evolving digital landscape. It:

- Translates complex digital rights principles into accessible language for non-technical audiences.
- Offers legal and policy analysis grounded in international, regional, and national human rights frameworks.
- Equips users with practical strategies to challenge violations such as censorship, unlawful data retention, internet shutdowns, and discriminatory tech practices.
- Integrates inclusion-focused recommendations to ensure that women, persons with disabilities, Indigenous communities, elderly persons, and digitally marginalized groups are not left behind.
- Presents real-life case studies, templates, and advocacy tools that can be used in litigation, policy engagement, public education, and community mobilization.

By empowering users with both knowledge and practical tools, the toolkit strengthens efforts to protect civic space, advance human rights, and promote a digital ecosystem that is open, inclusive, secure, and accountable.

SECTION

02

UNDERSTANDING DIGITAL RIGHTS

2.1 What Are Digital Rights?

Digital rights are the application of human rights in digital space. They refer to the rights and freedoms that individuals enjoy online and in relation to technology. At their core, they are not new rights but extensions of existing rights including freedom of expression, privacy, access to information, freedom to own property, equality, freedom of assembly and association, and many more freedoms in alignment with international human rights standards..

Key principles of digital rights include:

- **Universality and indivisibility**: Digital rights are human rights, not separate elements.
- **Equality and non-discrimination**: All individuals should have equitable access to enjoy digital rights equally, regardless of gender, race, disability, or socioeconomic status.
- **Accountability and transparency**: Governments and corporations must be held accountable for decisions affecting citizens digital rights online.

2.2 Digital Rights in International Human Rights Law

Digital rights are grounded in core human rights instruments:

- **Universal Declaration of Human Rights (UDHR, 1948)** – affirms rights to free expression in Article 19, assembly in Article 20, and participation in Article 21.
- **International Covenant on Civil and Political Rights (ICCPR, 1966)** – guarantees freedom of expression, privacy, and association in Articles 17, 19, 21, 22.
- **African Charter on Human and Peoples' Rights (ACHPR, 1981)** – emphasizes dignity, freedom of expression, and participation in governance in Articles 5, 9 and 13.
- **The 2011 United Nations Human Rights Council Resolution on the promotion, protection and enjoyment of human rights on the Internet** (A/HRC/RES/20/8) adopted on 5 July 2012, is a landmark resolution that first articulated the global consensus that human rights apply equally online and offline. The 2011 resolution laid the foundation for recognizing Internet-based communication as a legitimate and essential medium for

exercising freedom of expression and other fundamental rights later strengthened by **Resolution 32/13 (2016)**, which expanded protection within the broader context of digital rights.

- **Human Rights Council Resolution 26/13 (2014)** — The United Nations Human Rights Council (UNHRC) affirmed that "the same rights that people have offline must also be protected online", particularly freedom of expression.
- **UN Human Rights Council Resolution 32/13 (2016)** – explicitly recognizes that "the same rights that people have offline must also be protected online."
- **Human Rights Council Resolution 38/7 (2018)** — Further reinforcement of the online rights principle; addresses issues like access, gender digital divide, corporate responsibility.
- **UN General Assembly Resolution 78/213 (2023**) — A recent resolution on "promotion and protection of human rights in the context of digital technologies".

These instruments provide the legal foundation for digital rights advocacy, litigation, and policy engagement.

2.3 The Link Between Civic Space and Digital Rights

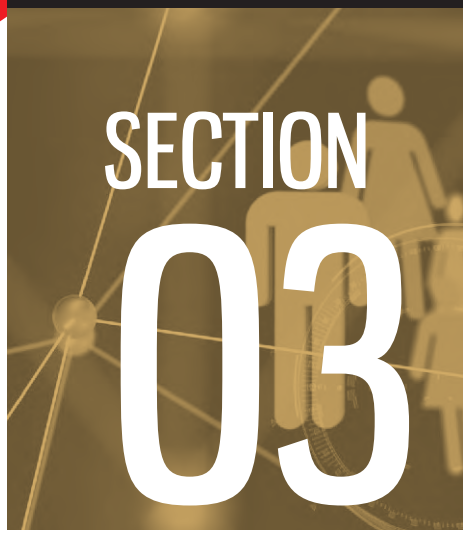
Across Africa, the digital rights landscape reflects both significant progress and deepening challenges. Democracy is a major system of governance in Africa, allowing citizens to exercise certain freedoms which have also now become exerciseable in the digital space. Digital rights involve the application and extension of universal human rights, such as freedom of expression, assembly, association, privacy, non-discrimination in the online space. These freedoms are essential for democratic participation and are aided by several digital tools that can enhance democracy by increasing citizen engagement and government transparency. On one hand, increased internet penetration and youth-driven innovation have opened new frontiers for expression, association, and civic engagement. Citizens now organize online, demand accountability, and build solidarity across borders in ways previously unimaginable. Yet, this same digital space have become contested terrain. Governments, citing national security and public order, frequently deploy restrictive laws, internet shutdowns, and digital surveillance to stifle dissent. Journalists, activists, and ordinary citizens face online harassment, censorship, and shrinking access to reliable information.

The link between the civic space and digital rights is therefore undeniable, a free and open internet sustains the same freedoms that underpin democratic societies: speech, assembly, and participation. When digital rights are undermined, civic space shrinks; when citizens cannot speak or organize safely online, democracy itself weakens. Strengthening digital rights protection across Africa is not just about technology, it is about safeguarding human dignity, accountability, and the right of every person to participate fully in the public life of their nation.

In the digital age, civic space increasingly exists online through social media, online campaigns, digital protests, and virtual communities. However, when digital rights are curtailed, civic space shrinks.This manifests in many ways including:

- Internet shutdowns to disrupt protests and elections.
- Criminalization of online speech silences dissent.
- Surveillance to discourage participation and activism.
- Manipulation and misinformation
- Algorithmic bias that can be susceptible to perpetuating social inequalities and injustices
- Security threats in the cyber attacks

Thus, digital rights and the civic space are interdependent. Advocacy for one strengthens the other.



KEY DIGITAL RIGHTS ISSUES

This section highlights pressing digital rights issues. Understanding these issues is essential for legal professionals, civil society, grassroots advocates, and everyday citizens who want to engage in meaningful advocacy.

In today's complex digital ecosystem, emerging issues such as take-down notices, internet shutdowns, throttling, synthetic media, data misuse, and other forms of network disruptions highlight the urgent need for balanced and rights-based digital governance. While take-down notices are intended to remove harmful or illegal content, they are often misused to suppress dissent, whereas internet shutdowns represent a more extreme violation that disrupts access to information and infringes on freedom of expression and association. For instance, in the Amnesty International Togo case v The Republic of Togo, Judgment no ECW/CCJ/JUD/09/20 (25 June 2020), the ECOWAS Court found that Togo's 2017 internet shutdowns violated freedom of expression and ordered remedies and reforms, underscoring that state-ordered network disruptions are not a legitimate substitute for lawful restrictions and must comply with human-rights standards. This is a clear judicial recognition that shutdowns are an extreme form of interference with civic space and access to information.

Following its decision in the Amnesty Togo case, the Community Court of ECOWAS was approached to decide the legality of the suspension of Twitter in the ***SERAP AND OTHERS V NIGERIA*** *(*the Twitter Ban case).[1] The Court held that because access to the internet facilitates freedom of expression, 'denial of access to the internet or services provided via the internet… operates as denial of the right to freedom of expression and to receive information'. It therefore overruled Nigeria's objection to its jurisdiction. On the merits, *it reasoned that access to social media like Twitter is essential for exercising freedom of expression; therefore, access to social*

[1] The consolidated Case of four applications- The cases of Suit **No. ECW/CCJ/APP/23/21**, filed by Mr. Femi Falana (SAN), on behalf of Socio-Economic Rights and Accountability Project (SERAP), a Lagos-based NGO, and 176 Nigerians; Suit **No. ECW/CCJ/APP/24/21**, filed by Chief Malcolm Omirhobo, a Lagos-based human rights lawyer; Suit **No. ECW/CCJ/APP/26/21**. Filed by Mr. Patrick Elohor, President of the NGO, One Love Foundation; and Suit **No. ECW/CCJ/APP/29/21** filed by Mrs. Mojirayo Ogunlana-Nkanga on behalf of Media Rights Agenda and four other non-governmental organizations as well as four journalists (Accessible at https://mediarightsagenda.org/media-rights-agenda-others-win-suit-over-twitter-ban-as-ecowas-court-rules-nigerian-governments-action-unlawful-2/)

media including Twitter should be regarded as a component of freedom of expression and protected from unlawful, arbitrary, or disproportionate restrictions. It therefore concluded that Nigeria's ban of Twitter without the backing of a law or court order violated freedom of expression under the African Charter and the ICCPR.

Notably, the ECOWAS Court also condemned internet shutdowns in Guinea in the case of **ASSOCIATION DES BLOGUEURS DE GUINÉE (ABLOGUI) AND OTHERS V THE STATE OF GUINEA ECW/CCJ/JUD/38/23/22 (31 October 2023),** the four claimants argued that Guinea's decision to restrict internet access and block social media platforms amounted to an unlawful infringement of their rights to freedom of expression and access to information, as protected under the African Charter and the International Covenant on Civil and Political Rights. This judgment reinforces the growing body of jurisprudence affirming that internet shutdowns are unlawful and that states have a positive duty to ensure continuous, unhindered access to the internet.

Following its decision in the Amnesty Togo case, the Community Court of ECOWAS was approached to decide the legality of the suspension of Twitter in the **SERAP AND OTHERS V NIGERIA** (the Twitter Ban case).[2] The Court held that because access to the internet facilitates freedom of expression, 'denial of access to the internet or services provided via the internet… operates as denial of the right to freedom of expression and to receive information'. It therefore overruled Nigeria's objection to its jurisdiction. On the merits, *it reasoned that access to social media like Twitter is essential for exercising freedom of expression; therefore, access to social media including Twitter should be regarded as a component of freedom of expression and protected from unlawful, arbitrary, or disproportionate restrictions.* It therefore concluded that Nigeria's ban of Twitter without the backing of a law or court order violated freedom of expression under the African Charter and the ICCPR.

