

DIGITAL RIGHTS MANUAL FOR BEGINNERS



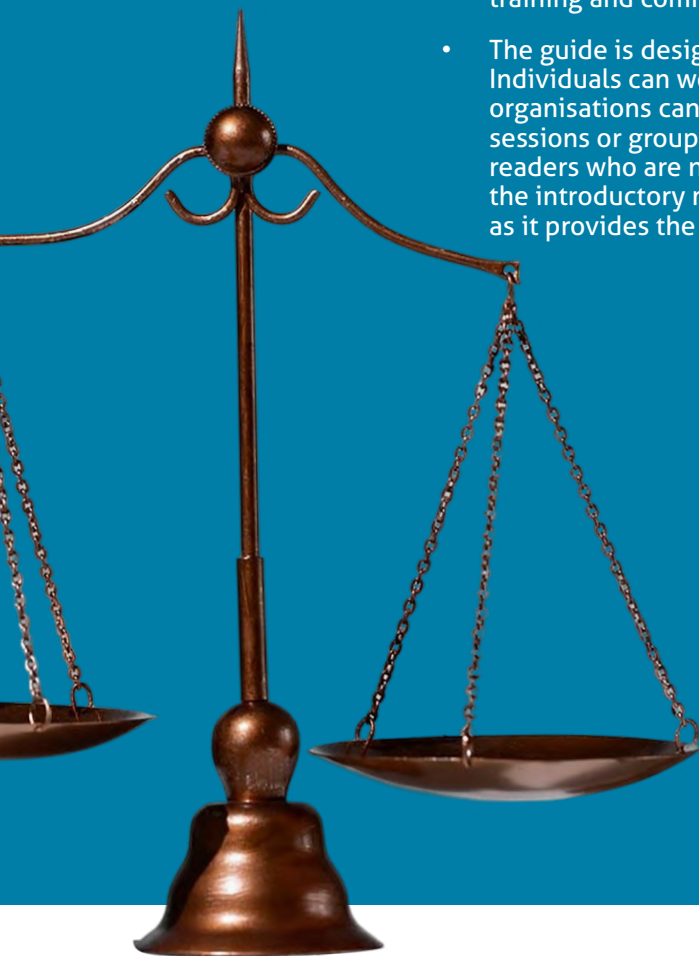


Contents

Introduction	4
Module 1 : Introduction to Digital Rights.....	5
Module 2 : Freedom of Expression in the Digital Space	13
Module 3 : Inclusion and access	19
Module 4 : Online Safety and Security	25
Module 5 : Advocacy for Digital Rights	29
Module 6 : Empowerment through training and community engagement	33
Module 7 : Emerging technologies	43
Appendices and resources.....	49
Editorial team	55

Introduction

- This guide was developed as an entry point to anyone new to digital rights. It aims to help readers understand what digital rights are, why they matter, and how civil society can play an active role in protecting and promoting them. It is intended for civil society organisations, community groups, human rights defenders, journalists, activists and anyone interested in understanding and engaging with digital rights issues.
- As part of the Digital for Girls and Women project, this guide was developed through consultations with civil society organisations from across Africa to ensure it responds directly to the realities, priorities and challenges faced by organisations working on the ground. Its focus on Africa reflects the geographic scope of Enabel's work and its engagement with partners across the continent, while recognising that digital rights challenges and opportunities vary across countries and contexts. Drawing on the experiences and expertise of African civil society organisations, the guide provides practical, accessible information that can help readers understand digital rights and identify opportunities for advocacy and engagement in their own contexts.
- The guide is divided into seven modules covering the foundations of digital rights, freedom of expression in the digital space, digital inclusion and access, online safety and security, digital rights advocacy, emerging technologies and empowerment through training and community engagement.
- The guide is designed for both self-study and facilitated learning. Individuals can work through the modules at their own pace, while organisations can use them as the basis for workshops, training sessions or group discussions. Although each module stands alone, readers who are new to digital rights are encouraged to begin with the introductory module before exploring the remaining sections, as it provides the foundation for the topics that follow.



An abstract graphic in the top left corner of the page, featuring a complex network of white lines and dots on a blue background, resembling a digital circuit or data flow diagram.

Module 1:

Introduction to digital rights

Objective: Provide a basic understanding of digital rights and introduce foundational concepts.