Also, the rise of synthetic media and deepfakes further complicates digital authenticity, demanding mechanisms to verify truth without undermining creative expression or privacy. Equally vital is the right to control personal information, ensuring individuals can prevent unauthorized use of their data through clear consent, permission, and authorization protocols. Addressing plagiarized content and the misuse of digital spaces for harmful purposes calls for stronger digital ethics and accountability. Moreover, targeted data protection must extend to vulnerable populations such as

[2] The consolidated Case of four applications- The cases of Suit No. ECW/CCJ/APP/23/21, filed by Mr. Femi Falana (SAN), on behalf of Socio-Economic Rights and Accountability Project (SERAP), a Lagos-based NGO, and 176 Nigerians; Suit No. ECW/CCJ/APP/24/21, filed by Chief Malcolm Omirhobo, a Lagos-based human rights lawyer; Suit No. ECW/CCJ/APP/26/21. Filed by Mr. Patrick Elohor, President of the NGO, One Love Foundation; and Suit No. ECW/CCJ/APP/29/21 filed by Mrs. Mojirayo Ogunlana-Nkanga on behalf of Media Rights Agenda and four other non-governmental organizations as well as four journalists https://mediarightsagenda.org/media-rights-agenda-others-win-suit-over-twitter-ban-as-ecowas-court-rules-nigerian-governments-action-unlawful-2/ accessed December 5, 2025.

the elderly, while accessible and authenticated information must be prioritized to uphold the digital rights of persons with visual impairments. Collectively, these challenges demand comprehensive legal frameworks and advocacy strategies that protect human rights, promote accountability, and foster an inclusive and trustworthy digital environment.

3.1 Freedom of Expression Online

The internet has become the central space for exercising free speech, yet States, tech giants and private actors increasingly restrict online expression.

- **Threats:** Arrests for social media posts, criminal defamation laws, censorship of online content, restrictions on press freedom - parody, skits, and content, cyberbullying, cyberstalking under Cybercrime Act. Also breach of privacy claims.
- **Legal Frameworks:** National Constitution, African Commission's 2016 Resolution 362 on the Right to Freedom of Information and Expression on the Internet, Universal Declaration on Human Rights (UDHR),. Article 19 of the International Covenant on Civil and Political Rights (ICCPR), Article 9 of the The African Charter on Human and Peoples Right (ACHPR) guarantee freedom of expression. Limitations must be necessary, proportionate, and provided by law. In addition, principles such as the Declaration of Principles on Freedom of Expression in Africa are relevant in protecting free speech in the digital space.
- **Advocacy Implications:**

    - Challenge vague or overly broad laws used to criminalize speech.
    - Promote judicial precedents that protect online dissent.
    - Engage tech companies on transparency and accountability in content moderation.
    - Deter internet users from infringing on the rights of other users to express themselves.

3.2 Access to Information

Access to information is a cornerstone of democracy, and in the digital age, this right must extend to universal and affordable internet access as a basic necessity for participation in modern life. Everyone should be able to connect, as exclusion from the internet effectively means exclusion from opportunities for education, economic advancement, and civic engagement. Telecommunications companies (telcos) play a crucial role in enabling this access as their infrastructure, pricing models, and adherence to net neutrality principles determine who gets connected and how freely information flows. However, access alone is not enough; digital literacy significantly affects how individuals use the internet to seek, evaluate, and share information. While digital literacy empowers citizens to engage meaningfully, spot misinformation, and hold power accountable, its absence can deepen inequality and expose users to exploitation, privacy

breaches, and manipulation. Therefore, promoting inclusive connectivity, responsible telco practices, and digital literacy is essential for realizing the full democratic potential of access to information in the digital era.

- **Threats:** Internet shutdowns, high data costs, lack of infrastructure, digital divides between urban/rural and men/women, including marginalised people.
- **Legal Frameworks:** the Constitution, national access to information law, Article 9 of the ACHPR recognizes the right to receive and impart information, International Covenant on Civil and Political Rights (ICCPR) 1966, Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019. The Internet is a catalyst for the enjoyment of human rights as it facilitates the realization of a range of other human rights.
- **Advocacy Implications:**
    - Campaign against shutdowns through litigation, public campaigns, and international pressure.
    - Push for universal service policies to expand affordable internet.
    - Promote open data initiatives for transparency.

3.3 Data Protection and Privacy

Personal data is constantly processed by governments, corporations, and digital platforms, making data protection and privacy critical components of modern human rights. Without clear safeguards, such data processing can lead to profiling, discrimination, surveillance, and abuse. Effective protection must therefore go beyond mere processing to include how long data is retained, how it is processed, and the measures taken to secure it. Individuals should have the right to know who holds their data, for what purpose, and how it is used or shared, consistent with data protection law or related laws and regulations, and international best practices such as data minimization and purpose limitation. Establishing clear data retention policies prevents indefinite storage and potential misuse, while robust encryption and security protocols protect against unauthorized access. Transparent oversight mechanisms, accountability from both state and private actors, and user empowerment through digital literacy are essential to ensure that personal data collection supports innovation and governance without compromising privacy, autonomy, or human dignity.

- **Threats:** Over collection of data, mass surveillance, biometric data misuse, lack of consent, unlawful retention of data, inaccurate personal data, data breaches .
- **Legal Frameworks:** National Constitution, Data Protection Law or Regulations, Convention on the Right of the Child (CRC), African Charter on Human and Peoples' Rights (ACHPR), 1981,Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019), SADC Model Law on Data Protection, 2012 Article 17 of the ICCPR (privacy), ECOWAS supplementary Act on data protection 2010, African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), EAC Framework for Cyberlaws, Phase II (2011–2014), AU Digital Transformation

Strategy (2020–2030),African Data Policy Framework (2022).

- **Advocacy Implications:**
    - Push for strong, independent data protection authorities.
    - Challenge data breaches.
    - Educate the public on data rights and digital hygiene.
    - Translation of laws to local languages. Such as what the National Data Protection Commission did, translating the Nigeria Data Protection Act 2023 into three languages(Yoruba, Igbo and Hausa).
    - Use of information, educational and communication resources and materials across all education segments

3.4 Freedom of Assembly and Association Online

Digital platforms have become the new public squares where people gather, organize, and influence social and political change. Across Africa, restrictions on online organizing and association have had direct consequences on civic movements: during #EndSARS in Nigeria (2020), authorities froze organizers' bank accounts and deployed digital surveillance to deter mobilization; in Uganda's 2021 elections, a nationwide social media shutdown silenced opposition voices and cut off real-time reporting; in Ethiopia, intermittent internet shutdowns during political tensions severely disrupted community organizing and humanitarian coordination; in Zimbabwe, activists behind campaigns like *#ThisFlag* and *#ShutdownZimbabwe* faced digital intimidation, arrests, and blocking of online content; and in Sudan, authorities repeatedly shut down the internet during pro-democracy protests to prevent citizens from coordinating demonstrations. These instances illustrate that when states restrict digital platforms, they do more than interfere with technology, they constrict civic space, weaken democratic participation, and undermine the fundamental rights of people to connect, assemble, and advocate for change.

- **Threats:** Blocking of online groups, criminalization of digital protests, cyber-harassment of activists/media practitioners, doxxing, throttling and various forms of technologically facilitated violence, Propaganda and Online harassment, Mal-information .
- **Legal Frameworks:** Section 40 of the 1999 Constitution of the Federal Republic of Nigeria (as amended), Article 21 and Article 22 of the ICCPR, Article 19 of the International Covenant on Civic and Political Rights (ICCPR), Article 10 and 11 of the African Charter on Human and People Right (ACHPR) guarantee freedom of assembly and association. Limitations must be necessary, proportionate, and provided by law. In addition, protocols such as the Declaration of Principles on Freedom of Expression in Africa are relevant in protecting free speech in the digital space.
- **Advocacy Implications:**

    - Defend activists and organizations facing repression for online organizing.

- Challenge unjustified restrictions on digital assemblies.
- Advocate for the protection of anonymous and pseudo-work.
- Promote online civic education to expand participation.
- Post monitoring of violations, compliance with the curating of terms of reference or outline.

3.5 Surveillance, Security, and Encryption

Surveillance technology is expanding rapidly from biometrics (facial recognition, finger print, retina, voice recognition) to spyware. Unlawful and excessive surveillance can infringe on digital rights by State and non-state actors. While States justify it as preserving national security, it often undermines fundamental rights. In most cases this technology is repurposed to target civic actors and silence dissent.

- **Threats:**
  - **Chilling Effect on Participation:** When activists, journalists, and human rights defenders fear being monitored, they are less likely to organize online, share dissenting views, or engage in advocacy.
  - **Weaponization Against Civil Society:** Governments have used spyware and digital surveillance tools to monitor opposition leaders, journalists, and CSOs.
  - **Data Misuse and Profiling:** Facial recognition databases, SIM card registration systems, and biometric ID programs can be repurposed for political profiling or targeting minority voices.
  - **Criminalization of Encryption:** Restrictions on encryption undermine secure communication channels essential for whistleblowers, investigative journalists, human rights defenders, and civic movements.
- **Legal Frameworks:** African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), African Charter on Human and Peoples' Rights (ACHPR), ACHPR Resolution 362 (2016) on the Right to Freedom of Information and Expression on the Internet, ACHPR/Res. 473 (2021) on Protecting Privacy and Personal Data, ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019)
- **Advocacy Implications:**
  - Push for strong legal protections that recognize encryption and anonymous communication as essential components of privacy and free expression.
  - Challenge overbroad surveillance and cybercrime laws that grant unchecked powers to state agencies.
  - Demand transparency and independent oversight over all government and telecom surveillance activities.

- Litigate to eliminate legal provisions that criminalize the legitimate use of encryption and insist on judicial authorization, necessity, and proportionality as conditions for any surveillance operation.
- Emphasize on the vitality of encryption for the protection of journalistic sources and investigative reporting.
- Build multi-stakeholder coalitions to strengthen unified pressure for rights-respecting digital security reforms.
- Regional harmonization efforts to push African states to adopt AU-aligned standards that protect privacy and secure communications.
- Encourage digital platforms and telecom companies to deploy encryption-by-default and resist unlawful data requests.

3.6 Misinformation, Disinformation, and Hate Speech

Misinformation refers to false or inaccurate information that is shared without the intent to deceive, often because the person sharing it believes it to be true. Disinformation, on the other hand, is deliberately created or distributed to mislead, manipulate, or cause harm, making intentional deception its defining feature.

While hate speech refers to any form of expression that is spoken, written, or symbolic that attacks, demeans, or incites hostility or violence against a person or group based on protected characteristics such as race, ethnicity, religion, gender, disability, or nationality. It goes beyond mere offense by creating conditions that promote discrimination, exclusion, or harm toward targeted groups.

The spread of harmful content using digital platforms for spreading false information, intimidation, harassment, violent extremist and secessionist contents. Regulatory responses can also harm free expression through censorship, prior restraint, over criminalization and misapplication of laws.

Misinformation and disinformation undermine the integrity of public discourse, distort democratic participation, and create environments where truthful expression is drowned out, thereby weakening citizens' ability to make informed decisions. Furthermore, hate speech threatens the safety, dignity, and participation of targeted groups, effectively silencing their voices and shrinking the diversity of expression in civic spaces.

However, poorly designed regulatory responses to these issues such as blanket censorship, vague laws, or criminal sanctions can themselves become even greater threats to freedom of expression by suppressing legitimate speech. While these phenomena can harm freedom of expression, the way governments choose to regulate them can either protect rights or further erode them.

- **Legal Frameworks:** International Covenant on Civil and Political Rights (ICCPR), UN Human Rights Committee General Comment No. 34 (2011), Rabat Plan of Action (2012),

UN Strategy and Plan of Action on Hate Speech (2019), African Charter on Human and Peoples' Rights (ACHPR), ACHPR Model Law on Access to Information (2013), Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019), African Commission Resolution 362 (2016), African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), ECOWAS Supplementary Act on Personal Data Protection (2010), SADC Model Law on Computer Crime and Cybercrime (2013) and SADC Model Law on Data Protection (2013)

- **Advocacy Implications:**
    - Challenge legal frameworks that misuse misinformation laws to silence critical voices or suppress dissent.
    - Promote independent fact-checking and digital literacy.
    - Engage platforms for transparent moderation policies.
    - Require platforms to engage relevant stakeholders before making any fundamental change regarding fact checking

3.7 Gender and Digital Inclusion

Digital rights are not equally enjoyed across society, as women and girls, persons with disabilities or other beneficiary groups, rural communities, and individuals who are illiterate or have limited education face disproportionate levels of exclusion, limited access, and heightened vulnerability online.

- **Threats:** Online gender-based violence (OGBV), Cultural Orientation, Manipulation using tech tools like faceswap, Algorithmic and AI Bias, Digital Exclusion, Gendered Digital Literacy Gaps, Inadequate Online Safety Tools.
- **Legal Frameworks:** Universal Declaration of Human Rights (UDHR, 1948), Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW, 1979), Convention on the Rights of Persons with Disabilities (CRPD, 2006), International Covenant on Civil and Political Rights (ICCPR), African Charter on Human and Peoples' Rights (ACHPR), Protocol to the African Charter on the Rights of Women in Africa (Maputo Protocol), Protocol to the African Charter on the Rights of Persons with Disabilities in Africa (2018), ACHPR Declaration of Principles on Freedom of Expression & Access to Information in Africa (2019), African Union Digital Transformation Strategy (2020–2030), AU Convention on Cybersecurity & Personal Data Protection (Malabo Convention), ECOWAS Gender Policy, SADC Protocol on Gender and Development.
- **Advocacy Implications:**
    - Push for gender-sensitive and inclusive digital policies. Promote a balanced approach that safeguards fundamental human rights while respecting cultural preservation and ensuring inclusive access to digital rights.
    - Develop response mechanisms for OGBV, including legal aid and reporting platforms.

- Advocacy for digital rights must intentionally integrate indigenous and gender perspectives to ensure equitable access, cultural inclusion, cultural re-orientation, and protection from discrimination in the digital sphere.
- Ensure digital accessibility standards in law and practice.
- Engage law enforcement Agencies on proactive enforcement of law

3.8 Artificial Intelligence (AI) and Emerging Technologies

AI systems are technologies or tools that mimic or augment human intelligence in decision making. These systems are trained using a large amount of data ranging from structured, semi-structured and unstructured data.

Threat: Deep fakes, fraud, algorithm bias, discrimination, data breach, false information and identity theft.

Legal Framework: NDPA 2023, Article 43 of NDPA GAID, National AI strategy 2024, African Union AI Strategy 2024, NDPA, Copyrights Act

Advocacy Implications

- Advocate for AI guidelines
- Advocate for a comprehensive AI law with input from relevant stakeholders (CSOs, private actors, PWD, rural communities, women and vulnerable groups)
- Advocate for inclusive AI technologies

SECTION

04

ADVOCACY FOUNDATIONS

Advocacy is the deliberate process of influencing decision-makers, institutions, and the public to achieve social or policy change. In the context of digital rights, advocacy involves using legal, technology, policy, and grassroots tools to defend and expand civic space online.

This section introduces the advocacy cycle, power mapping, and evidence-building, providing a roadmap for effective campaigns.

4.1 Principles of Advocacy

Before diving into the specifics, effective advocacy is grounded in a few core principles:

1. **Legitimacy:** Advocacy must reflect genuine needs of communities and constituencies.
2. **Evidence-based:** Arguments carry weight when backed by facts, case law, or lived experiences.
3. **Inclusivity:** Advocacy must include marginalized groups and voices.
4. **Non-violence:** Peaceful, rights-based methods strengthen credibility.
5. **Sustainability:** Advocacy is rarely won in one step. It requires long-term commitment and consistency.
6. **Outcomes:** Advocacy must have a call to action or an 'ask'.

4.2 The Advocacy Cycle

The advocacy cycle provides a structured approach to planning and implementing campaigns:

1. **Issue Identification**
    - Define the digital rights issue clearly (e.g., criminalization of online speech, data privacy violations, surveillance, silent dissent and internet shutdowns).
    - Ensure the issue is timely, relevant, and actionable.
2. **Research and Evidence Gathering**
    - Collect data: laws, cases, statistics, testimonies.
    - Document violations (e.g., reports of shutdowns, arrests, or OGBV incidents).

- Use both quantitative (numbers) and qualitative (stories) evidence.

3. **Goal and Objective Setting**
   - **Goal:** The broad change desired (e.g., passage of a digital rights law, regulation of dual-use surveillance tools, repeal of a restrictive cybercrime law).
   - **Objectives:** SMART Specific, measurable steps toward the goal (e.g., filing litigation, mobilizing parliamentarians, public awareness)

4. **Strategy Development**
   - Choose tactics: litigation, lobbying, grassroots campaigns, media or policy advocacy.
   - Consider resources, risks, and political context.

5. **Implementation**
   - Mobilize networks and coalitions.
   - Use media (traditional and digital).
   - Engage policymakers, Executive, judiciary and institutions directly.

6. **Monitoring and Evaluation (M&E)**
   - Track progress using indicators (e.g., policy amendments, court rulings, increased awareness).
   - Adjust strategies based on lessons learned.

4.3 Mapping: Identifying Stakeholders

Advocacy is not only about knowing what change is needed, it's about knowing who can make it happen. Mapping helps identify and prioritize stakeholders.

Steps for Mapping:

1. **List key stakeholders:** Government agencies, legislators, regulators, courts, tech companies, civil society, international bodies, academia, etc.
2. **Assess their positions:** Supportive, neutral, opposed.
3. **Determine their influence:** High, medium, low.
4. **Map allies and opponents:** Build alliances with supportive actors, neutralize or engage opponents.

Example:

- **Target:** Government and its institutions → Has power to enforce shutdowns, private sectors, tech giants (online content moderation), ISPs and Fintech
- **Allies:** Government, Civil society, digital rights coalition → Mobilizes public and media.
- **Influencers:** International organizations, donor agencies → Apply diplomatic pressure.
- **Pressure Group:** CSOs, Labour Unions, NBA, NUJ, ASUU → Apply local pressure

4.4 Building Evidence: Research, Documentation, and Storytelling

Evidence is the backbone of advocacy. Without proof of violations, advocacy risks being dismissed as opinion.

Types of Evidence:

- **Legal Evidence:** Statutes, constitution, treaties, and court judgments.
- **Empirical Evidence:** Statistics on shutdowns, interviews, polls, reports, arrests, or OGBV prevalence with their respective consequences.
- **Narrative Evidence:** Victim/survivors testimonies, community stories, case studies.

Documentation Tools:

- Fact sheets, legal briefs, incident reports.
- Audio-visual documentation (with consent and protection for victims).
- Secure digital tools for recording violations
- Research.

Storytelling in Advocacy:
Data speaks, but stories move people. Effective advocacy frames digital rights as human stories

- Storytelling strategies
- Instead of saying: *"There were 15 internet shutdowns this year."*
- Say: *"A shutdown cut off students from their online exams, traders from their customers, and patients from telemedicine services."*

4.5 Intersection of Advocacy and Litigation

Legal advocacy is often paired with strategic litigation to achieve reform.

- **Litigation:** Challenges laws, arbitrary or unconstitutional government decisions and actions, holds States accountable, and creates legal precedents.
- **Advocacy:** Amplifies litigation outcomes, ensuring they translate into policy or behavioral change.

Example: Litigation against internet shutdowns in East Africa was strengthened by simultaneous public campaigns that framed the shutdowns as economic and human rights violations. Cases of Litigation and Public Campaigns against Internet Shutdowns in Africa.

Below are real-life examples from the African continent where litigation and public advocacy campaigns against internet shutdowns (or similar disruptions) have been used,or are being used,

together. These illustrate how legal efforts are reinforced by public pressure, framing shutdowns as economic, civic, and human-rights violations.

In Kenya (2025), a coalition of civil society actors including CIPESA, Bloggers Association of Kenya (BAKE), Paradigm Initiative (PIN), Law Society of Kenya (LSK), among others filed a public-interest petition at the High Court challenging recurring internet shutdowns and digital-communication disruptions. The suit argues such shutdowns violate constitutional rights like free expression and access to information.[3] The public campaign accompanying the litigation highlighted how shutdowns disrupt livelihoods, education (especially for students during critical exams), and access to vital services — making the case relatable to ordinary citizens beyond a narrow legal context.