1. What is a right?

- A right is a recognition, by society or a legitimate authority, of a prerogative essential to the dignity and well-being of each individual;
- It is a freedom or protection granted to a person, guaranteeing they can live, act, and express themselves with respect for their dignity;
- It is the foundation of a respectful, just, and inclusive society where every human being can live freely and with dignity.

2. What is digital?

- Digital technologies are technologies that structure, process, store, or transmit information electronically (via 'digits', i.e. numerical symbols). As these technologies are increasingly adopted across all spheres of life, they are transforming how we work, connect to other people, access information and services, and participate in societal debate.
- As digital technologies increasingly mediate our interactions, this raises important questions about how to protect human rights in a digitalised world.



3. What are Digital Rights?

- Digital rights are fundamental human rights principles (including those set out in the 1948 Universal Declaration of Human Rights (UDHR)), such as the right to access information, freedom of expression and security of person, transposed to digital technologies. Digital rights allow individuals to access, use, create, and publish digital media, as well as access and use computers, other electronic devices, and telecommunications networks without restriction or surveillance.
- These rights are extensions of traditional human rights, tailored to the unique challenges and opportunities presented by the internet and technology.

4. Why are digital rights important?

Digital rights are crucial because they enable individuals to safely engage in the digital world, safeguard their personal data, and exercise free expression online without the risk of censorship or discrimination.

They protect fundamental freedoms in the digital age.



5. Key stakeholders in digital rights

- **Government bodies**

Governments have a role in creating laws and regulations that protect digital rights. This includes developing and implementing data protection laws, combating cybercrime, and promoting digital inclusion. Governments should also ensure independent courts where citizens can seek justice and remedies for digital rights violations.

- **Civil society organizations**

Civil society organizations require access to digital tools to raise awareness, organize campaigns, and reach communities without facing censorship or restrictions. However, in countries where freedom of speech is restricted, these organizations can be faced with restrictions on their activities such as the blocking of their websites or censorship. Yet, to do their work, Civil society organizations (CSO) must have the right to express their views, share information, and advocate for change in the digital space without censorship or undue restrictions. Access to reliable, uncensored information is critical for research, advocacy, and communication.

Civil society organizations can also advocate for digital rights. They hold governments to account for their human rights obligations, including through monitoring and documenting digital rights violations.

- **Internet providers and platforms**

Information and Communication Technologies (ICT) companies must protect the privacy of their users' data as well as enable free expression, access to information and the security and wellbeing of users. This involves implementing strong data protection measures, being transparent about data collection and usage practices, and obtaining informed consent from users.

ICT companies should also follow the United Nations Guiding Principles on Business and Human Rights (UNGPs), which establish a corporate responsibility to respect human rights and to prevent and address adverse human rights impacts linked to their activities. This responsibility is particularly important when companies receive government requests or orders that may restrict digital rights. Companies should assess such requests against human rights standards and, where possible, challenge or resist unlawful or rights-violating demands, including orders to implement internet shutdowns or other restrictions on access to information and communication. They should also promote transparency about government requests and provide effective avenues for users to seek remedy where their rights have been adversely affected.



Civil society

• Global organizations

- ✓ **Electronic Frontier Foundation (EFF):** focuses on defending civil liberties in the digital world, particularly freedom of expression, privacy, and innovation.
- ✓ **Access Now:** works to protect and extend the digital rights of users globally, focusing on issues like data privacy, freedom of expression, and internet shutdowns.
- ✓ **Privacy International:** advocates for privacy rights and opposes government surveillance programs.
- ✓ **Human Rights Watch (HRW):** while focusing on general human rights, HRW also covers digital rights issues like internet censorship, privacy violations, and online freedom of expression.
- ✓ **Global Network Initiative (GNI):** a coalition of companies, civil society organizations, and academics working together to protect and advance free expression and privacy in the ICT sector.
- ✓ **Association for Progressive Communications (APC):** an international network of civil society organisations, dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment through ICTs.
- ✓ **Article 19:** works globally to protect and promote the right to freedom of expression and access to information. It advocates for laws and policies that uphold freedom of expression, including online, and challenges censorship, restrictions on access to information, and other violations of freedom of expression.