In Senegal (2023–2024), after the government imposed internet and social-media shutdowns during protests, a civil society coalition led by AfricTivistes filed a case before the ECOWAS Court of Justice (case No. ECW/CCJ/APP/37/23), seeking redress for violations of freedom of expression, information, assembly, and the right to work.[4] The court ruled that the shutdown was arbitrary and unlawful, violating the applicants' human rights, underscoring that regional courts can affirm rights to internet access and information when national governments misuse shutdowns.[5]
In a 2020 precedent, the same court ruled in favour of plaintiffs against Togo for a 2017 shutdown, finding the disruption violated freedom of expression and ordering legal reforms to prevent future shutdowns.[6]

There are documented cases of litigation and court orders restoring internet access after shutdowns or network disruptions. For example, in Sudan (2019), courts ordered telecom providers to restore service after state-imposed shutdowns, following lawsuits by consumer-protection and civic organisations.[7]
Such judgements illustrate that legal remedies tied to public interest litigation and civil society

[3] CIPESA Joins Six Civil Society Organisations in Landmark Case Challenging Internet Shutdowns in Kenya, https://cipesa.org/2025/05/cipesa-joins-six-civil-society-organisations-in-landmark-case-challenging-internet-shutdowns-in-kenya/, accessed Decmber 5, 2025.
[4] Business and Human Rights Centre, Activists filed a lawsuit before the ECOWAS Court of Justice to challenge Internet shutdowns in Senegal, https://www.business-humanrights.org/en/latest-news/activistes-filed-a-lawsuit-before-the-ecowas-court-of-justice-to-challenge-internet-shutdowns-in-senegal/ accessed Decmber 5, 2025.
[5] Premium Times, ECOWAS Court declares Senegal's internet shutdown unlawful,https://www.premiumtimesng.com/foreign/west-africa-foreign/794267-ecowas-court-declares-senegals-internet-shutdown-unlawful accessed December 5, 2025.
[6] Media Defence, Landmark Judgment: ECOWAS Court Finds Togo Violated FoE with Internet Shutdown,https://www.mediadefence.org/news/landmark-judgment-ecowas-court-finds-togo-violated-foe-with-internet-shutdown/ accessed December 5, 2025.
[7] CIPSA, Litigating Internet Disruptions in Africa: Lessons from Sudan, https://cipesa.org/2022/03/litigating-internet-disruptions-in-africa-lessons-from-sudan/ accessed December 6, 2025.

SECTION 05 TOOLS FOR ADVOCACY

Advocacy requires not only vision and strategy but also the right set of tools. These tools enable advocates to act effectively in legal spaces, policy-making, the media, and communities. In digital rights work, combining these approaches ensures stronger, more inclusive outcomes.

5.1 Legal Tools: Litigation and Legal Aid

Strategic Litigation

Litigation can create precedent, repeal repressive laws, and affirm rights. Strategic litigation means selecting cases that will have systemic impact, not just individual relief.[8]

- Example: Challenging unconstitutional provisions of existing laws that can be misapplied. For instance in Uganda, on 10 January 2023, the constitutional court struck down Section 25 of the National Computer Misuse Act, the provision criminalizing "offensive communication." The court found the clause "vague, overly broad and ambiguous," and held that its enforcement violated constitutional protections for free speech and access to information.[9]

  In ASUTIC v. Republic of Senegal, the ECOWAS Court held that the government's shutdown of internet and social media during protests violated the rights to freedom of expression and access to information under regional and international human rights instruments.[10]

- Impact: A judicial decision that digital rights are for all citizens.
- Provide comparative judicial decisions from other jurisdictions to serve as guiding jurisprudence for judicial officers

Public Interest Litigation (PIL)

Where available, PIL allows NGOs or individuals to sue on behalf of affected groups (e.g., victims

[8] Media Defence, Litigating Digital Rights Cases in Africa, https://www.mediadefence.org/resource-hub/litigating-digital-rights-cases-in-africa/ accessed December 6, 2025.
[9] Committee to Protect Journalists, Ugandan constitutional court strikes down criminalization of 'offensive communication', https://cpj.org/2023/01/ugandan-constitutional-court-strikes-down-criminalization-of-offensive-communication/ accessed December 6, 2025.
[10] Global Freedom of Expression (Columbia University), A SUTIC v. Senegal https://globalfreedomofexpression.columbia.edu/cases/asutic-v-senegal/ accessed December 6, 2025.

of an internet shutdown).For Instance: ASUTIC v. Republic of Senegal ECW/CCJ/JUD/29/25,[11] Amnesty International Togo & Others v. Togo- ECOWAS Court of Justice, Amnesty International Togo and others v The Togolese Republic Judgment no ECW/CCJ/JUD/09/20 (25 June 2020), ECOWAS Court of Justice, Association des Blogueurs de Guinée (ABLOGUI) and others v The State of Guinea, Judgment no. ECW/CCJ/JUD/38/23/22 (31 October 2023), among others.

Legal Aid and Pro Bono Support

Access to justice requires ensuring that victims of digital rights violations have access or capacity to seek redress. Legal aid programs and pro bono lawyers are essential for defending journalists, activists, or ordinary citizens targeted for online speech.

Practical Tips for Legal Professionals:

- Frame cases within both domestic law and international human rights standards.
- Partner with civil society to strengthen litigation with advocacy.
- Document jurisprudence for use in future cases.

5.2 Policy Tools: Submissions, Consultations, and Reform Campaigns

Laws and regulations shape digital rights. Engaging in policy advocacy ensures reforms are inclusive and rights-respecting.

Policy Submissions

- Draft position papers for parliamentary committees, regulators, ministries, etc.
- Provide a comparative analysis of best practices from other jurisdictions.
- Well researched policy briefs that are specific, relevant, measurable and attainable.

Public Consultations

- Participate in government consultations on draft issues. For example: cyber laws, Digital Rights bill, AI bills, or digital economy strategies.
- Mobilize citizens to submit inputs collectively.
- Awareness and feedback collection from grassroots communities

Reform Campaigns

- Advocate for repealing vague or repressive laws (e.g., “fake news” provisions).
- Push for adoption of inclusive digital rights policies (e.g., universal broadband, data protection frameworks).

[11] Ibid.

Practical Tips for Civil Society:

- Simplify complex legal issues into clear, accessible language for decision-makers.
- Build coalitions across sectors (lawyers, journalists, technologists).
- Use research evidence to back up proposals.

5.3 Media and Communications Tools

The media is a powerful amplifier for advocacy. By shaping narratives, advocates can mobilize public opinion and influence policymakers.

Traditional Media:

- Press releases, op-eds, opinion pieces, interviews to highlight digital rights issues.
- Partnering with investigative journalists to expose abuses (e.g., surveillance, shutdowns).
- Engagement with cultural custodians

Digital Media:

- Social media campaigns using hashtags and visuals.
- Short videos or infographics explaining rights and violations.
- Online petitions to gather citizen support.
- Digital formats that targets grassroots people

Framing Matters:

- Rights-based framing: *"Shutdowns violate human rights and harm economies." "Digital Rights are Human Rights"*
- Human stories: *"During the shutdown, farmers couldn't sell their produce online."*
- Data-driven: *"Each day of shutdown costs $1.5M in lost productivity."*

5.4 Grassroots Organizing and Coalition Building

At the core of advocacy is people power. Grassroots mobilization ensures advocacy reflects real community needs and builds legitimacy.

Grassroots Tools:

- Community forums to discuss digital rights in local languages (Indigenous rights, translation and adaptation rights, international Cultural Heritage as it applies to cultural preservation)
- Leveraging traditional institutions
- Digital literacy workshops (privacy, security, online safety).
- Rapid response networks during crises (e.g., reporting shutdowns).

Coalition Building:

- Cross-sector alliances: human rights groups, women's organizations, organisations that cater to social diversity, labor unions, tech hubs.
- Regional coalitions: e.g., African civil society working together on AU-level digital policies.
- International solidarity: leveraging global organizations for pressure and visibility.

Practical Tips for Grassroots Advocates:

- Center marginalized voices in campaigns (women, rural communities, persons with disabilities).
- Use local examples to connect digital rights to daily life.
- Ensure the security and safety of activists, both online and offline.

5.5 Integrating Tools for Impact

The most effective advocacy combines these tools:

- **Litigation + Media:** Court cases amplified by media campaigns to build public pressure.
- **Policy + Grassroots:** Policy submissions backed by grassroots mobilization to show legitimacy.
- **Coalition + Litigation:** Regional coalitions filing amicus briefs in strategic and public interest litigation cases.

Digital rights advocacy is strongest when legal, policy, media, and grassroots strategies are used together.

5.6 Digital Rights Monitoring Tools

These tools are very important for tracking digital rights violations, which can determine the health of civic space in a country.
Examples

- Closing spaces database (Space4Change), Civicus Monitor, Accessnow, Ripoti by Paradigm Initiative, Kuram by TechHer ng,Open Observatory of Network Interference (OONI).

SECTION 06

INCLUSIVE POLICY FRAMEWORKS

Digital rights advocacy is only effective when it is inclusive. Too often, marginalized groups such as women, youth, people with disabilities, rural communities, older persons and ethnic minorities are excluded from decision-making on digital policy. An inclusive framework ensures that all people can access, enjoy, and shape their digital rights.

6.1 What Inclusive Policy-Making Means

Inclusive policy-making is participatory, equitable, and responsive to the needs of diverse groups. This means:

- Policies that do not discriminate in access to technology or online spaces.
- Mechanisms that allow meaningful participation in drafting laws and policies.
- Safeguards that protect vulnerable groups from online harms.

Why it matters:

- Exclusion leads to laws that fail to reflect lived realities.
- Inclusivity builds legitimacy and public trust in governance.
- Inclusive policies strengthen democracy and civic space.

6.2 Ensuring Marginalized Voices in Digital Rights Advocacy

To achieve inclusive digital rights advocacy:

- **Representation:** Ensure women, youth, rural actors, and minorities are represented in advocacy coalitions.
- **Consultation:** Conduct participatory consultations with affected groups before drafting policy positions.
- Public Awareness and Education
- **Accessibility:** Translate materials into local languages and make them available in accessible formats (Braille, audio).

- **Empowerment:** Provide digital literacy training to communities to enable meaningful participation.

6.3 Gender-Responsive Digital Policy

Challenges:

- Women face disproportionate barriers: cost of access, digital literacy gaps, and exposure to online gender-based violence (OGBV).
- Policy processes are often male-dominated.

Strategies:

- Conduct gender impact assessments before passing digital laws.
- Ensure laws address OGBV with clear reporting, redress, and enforcement mechanisms.
- Support women-led organizations to participate in digital rights advocacy.
- Promote safe spaces online where women and girls can organize without harassment.

6.4 Youth Participation

Young people are often the most active users of digital spaces, yet their voices are overlooked in policymaking.

Strategies:

- Include youth representatives in policy consultations.
- Encourage youth-driven publications.
- Support youth-led digital rights campaigns and innovations.
- Provide civic education on digital rights in schools and universities.
- Create mentorship opportunities linking youth advocates with experienced legal and civil society actors.

6.5 Disability and Digital Inclusion

Persons with disabilities face exclusion due to inaccessible technology, websites, and policies that overlook their needs.

Strategies:

- Mandate accessibility standards (Web Content Accessibility Guidelines).
- Require government and corporate platforms to provide accessibility features (screen readers, captions, sign language).

- Involve disability rights organizations in all digital policy processes.
- Ensure affordability of assistive technologies.

6.6 Minority and Rural Communities

Ethnic, linguistic, and rural communities often lack reliable internet, making digital exclusion structural.

Strategies:

- Advocate for universal service funds to expand affordable internet to underserved areas.
- Promote local-language content and platforms.
- Support community networks as alternatives in hard-to-reach regions.
- Ensure representation of rural communities in consultations.

6.7 From Principles to Practice

To ensure inclusivity in practice:

1. **Audit:** Review digital laws and policies for inclusivity gaps.
2. **Participate:** Include marginalized groups in advocacy coalitions.
3. **Advocate:** Push governments to adopt inclusive consultation mechanisms.
4. **Monitor:** Track the impact of digital policies on different groups.

Example: A coalition campaigning against online harassment in Nigeria included women-led organizations, youth groups, and disability rights actors. Their diversity strengthened the campaign's credibility and ensured the resulting draft bill was more inclusive.

SECTION

07

PRACTICAL ADVOCACY STRATEGIES

This section provides step-by-step approaches for tackling some of the most pressing digital rights challenges. These strategies draw from real-world campaigns and are designed to be adaptable across different contexts.

7.1 Campaigning Against Internet Shutdowns

The Problem:
Governments increasingly resort to internet shutdowns to suppress protests, elections monitoring, or dissent. Shutdowns harm rights and economies.

Strategies:

1. **Documentation:** Collect evidence of shutdowns such as dates, duration, economic impact, human stories. (Eg partner with organizations that collect pictorial evidence, such as WITNESS).
2. **Litigation:** File lawsuits arguing shutdowns violate constitutional rights (expression, assembly, access to information).
3. Ascertain the law under which the shutdown was ordered. Identify the main actors and the basis of their actions. Apportion responsibility and blame, while also identifying redress mechanisms and accessibility.
4. **Public Awareness:** Extensive use of social media and traditional media, use of technological tools for accessing transparent information(Budgit and KDI A.I tools) Launch campaigns highlighting economic and human costs. For example: "#KeepItOn" campaign mobilized global solidarity.
5. **International Pressure:** Apply for sanctions, Engage African Union, UN, and donors to pressure governments.
6. **Coalition Action:** Build regional solidarity networks to resist shutdowns collectively.

7.2 Advocacy Against Repressive Laws

The Problem:
Misapplication and the excessive use of police discretion in interpreting laws pose a great threat to digital rights and the civic space.

Strategies:

1. **Legal Analysis:** Identify problematic provisions in legislation (e.g., vague definitions of some offences such as the publication of false statements, false news, defamation, etc.).
2. **Policy Engagement:** Submit reform proposals or repeal requests to legislators.
3. **Research:** Identify parties affected by the offensive provisions e.g journalist charged or jailed under the provisions.
4. **Strategic Litigation:** Identify parties affected by the offensive provisions e.g journalist charged or jailed under the provisions and challenge unconstitutional provisions in courts.
5. **Media Advocacy:** Use cases of journalists or activists targeted to humanize the issue.
6. **Grassroots Mobilization:** Organize town halls and social media campaigns to inform citizens.

7.3 Addressing Online Gender-Based Violence (OGBV)

The Problem:
Women and marginalized groups face harassment, threats, and abuse online, often with no legal remedy, injustice to other social diversity.

Strategies:

1. **Legal Reform:** Advocate for explicit recognition of OGBV in cyber laws.
2. **Support Systems:** Develop reporting platforms, partner with already existing reporting systems, and legal aid programs for survivors.
3. **Awareness:** Campaigns to shift public perception of OGBV as a serious rights violation.
4. **Engage Platforms:** Pressure social media companies to improve reporting and content moderation.
5. **Digital Safety Training:** Equip women and marginalized groups with tools to stay safe online.

7.4 Engaging Policymakers and International Bodies

The Problem:
Policymakers often lack awareness of digital rights issues, while international bodies can exert pressure but need evidence and advocacy.

Strategies:

1. **Direct Engagement:** Request meetings with legislators, regulators, ministries, the executive, etc.
2. **Policy Briefs:** Share short, evidence-based briefs highlighting the issue and recommendations.

3. **International Advocacy:** Submit shadow reports to UN treaty bodies, African Commission, or UPR processes.
4. **Leverage Diplomacy:** Work with foreign missions and donor agencies to raise concerns.
5. **Track Commitments:** Hold governments accountable for regional or global commitments (e.g., ACHPR resolutions).

7.5 Digital Safety and Security for Advocates

The Problem:
Advocates themselves are often targeted through surveillance, hacking, or harassment.

Strategies:

1. **Risk Assessment:** Identify threats specific to your context.
2. **Digital Hygiene:** Use secure passwords, two-factor authentication, encrypted communications.
3. **Capacity Building:** Train activists in digital security basics.
4. **Incident Response:** Have a rapid response plan for breaches or threats.
5. **Holistic Security:** Combine digital, physical, and psychosocial safety measures.

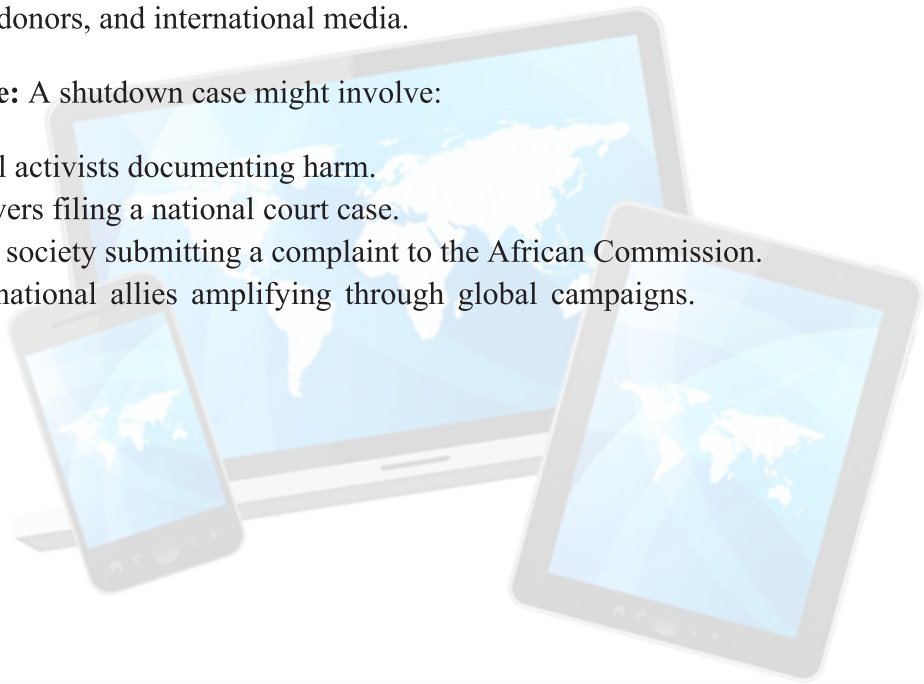
7.6 Building Multi-Level Strategies

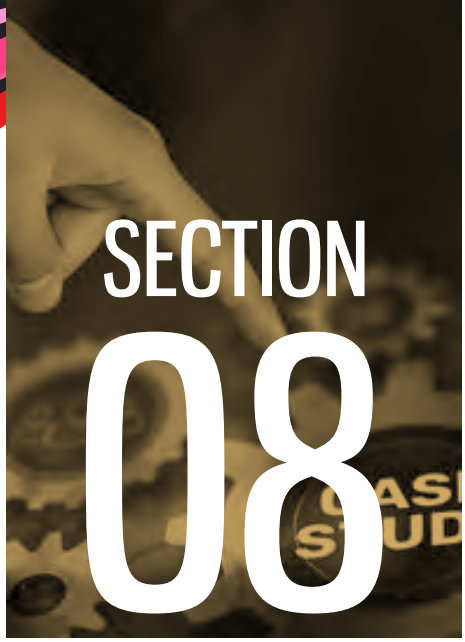
The strongest advocacy is multi-level:

- **Local:** Mobilize communities and grassroots advocates.
- **National:** Engage courts, parliaments, and regulators.
- **Regional:** Use regional mechanisms, such as ECOWAS, EAC, SADC, AU mechanisms.
- **Global:** Engage international human rights mechanisms, such as, Special Rapporteurs, UN, donors, and international media.

For example: A shutdown case might involve:

- Local activists documenting harm.
- Lawyers filing a national court case.
- Civil society submitting a complaint to the African Commission.
- International allies amplifying through global campaigns.





CASE STUDIES

Case studies demonstrate how strategies discussed earlier have been successfully applied in Africa and globally. They highlight lessons learned and practical takeaways for future advocacy.