• Africa

- ✓ **Collaboration on International ICT Policy for East and Southern Africa (CIPESA):** focuses on advancing digital rights, cybersecurity, and inclusive ICT policies across Africa. They conduct research and advocacy work on internet shutdowns, data protection, and freedom of expression.
- ✓ **Paradigm Initiative:** advocates for digital rights and inclusion in Africa.
- ✓ **Media Foundation for West Africa:** Advocates for digital rights and media freedoms in West Africa.
- ✓ **The Media Institute of Southern Africa (MISA):** advocates for media freedom and freedom of expression in southern Africa.

6. Digital rights in Africa:

The current landscape

Digital rights in Africa are evolving, with the continent facing challenges related to internet access and the digital divide, censorship, and surveillance, AI related threats, cybersecurity, technology facilitated gender-based violence, shutdowns, and disinformation. At the same time more and more civil society organizations and citizens are aware of the importance of digital technologies to assert their rights, and civil society movements arise on critical issues such as high connectivity costs. Many African countries are increasingly investing in expanding digital infrastructure, but issues such as government-imposed internet shutdowns and limited data privacy protections are widespread, especially during election times.

Opportunities and challenges



- **Emerging threats to digital rights**

- ✓ **Surveillance and Privacy Violations** by governments and corporations collecting data on individuals, without meaningful consent or knowledge.
- ✓ **Algorithmic Bias and Discrimination** generated by Artificial Intelligence (AI) and algorithm-driven decisions can perpetuate bias such as gender bias, especially on social media apps.
- ✓ **Fragmented regional and global regulation:** Different countries and regions have varying approaches to digital governance, with differing laws around data protection, digital trade, and content moderation. This fragmentation makes it difficult to create global standards that protect digital rights.
- ✓ **Corporate Influence:** Large tech companies hold significant power over

digital infrastructure and governance, and their profit-making incentives can override other considerations like the human rights and wellbeing of people and societies. Their influence on global governance can undermine efforts to regulate the digital landscape.

- ✓ **Cross-Border Jurisdiction:** the borderless nature of the internet presents legal challenges regarding jurisdiction over digital activities, making it hard to enforce laws consistently across different countries.
- ✓ **Security and privacy:** Governments are increasingly required to implement measures to address cybercrime, but there are risks that these efforts may lead to government overreach, surveillance and erosion of privacy rights.

- **The future of digital governance**

To close the digital divide, governments have to ensure equal access to digital technologies and opportunities and as well invest in digital infrastructure, especially in underserved regions. Governments have to implement frameworks and policies that protect against threats, such as violence against women and girls online, while also respecting rights to privacy and free expression. There is a growing need for international standards and regulations that protect digital rights across borders. Regulations such as the European Union's General Data Protection Regulation (GDPR) have led the way. However, the rapid development of technologies such as artificial intelligence (AI) raises new challenges, requiring both the continued interpretation of existing regulations and the development of new regulatory frameworks.

✓ **Global digital rights standards and principles:** There is a growing need for international cooperation to develop global digital rights standards, ensuring that data privacy, freedom of expression, and cybersecurity are protected worldwide. Existing international law establishes a framework defining State responsibility and shaping corporate responsibility for conduct online and digitally mediated harms. However, the increased use and influence of digital technologies on our daily lives, and rapid technological developments, have given rise to particular challenges that require the interpretation of international standards to be made more explicit, or tailored to the specificities of technology enabled violations and abuses. Global Initiatives like the UN Global Digital Compact aim to address this.

✓ **Multi-stakeholder governance:** Because the internet and digital ecosystem is inherently distributed, with cross-border dimensions, future digital governance requires a collaborative approach between governments worldwide, tech companies, civil society, and international organizations to address challenges such as security, and content moderation.

✓ **Digital Citizenship and Literacy:** To foster better governance, individuals need to be educated about their digital rights and responsibilities. Programs promoting digital literacy play an important role in empowering citizens to participate effectively in digital governance and assert their rights in the digital space.



An abstract, light yellow circuit-like pattern on a darker yellow background, featuring various lines, dots, and geometric shapes resembling a network or data flow.

Module 2:

Freedom of expression in the digital space



Objective: Empower individuals to express themselves freely online while understanding their rights.

1. What is Freedom of Expression?

Freedom of expression is a fundamental right that allows individuals to share opinions, access information, and contribute to democracy. Freedom of expression is recognized as a fundamental human right under Article 19 of the Universal Declaration of Human Rights (UDHR), which states that everyone has the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. For African contexts, this right is further protected under Article 9 of the African Charter on Human and Peoples' Rights (ACHPR), which guarantees the right to receive information and to express and disseminate opinions within the law.