8.1 Strategic Litigation Against Internet Shutdowns in Africa

Context:

In September 2017, during widespread anti-government protests in Togo, the government shut down mobile internet and social media platforms across the country for several days. The blackout limited citizens' ability to organize, restricted journalists' work, and suppressed access to information in a period of political tension.

Action Taken

A coalition of civil-society organizations, including Amnesty International Togo, associations of journalists, and other digital-rights advocates, filed a case before the ECOWAS Court of Justice, arguing that the shutdown violated the rights to freedom of expression and access to information guaranteed under the African Charter and other regional instruments. They presented technical evidence, affidavits from affected citizens, and expert testimonies on the human-rights and economic impact of the shutdown.

Outcome

In its June 2020 judgment, the ECOWAS Court held that the internet shutdown was unlawful, arbitrary, and disproportionate, finding that it violated Article 9 of the African Charter on Human and Peoples' Rights. The Court ordered the Togolese government to pay compensation to the applicants, adopt measures to prevent future shutdowns, and align national laws with regional human-rights standards,setting a major precedent for digital-rights litigation across West Africa.

Lesson:
The case shows that strategic regional litigation, supported by solid civil-society evidence, can successfully challenge unlawful internet shutdowns and reinforce that access to the internet is a fundamental component of freedom of expression.

8.2 Challenging Repressive Cybercrime Laws

Context:
In Nigeria, the 2015 Cybercrimes Act (especially its original Section 24) criminalized vague offences including "grossly offensive" messages or messages sent "knowing it to be false" for purposes such as causing "annoyance, inconvenience, danger … insult … or needless anxiety." Activists, journalists, and bloggers argued that the law was used to harass, intimidate, and prosecute legitimate expression.[12] In one of the high-profile attempts to challenge the constitutionality of Section 24 occurred in the case Okedara v. Attorney General, CA/L/174/18- the Court of Appeal in Lagos dismissed the challenge in 2017, holding that the provision was clear enough and within the constitution's permissible restrictions on expression.[13]

Separately, a related case was filed at the ECOWAS Community Court of Justice, which in its judgment found that certain provisions of the Cybercrime Act, specifically Section 24, violated the right to freedom of expression under international law and ordered the Nigerian government to repeal or amend that section.[14]

Action:

- Lawyers, with civil society support, filed constitutional challenges.
- Advocacy groups launched campaigns highlighting cases where the law was abused.
- Media engagement amplified personal stories of affected activists.

Outcome:
The constitutionality of some provisions, like Section 24, has been questioned in court, though the provision remains in effect. Though it was amended in 2024 to refine the language, some parts of Act still remain broad enough to potentially impact free expression and invite subjective interpretation

Lesson:
Strategic litigation supported by grassroots storytelling humanizes complex legal issues. Advocacy is a long term commitment, celebrating small wins.

---

[12] Aljazeera, Nigeria's cybercrime reforms leave journalists at risk, https://www.aljazeera.com/opinions/2024/4/20/nigerias-cybercrime-reforms-leave-journalists-at-risk accessed December 7, 2025.
[13] Global Freedom of Expression (Columbia Law), https://globalfreedomofexpression.columbia.edu/cases/okedara-v-attorney-general/, accessed December 7, 2025.
[14] Incorporated Trustees of Laws and Rights Awareness Initiatives v Federal Republic of Nigeria (ECW/CCJ/APP/53/2018; ECW/CCJ/JUD/16/20) [2020] ECOWASCJ 6 (10 July 2020) https://africanlii.org/fr/akn/aa-au/judgment/ecowascj/2020/6/eng@2020-07-10#:~:text=1.,Olumide%20Babalola%2C%20Esq.&text=3.,Court%20on%207th%20February%202020. accessed December 7, 2025.

8.3 Combating Online Gender-Based Violence (OGBV) in Kenya

Context:
Women politicians and activists in Kenya were subjected to widespread online harassment, especially during elections.[15]

Action:
Civil society organizations documented OGBV cases and presented evidence to parliament. They collaborated with tech companies to improve reporting channels and launched public awareness campaigns.[16]

Outcome:

- Some lawmakers and commissions, such as Kenya's National Gender and Equality Commission (NGEC), acknowledged the problem and considered reviewing cyber laws to include OGBV protections
- Women candidates and elected officials received training on how to protect their digital identities, manage harassment, and report abuse effectively.
- Platforms such as Google piloted tailored safety and moderation tools for East Africa, improving reporting channels.
- Civil society campaigns and research reports highlighted the scale of OGBV, showing that harassment was widespread during elections.

Lesson:
Advocacy is strongest when it combines law reform, survivor support, and platform accountability.

8.4 Digital Rights in Regional Courts: ECOWAS Case

Context:
In 2017, during political protests in Togo, authorities shut down the internet. National courts were unresponsive.[17]

[15] Westminster Foundation for Democracy (WFD), Policy briefs: Violence against women in politics in Kenya, https://www.wfd.org/what-we-do/resources/policy-briefs-violence-against-women-politics-kenya#:~:text=Despite%20constitutional%20and%20legal%20frameworks%20supporting%20gender,and%20pervasive%20cultures%20of%20patriarchy%20and%20impunity, accessed December 7, 2025.
[16] Citizen Digital, Google partners with women legislators to tame online trolls during elections, https://www.citizen.digital/article/google-partners-with-women-legislators-to-tame-online-trolls-during-elections-n295447 accessed December 7, 2025.
[17] Amnesty International, Togo V The Republic Of Togo ECW/CCJ/APP/61/18.

Action:
Civil society organizations escalated the case to the ECOWAS Court of Justice, arguing that shutdowns violated the right to freedom of expression and access to information.

Outcome:
The ECOWAS Court ruled against the government, setting a binding precedent across West Africa that internet shutdowns violate human rights.

Lesson:
Regional mechanisms can be powerful when national courts fail.

8.5 Grassroots Digital Rights Advocacy in Cameroon

Context:
In 2017, the Anglophone regions in Cameroon experienced one of the longest internet shutdowns in Africa.[18]

Action:
Grassroots groups documented the shutdown's impact on students, hospitals, and small businesses. They shared testimonies via international media and collaborated with diaspora networks to amplify the campaign.

Outcome:
While the shutdown lasted months, the advocacy forced international pressure on the government and generated strong precedents for documenting harms of shutdowns.

Lesson:
Grassroots documentation and storytelling are essential, especially when formal legal remedies are weak.

8.6 Global Example: GDPR and Data Protection Advocacy in Europe

Context:
Europe faced growing privacy challenges due to technological advancements, cross-border data flows, and the widespread collection of personal information. The existing 1995 Data Protection Directive was outdated and insufficient to protect individuals' privacy in the digital era. Civil society groups, privacy advocates, and regulatory bodies recognized the need for a modern,

[18] Access Now, Access Now files new legal intervention in Cameroon against shutdowns, https://www.accessnow.org/press-release/access-now-files-supporting-intervention-in-renewed-legal-challenge-to-internet-shutdown-in-cameroon/ ; Internet Without Borders,New Internet shutdown ordered in Cameroon - Internet Sans Frontières, https://internetwithoutborders.org/new-internet-shutdown-ordered-in-cameroon/ accessed December 7, 2025.

enforceable framework to secure personal data rights. These civil society groups campaigned for stronger data protection laws in the EU, resulting in the General Data Protection Regulation (GDPR).

Action:

- Coalition advocacy across EU states.
- Strategic engagement with lawmakers.
- Strong public communication on why data privacy matters.

Outcome:
GDPR became the world's strongest data protection framework, inspiring laws globally (including in Africa).

Lesson:
Sustained coalition-building and public engagement can lead to transformative policy reforms.

8. 7 Key Takeaways from Case Studies

1. Documentation is powerful: Without evidence, advocacy struggles to gain traction.
2. Litigation works best with public campaigns: Legal action alone may not pressure governments.

3. Regional and international mechanisms matter: When domestic systems fail, look outward.
4. Grassroots voices humanize the struggle: Stories from affected communities resonate globally.
5. Coalitions create strength: No single actor can shift digital rights alone.

SECTION 09

TOOLS AND RESOURCES

This section provides practical tools to support digital rights advocacy. They can be adapted depending on your context, whether you are a lawyer preparing litigation, a civil society actor leading a campaign, or a grassroots advocate mobilizing your community.

9.1 Internet Shutdown Documentation Checklist

When documenting a shutdown, ensure you gather:

CATEGORY	DATA / EVIDENCE TO COLLECT
Basic Facts	○ Date and time shutdown began/ended ○ Geographic areas affected ○ Type of shutdown (social media block, complete blackout, bandwidth throttling)
Evidence Sources	○ Reports from affected users ○ Network measurement tools (e.g., OONI, NetBlocks) ○ Screenshots of error messages
Impact Assessment	○ Business losses (SMEs, mobile money, startups) ○ Education disruptions (students unable to access online resources) ○ Health sector impact (hospitals unable to communicate) ○ Human rights violations (protests disrupted, activists silenced)

Storytelling	○ Collect testimonies from individuals ○ Record video/audio interviews where safe ○ Translate stories for broader audiences

9.2 Advocacy Brief Template

A simple structure for advocacy briefs:

1. **Title** – Short and clear (e.g., *"Internet Shutdowns Harm Democracy and Business"*).
2. **Background** – Describe the issue briefly.
3. **Problem Statement** – Why this matters (legal, economic, social impacts).
4. **Evidence** – Key facts, case studies, testimonies, statistics.
5. **Legal/Policy Framework** – Cite relevant constitutional, regional, and international instruments.
6. **Recommendations** – What decision-makers should do (clear, actionable steps).
7. **Call to Action** – Specific appeal (e.g., repeal a law, stop shutdowns, pass a bill).

9.3 Litigation Strategy Checklist

For legal professionals considering strategic litigation:

CATEGORY	DATA / EVIDENCE TO COLLECT
Pre-litigation Research	○ Identify victims/clients willing to come forward ○ Analyze relevant laws and possible constitutional challenges ○ Review past judgments in local and regional courts
Building the Case	○ Collect evidence- statements,, testimonies, and expert reports ○ Partner with technical experts (to explain shutdowns or surveillance)

	○ Document economic and social impact evidence
Allies and Support	○ Build coalitions with civil society groups ○ Engage media to amplify the case ○ Connect with international advocacy groups for solidarity
After the Judgment	○ Publicize the outcome widely ○ Monitor government compliance ○ Leverage the ruling for broader reforms ○ Appeal unfavourable judgments where necessary.

9.4 Digital Security Checklist for Advocates

To reduce the risk of surveillance, hacking, or harassment:

- Use two-factor authentication on all accounts
- Install encrypted messaging apps (Signal, WhatsApp)
- Regularly update devices and apps
- Use VPNs during sensitive activities
- Store files securely (encrypted drives/clouds)
- Back up important evidence offline
- Be cautious of phishing emails or suspicious links
- Conduct regular security trainings for your team

9.5 Stakeholder Mapping Worksheet

When planning advocacy, map out:

- **Primary Targets:** Who has the power to change the law/policy? (e.g., legislators, regulators, the Executive, courts).
- **Secondary Targets:** Who influences the decision-makers? (e.g., media, donors, international bodies)
- **Allies:** Civil society groups, tech companies, grassroots leaders, professional associations
- **Opponents:** Actors who may resist change (e.g., government agencies, security forces)

- **Neutral Parties:** Groups you can educate and bring to your side

9.6 Metrics for measuring and mapping advocacy

This is critical for identifying and tracking outcomes.

1. User Engagements: This is to account and track how actively people are interacting with the advocacy message offline and online. This includes, web connection, social media interaction, content interaction, online participation, physical availability:

    - **Website analytics:** Monitoring visits to campaign landing pages, petition pages, or information portals using tools like Google Analytics.
    - Social media engagement on posts, campaigns, flyers, etc. Tracking likes, shares, comments, hashtag usage, and overall reach or impressions.
    - **Active Participation Rate:** Measuring specific actions such as the number of volunteers recruited, hours contributed, petition signatures collected, or event attendance at rallies or webinars.
    - **Email Analytics:** Tracking open rates, click-through rates, and conversion rates from advocacy-focused emails.

2. Impact: This aims to measure influence and behavioral shifts:

    - Media: tracking articles, TV segments, or blog posts that mention your message in order to amplify it.
    - Interactions: tracking comments, discourse, arguments, debates, sentiments, and other engagements related to the cause/message.
    - **Behavioral Influence:** Tracking changes in public habits. For example, a recycling campaign might measure increased recycling rates in targeted areas.
    - **User-Generated Content (UGC):** Quantifying the volume and positive nature of reviews, testimonials, photos, and videos created by advocates.

3. Outcomes: This is connected to the overall message. It measures data to ascertain if desired results were achieved by a message/program/event/campaign, etc. It distinguishes true success from just activities by assessing changes in behaviour, knowledge or condition.
    - **Policy/Legislative Changes:** Did the advocacy successfully influence a new law, regulation, or specific legislative votes?
    - **Net Promoter Score (NPS):** Assesses how likely individuals are to recommend the organization or cause to others, reflecting the strength and potential of advocacy support.
    - **Referral Rate/Conversions:** Monitoring the number of new supporters or participants gained through referrals, providing a measurable indicator of advocacy impact.

- **Funds Mobilized:** Tracks donations, grants, or financial contributions generated directly from advocacy activities.
- **Supporter Lifetime Value (SLV):** Evaluates the long-term engagement and contributions of advocates, including retention and overall value to the organization.

9.7 Key Digital Rights Resources

- **Measurement & Evidence**
  - OONI – Open Observatory of Network Interference
  - NetBlocks – Internet shutdown monitoring
- **Advocacy Networks**
  - #KeepItOn Coalition
  - African Declaration on Internet Rights and Freedoms
- **Legal Frameworks**
  - African Charter on Human and Peoples' Rights (ACHPR)
  - International Covenant on Civil and Political Rights (ICCPR)
  - UN Human Rights Council Resolution on Internet Shutdowns
- **Digital Security**
  - Security in a Box
  - Access Now Digital Security Helpline

SECTION 10

CONCLUSION & NEXT STEPS

Digital rights are no longer abstract legal principles. They are central to how we communicate, organize, work, and participate in democracy. Protecting these rights requires coordinated efforts from lawyers, civil society, grassroots advocates, and everyday citizens. This toolkit has outlined the legal frameworks, advocacy strategies, case studies, and practical tools needed to advance digital rights in Africa and beyond.

10.1 Key Lessons

1. **Digital rights = human rights:** Access to the internet, privacy, freedom of expression, and assembly must be protected online just as offline.
2. **Multi-level advocacy works best:** Success comes when local action is linked with national, regional, and global efforts.
3. **Evidence and storytelling are powerful:** Documenting violations and amplifying human stories makes the legal and policy arguments stronger.
4. **Security matters:** Protecting advocates and victims is essential for sustainable activism.
5. **Coalitions are stronger than individuals:** Lasting change requires partnerships across sectors.

10.2 Next Steps for various Stakeholders

For Legal Professionals

- Pursue strategic litigation that sets precedents for digital rights.
- Provide pro bono support to victims of online violations.
- Engage with policymakers to draft rights-respecting legislation.

For Civil Society Organizations

- Build broad-based coalitions to amplify advocacy.

- Monitor digital rights violations and publish evidence-based reports.
- Develop public education campaigns on internet freedom and privacy.

For Grassroots Advocates

- Mobilize communities to resist repressive laws and shutdowns.
- Collect testimonies and stories that humanize digital rights struggles.
- Train communities in digital security and safe online practices.

For Members of the General Public

- Learn your digital rights and demand accountability from the government and companies.
- Practice good digital security to protect your data and communications.
- Participate in advocacy campaigns, your voice matters.

10.3 Building Inclusive Policy Frameworks

The future of digital rights depends on inclusive, participatory policy-making. Governments, regulators, civil society, and citizens must co-create laws and policies that balance security with freedom. This requires:

- Transparency in law-making processes.
- Public consultations with diverse communities.
- Accountability mechanisms for state and corporate actors.
- Ongoing monitoring of implementation and enforcement.

10.4 Call to Action

Every shutdown challenged, every law reformed, every voice raised online or offline contributes to a stronger civic space. Advocacy is not the role of one group alone, it requires collective action.

- **Lawyers:** Use the courts as a shield and a sword.
- **Civil society:** Keep building movements that resist repression.
- **Grassroots advocates:** Stand as the voice of communities often left out of digital policy debates.
- **Citizens:** Claim your rights and hold leaders accountable.

Digital rights are not gifts, they are rights to be demanded, defended, and expanded.

ANNEXURES
PRACTICAL ADVOCACY TOOLS

1. Advocacy Cycle Tools

These tools streamline the planning and implementation of the six-stage advocacy cycle.

1.1. Issue Identification & Prioritization Matrix

This tool helps define and test the viability of a potential advocacy issue.

Criterion	Score (1-5)	Rationale	Actionability Check
Timeliness (Is it a current/impending threat?)			Is there a legislative window or an immediate threat, and at what level is the impact/severity? Why should we prioritize, and what can happen if we do not?
Relevance (Impact on target community/rights)			Can we clearly articulate the harm?
Actionability (Can we realistically achieve change?)			Are there clear decision-makers to target?
Coalition Potential (Can we find strong allies?)			Who are the likely allies/opponents?

Resource Match (Do we have the capacity/skills?)			Do we need to fundraise/recruit specific skills (e.g., lawyers)?
Total Score (Max 25)			**Decision:** (Proceed/Re-scope/Park)

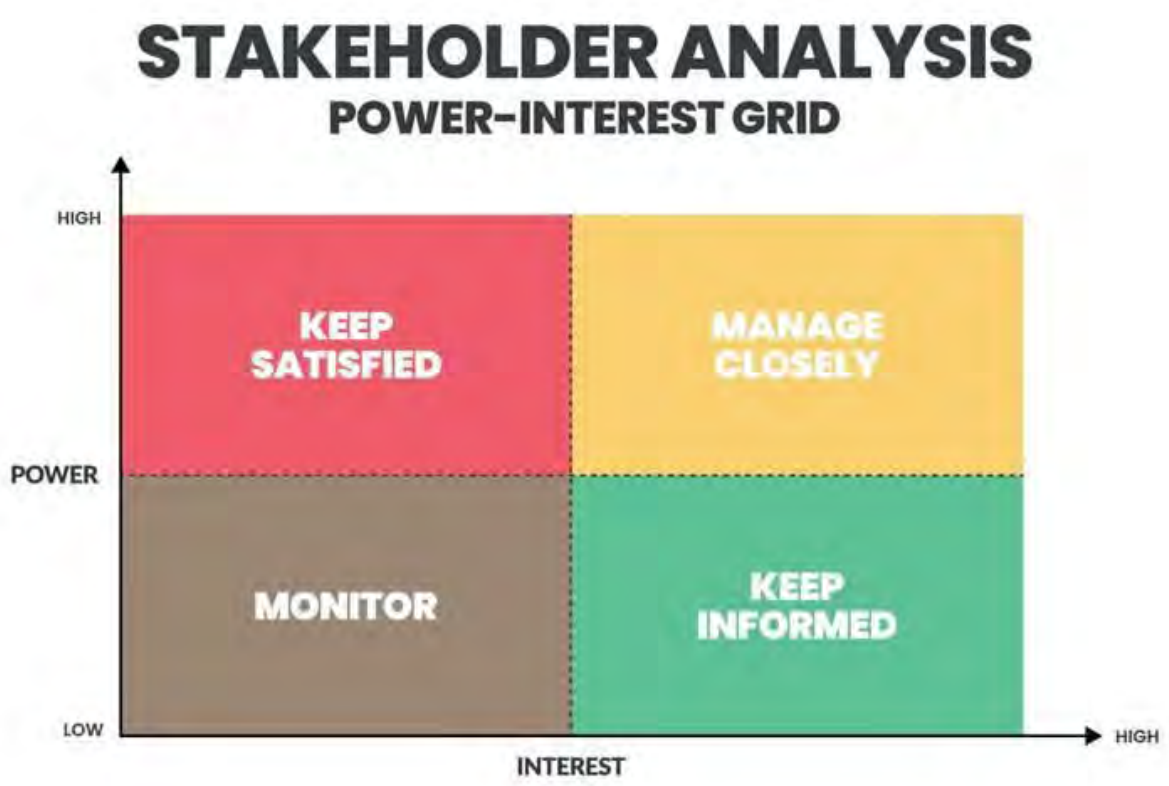
1.2. Goal-Objective-Activity (GOA) Tracker

This tool ensures objectives are **S**pecific, **M**easurable, **A**chievable, **R**elevant, and **T**ime-bound (**SMART**).