2. What is Freedom of Expression in the Digital Space

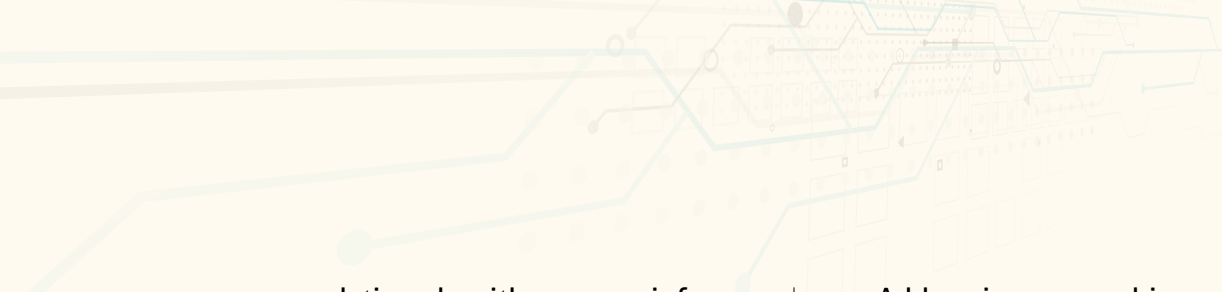
In the digital age, this right takes on new significance through widespread access to communication platforms.

- The Internet is a crucial space for communication and expression of opinions. Digital rights allow individuals to express themselves freely online, without fear of censorship or repression
- The right to express opinions, share ideas, and publish content on the internet without censorship or unjustified restrictions

3. Freedom of Expression for Women and Girls

For many women and girls, the digital space remains a site of discrimination, violence, and censorship that restricts their ability to fully exercise this right.

While the internet and social media provide powerful tools for expression and advocacy, women and girls often face cyber-harassment, threats, and hate speech, leading to psychological consequences, self-censorship and even offline violence. Moderation systems and



recommendation algorithms can reinforce gender biases, limiting the visibility of content created by women or amplifying hate speech and discriminatory narratives. Strengthening protection mechanisms against online harassment and harmful content is essential to ensuring a safe space for their expression. Digital freedom of expression presents both opportunities and challenges for the empowerment of women and girls. While technology enables new forms of activism and visibility, it also demands increased vigilance against abuse and discrimination. A comprehensive and collaborative approach involving legislators, technology actors, educators, and civil society is necessary to create a digital space where women's and girls' voices can be freely and safely expressed, fostering a more just and equal society.

4. Understanding Censorship and Restrictions Online

- Online censorship occurs when there is undue restriction in access to online platforms, for example through the blocking of accounts, or content moderation that deletes legitimate and legal content. It usually results from the actions of governments and private companies.
- Online censorship and internet shutdowns contribute to restricting certain freedoms, notably freedom of expression and the right to information;

- Addressing censorship requires joint efforts by governments, companies and civil society to implement policies and frameworks that promote and protect digital rights. This includes digital literacy, which can help users to understand how to participate in online platforms in a secure and responsible way.

5. Mindful expression

This is the practice of communicating with thoughtfulness, awareness, and intention. It involves being conscious of your words, tone, and actions to ensure that what you express aligns with your values and respects others

In digital spaces, mindful expression involves considering the impact of your posts, messages, or comments. Being intentional about what you share online, understanding that words can have a lasting effect.

6. Examples of how people use digital platforms to advocate for their rights

Digital platforms today offer powerful tools for citizens, collectives and organizations to defend their rights, express themselves freely and put pressure on public authorities.

- **Example of #EndSARS**

A notable example of digital civic mobilisation is Nigeria's #EndSARS movement in 2020. Citizens used social media platforms such as X (formerly Twitter), Facebook and Instagram, together with messaging applications, to document alleged human rights abuses by the Special Anti-Robbery Squad (SARS), organise peaceful protests, share verified information and coordinate legal, medical and humanitarian support for demonstrators. Digital platforms also facilitated fundraising, amplified local voices internationally and increased public scrutiny of law enforcement practices. The #EndSARS movement illustrates how digital technologies can strengthen civic participation, promote accountability and support the exercise of fundamental rights online.