Component	Example (Cybercrime Law Reform)	SMART Check (Y/N)
Goal (Broad Change)	The restrictive Section (section 24) of the Cybercrime Act is repealed.	N/A (Broad)
Objective 1 (Specific Step)	By **Q4 2025**, file a **Strategic Litigation** case challenging Section 24 in the High Court.	Yes
Activity 1.1 (Action)	Draft the legal brief and gather affidavits from 3 victims by Q3 2025.	Y
Activity 1.2 (Action)	Secure pro-bono representation from a reputable law firm.	Y
Objective 2 (Specific Step)	**Mobilize 5 key parliamentarians** to table an amendment motion by **Q1 2026**.	Y
Activity 2.1 (Action)	Host a closed-door briefing session for parliamentarians with a legal expert.	Y

2. Stakeholder and Influencer Mapping Tool

This structured approach helps prioritize targets and build alliances.



2.1. Power-Interest Grid & Influence Assessment

Use this grid to plot stakeholders based on their power to affect the outcome and their interest in the issue.

Stakeholder Name	Position (Supportive/Neutral/ Opposed)	Power (Influence) (High/Med/ Low)	Interest (High/Med/ Low)	Action Strategy	Classification

Ministry of Communications	Opposed	High	High	**Target/Engage** (Lobbying, Policy Advocacy)	**Key Player**
Digital Rights Coalition	Supportive	Medium	High	**Ally** (Mobilize, Resource Sharing)	**Keep Fully Engaged**
Private Tech Company	Neutral	High	Medium	**Neutralize /Win Over** (Demonstrate business risk)	**Keep Satisfied**
General Public	Neutral	Low	Medium	**Informer** (Public awareness campaigns)	**Minimum Effort**

3. Evidence Building and Storytelling Resources

These resources standardize evidence collection and maximize the impact of narrative.

3.1. Digital Rights Incident Report Template

A standardized form for documenting violations to ensure all necessary evidence is captured.

Section	Required Information	Documentation Type (local language, audio record)	Security Note

Incident Details	Date, Time, Location, Type of Violation (e.g., Shutdown, Arrest, OGBV)	Text/Chronology	**Secure storage is mandatory.**
Victim/Witness Data	Name (Alias for protection), Contact (Encrypted), Consent to Use Story	Affidavit/Consent Form	**Prioritize victim safety and anonymity.**
Violation Evidence	Screenshots, URLs, Error Messages, Arrest Warrants, Court Filings	Photo/Video/Digital Files	**Use secure channels for transfer (e.g., Pretty Good Privacy-PGP, etc).**
Consequence/Impact	Economic loss, Mental/physical harm, Disruption of services	Testimonies/Statistics	**Quantitative and Qualitative Data.**

3.2. Storytelling Framing Checklist

A guide to transform raw data into a compelling human narrative.

Checkpoint	Goal	Digital Rights Example
Identify the Hero	Center the narrative on a relatable victim or group.	*A single mother who relies on mobile money.*
Define the Villain	Clearly identify the entity responsible for the rights violation.	*The regulator who ordered the internet shutdown.*

Establish the Stakes	What is lost/at risk due to the violation?	*The mother can't pay her child's school fees or buy medicine. Economic, Fundamental human rights, security*
Call to Action (CtA)	What do you want the audience/policymaker to *do*?	*Sign the petition demanding an independent review of shutdown powers. E.g., repealing the Cybercrime Act*
Relate to Universal Values	Connect the digital right to a common value.	*Framing access to the internet as a fundamental right to **dignity** and **economic survival**. Fundamental human rights, security*

4. Monitoring and Evaluation (M&E) Toolkit

This toolkit provides indicators to track success and lessons learned.

4.1. M&E Indicators Dashboard

Advocacy success is measured in outputs (immediate actions) and outcomes (changes in policy/behavior).

Indicator Type	Metric/Indicator	Target (Example)	Data Source	Frequency
Output (Activity completion)	Number of policy briefs submitted to Parliament.	3	Submission Records	Quarterly
Output (Media Reach)	Number of unique media mentions (print/online) of the issue.	50	Media Monitoring Reports	Monthly

Outcome (Policy Change)	Evidence of a legislative or regulatory amendment initiated.	1	Official Gazettes/Parliamentary Records	Ongoing
Outcome (Behavioral Change)	Percentage increase in public awareness of the issue.	15%	Pre- and Post-Campaign Survey	Biannually
Litigation Outcome	Favorable court ruling achieved/New legal precedent set.	1	Court Records/Legal Analysis	After Judgment

4.2. Lessons Learned and Strategy Adjustment Template

This ensures continuous learning and adaptability, a core element of the M&E stage.

Strategy Component	What Worked? (Successes)	What Didn't Work? (Failures/Challenges)	Strategy Adjustment/Lesson Learned
Lobbying			**Action:** (e.g., Switch from direct lobbying to public pressure via media, use of intermediaries (PEA).)
Coalition Building			**Action:** (e.g., Recruit new allies (e.g., PLAC, CISLAC), higher political influence.)
Messaging			**Action:** (e.g., Re-frame the issue using economic impact instead of only human rights.)

Resources			**Action:** (e.g., Allocate more budget to digital advertising over radio and social media, including using social media influencers.)

Suggested Tools for Digital Rights Advocacy

Section	Current Concept	Suggested Practical Tools
5.1 Legal Tools	Strategic Litigation, PIL, Legal Aid, Documenting Jurisprudence.	**Litigation Triage Toolkit:** A standardized form/checklist to quickly assess a potential case's strategic impact (precedent potential, media appeal, cost-benefit). **Amicus Brief Template Library:** A repository of successful amicus curiae (friend of the court) briefs filed in digital rights cases across jurisdictions. **Secure Case Management System:** Encrypted platform (like ProtonMail or specialized legal tech) for handling sensitive client and case information.
5.2 Policy Tools	Policy Submissions, Public Consultations, Reform Campaigns, Research Evidence.	**Policy Brief Generator:** A structured template (e.g., 5-page max) requiring clear sections: Problem, International Standards, Comparative Examples, Proposed Solution, and Cost Analysis. **Legislative Tracker/Alert System:** A tool (using web scraping or APIs from official sources) to monitor the status of relevant bills and automatically alert advocates when a bill is nearing a critical stage (e.g., committee vote, public hearing). **Model Law Components Database:** A searchable database of best-practice clauses for key digital rights areas (e.g., data protection, net neutrality, surveillance oversight) that can be adapted for local policy submissions.

5.3 Media and Communications Tools	Traditional Media, Digital Media, Framing (Human Stories, Data-driven).	**Crisis Comms Playbook (Shutdown/Surveillance):** A pre-approved set of social media posts, press release drafts, and designated media contacts for immediate use during a digital rights crisis (e.g., internet shutdown, mass surveillance revelation). **Data Visualization Template Pack:** Reusable graphic templates (using tools like Canva or Tableau) to quickly turn legal/policy data (e.g., cost of shutdown, surveillance requests) into compelling, shareable infographics. **Testimonial Story Bank:** A secure, consent-based system for collecting and categorizing human impact stories (anonymized if needed) to easily match them with relevant advocacy campaigns and media outreach.
5.4 Grassroots Organizing and Coalition Building	Community Forums, Digital Literacy Workshops, Coalition Building, Centering Marginalized Voices.	**'Know Your Digital Rights' Workshop-in-a-Box:** A standardized, modular curriculum (slides, facilitator notes, hands-on exercises) for teaching digital literacy and safety, adaptable for various community groups and local languages. **Secure Digital Organizing Platform:** A decentralized, privacy-focused tool (e.g., Signal groups, encrypted email lists, or peer-to-peer apps) for safe, rapid mobilization and internal communication among coalition members. **Advocacy Impact Survey Template:** A simple, structured questionnaire for local advocates to collect qualitative and quantitative data on a policy's real-world effect on their community (e.g., before/after policy change data).

5.5 Integrating Tools for Impact: A Practical Example

The Integrated Advocacy Campaign Dashboard

This is a conceptual, high-level tool that acts as a central hub for a complex, multi-pronged campaign:

1. **Objective & Metrics:** Clearly defines the campaign goal (e.g., *Repeal Cybercrime Act's 'Fake News' clause*) and its key performance indicators (KPIs) across all four areas (Legal: *Filing date, Next Hearing*; Policy: *Number of Policy Submissions*; Media: *Media Mentions, Social Reach*; Grassroots: *Number of Mobilized Citizens*).
2. **Shared Calendar:** Integrates legal deadlines (court dates), policy consultation submission cutoffs, and scheduled media drops (op-eds, report launches).
3. Develop a strategic advocacy message to serve as talking points to clearly present key asks
4. **Resource Linker:** Provides quick access to the tools above: the **Amicus Brief Template**, the current **Policy Brief Generator** draft, the **Crisis Comms Playbook**, and the **Workshop-in-a-Box** materials for local training.
5. **Stakeholder Map:** A visual, color-coded chart identifying key decision-makers (judges, legislators, regulators), their known positions, and the targeted advocacy effort for each (e.g., *Legislator X: Target with Grassroots petition and Policy Submission*).

Digicivic initiative is a public interest driven non-governmental human rights organization that expands the frontiers of digital rights and civic participation in Africa. It is established to organize Public Interest actions, Strategic Litigation, Training and Advocacy for the promotion and preservation of digital rights and the civic space. **Digicivic Initiative** provides legal support for different groups, ranging from journalists, bloggers, independent media, human rights defenders, rights activists, and the public in cases involving privacy, data protection, digital assets, freedom of expression, association and assembly (online and offline), cyber harassment and all other digital rights abuses, while ensuring that citizens can freely access information, engage in public discourse and debate, meet and organize, build cohesion beyond politics and elections to ensure that governments are responsive and accountable.

Digicivicinitiatives@gmail.com **Digicivic Initiatives**

Sponsored by:
Luminate
Building Strong Societies