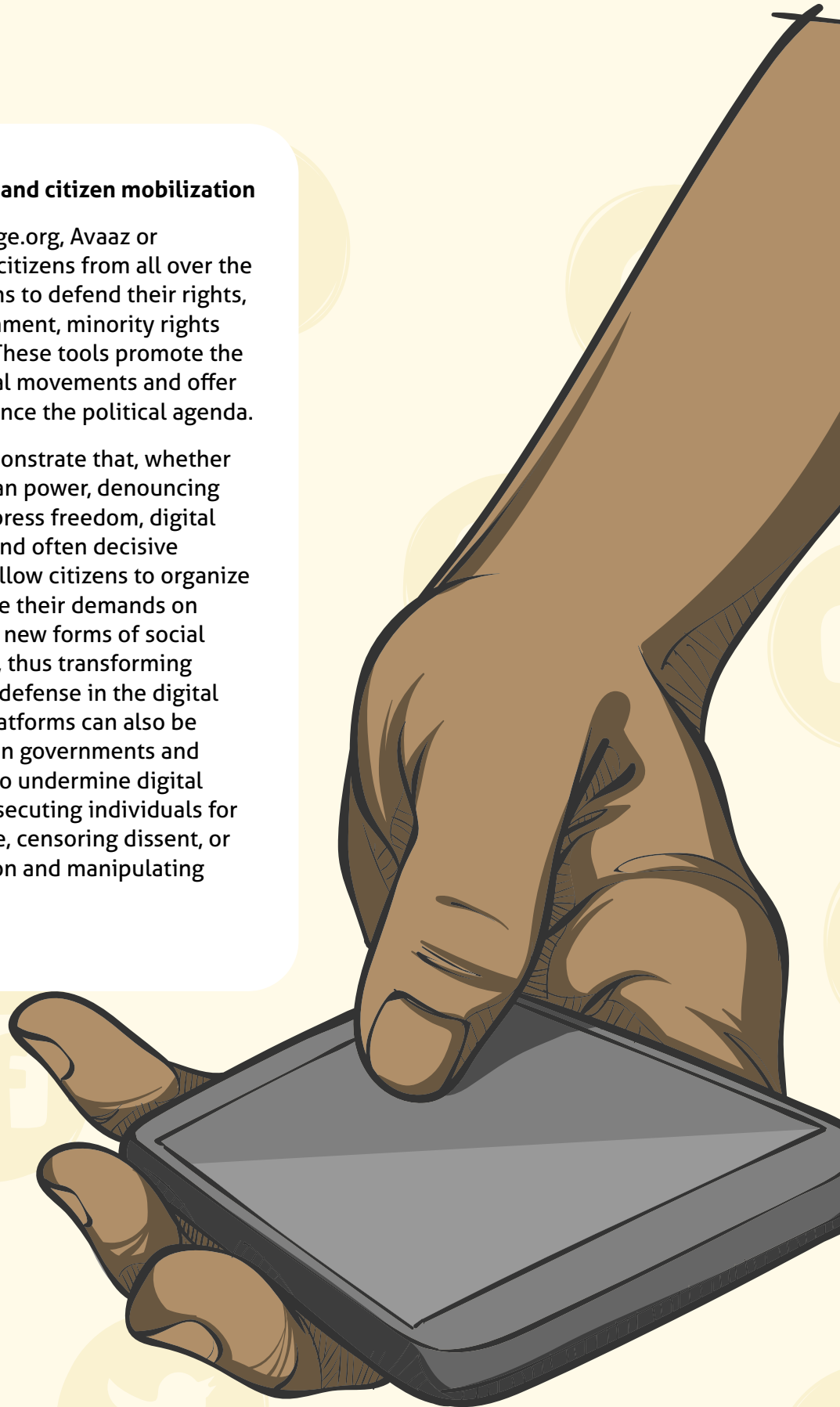
Defense of individual and collective rights through online activism: The case of the #MeToo movement and the #UneVraieFemmeAfricaine campaign



- **Petition campaigns and citizen mobilization**

Platforms such as Change.org, Avaaz or mesopinions.net allow citizens from all over the world to launch petitions to defend their rights, whether for the environment, minority rights or other social causes. These tools promote the creation of transnational movements and offer visibility that can influence the political agenda.

These case studies demonstrate that, whether challenging authoritarian power, denouncing violence or protecting press freedom, digital platforms offer varied and often decisive means of action. They allow citizens to organize collectively, disseminate their demands on a large scale and create new forms of social and political regulation, thus transforming the landscape of rights defense in the digital age. However, digital platforms can also be misused by authoritarian governments and other malicious actors to undermine digital rights, including by prosecuting individuals for statements made online, censoring dissent, or spreading disinformation and manipulating public debate.







Module 3:

Inclusion and access



Objective: Explore how to ensure digital spaces can be inclusive and accessible to all.

1. Inclusion of Marginalized Groups

Importance of reducing the digital divide

The digital divide refers to unequal access to information and communication technologies (ICTs), as well as disparities in the skills needed to use them effectively. Bridging this divide is a major challenge for several reasons:

1. Social and civic inclusion

- Access to e-government services: Administrative procedures are increasingly being digitalised, with many now conducted entirely online;
- Democratic participation: Access to information and online debates is crucial to exercising citizenship;
- Increasingly basic services such as health or education rely on the use of digital technologies. Students without access to the internet or a computer may be penalized (online homework, educational resources), and access to information about one's health or medical examinations is also often digitalised;
- During the pandemic, 1.3 billion students worldwide were deprived of school, worsening inequalities according to United Nations Educational, Scientific and Cultural Organisation (UNESCO);
- People without digital skills risk exclusion from the labor market.

2. Economic growth and employment

- Access to and the ability to master digital technologies can create job opportunities, and can stimulate entrepreneurship and innovation.

3. Persistence of inequalities

- Geographic: Rural areas, which are isolated or face major security challenges, are often less connected or not connected;
- Gendered: In developing countries, 327 million fewer women than men have a smartphone (GSMA, 2023).



Identifying barriers to inclusion

Obstacles to digital inclusion are linked to several aspects:

1. Access to digital infrastructures

- Lack of reliable and quality internet coverage in rural or isolated areas;
- The absence or limited availability of local data centers and internet exchange infrastructure can increase latency, as data must be routed through servers located abroad – leading to slower access to websites and online services.

2. Economic barriers

- Price of equipment (computers, smartphones, tablets) is unaffordable for certain populations;
- High cost of internet subscriptions and mobile plans for rural populations;
- High cost of electronic devices especially in rural or remote areas.

3. Inequalities in digital skills

- Lack of training in the use of digital tools;
- Low digital literacy among certain categories of the population (elderly people, rural populations, etc.);
- Lack of digital education programs in educational curricula from an early age.

4. Cultural and linguistic barriers

- Digital platforms and services may prioritise certain languages, cultures and perspectives, resulting in limited representation of local languages and cultural contexts and making digital content and services less accessible or relevant to some communities.



5. Accessibility issues

- Websites and apps poorly designed for accessibility, such as those living with disabilities (autism, dyslexia, visual impairment);
- Unequal access to assistive technologies and devices

6. Cybersecurity and Privacy Risks

- Lack of awareness about protecting private information;
- Exposure to cyber threats (scams, phishing, cyber harassment, etc.).

7. Social barriers

- Restrictive social and religious norms excluding a section of the population (such as women) from the use of digital tools.

2. Tackling the digital divide

- **Digital literacy programs and training**

Essential digital competences enable the confident, critical and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society. It includes the ability to use digital tools to communicate, find and share information online, but also media literacy, protecting personal data and cybersecurity and awareness about the environmental impact of digital technologies

- **Ensuring access to devices and internet**

Ensuring that digital services and technologies are inclusive and available to all individuals, regardless of their socioeconomic status, location, or disability. This includes providing affordable internet access, building inclusive digital infrastructure, and developing accessible technologies.

- **Strategies for capacity building in rural and marginalized areas**

Strengthening digital capacities in rural and marginalized areas can be based on axes such as:

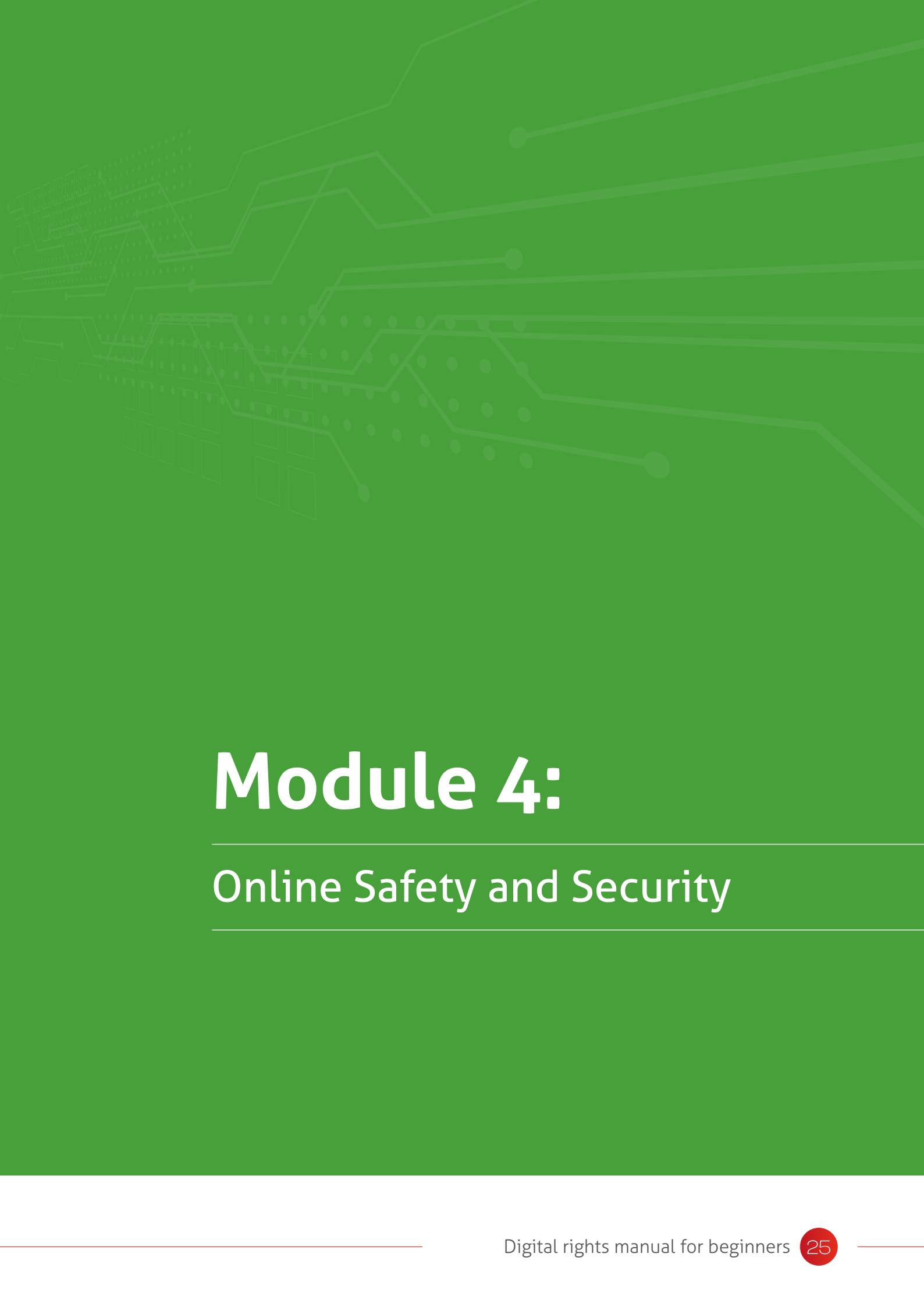
- ☒ **Mobile and itinerant training:**

- Organize workshops with mobile units (digital cars, temporary training centers);
- Adapting training to low resource settings.

- ☒ **Adaptation of content:** Offering training in local languages, visual and audio supports.

- ☒ **School education:** Integrating digital technology into schools and training teachers.





Module 4:

Online Safety and Security

1. Understanding digital footprint and protecting privacy

What is a digital footprint?

A digital footprint refers to the trail of personal data left online, including browsing history, social media activity, and information shared voluntarily or collected without full awareness.

2. Cybersecurity basics

Understanding and managing one's digital footprint is an important aspect of cybersecurity, as excessive or exposed personal information can be exploited for phishing, identity theft, social engineering and other cyberattacks.

Common cyber threats

- o **Hacking:** Unauthorized access to systems to steal data or sabotage services;
- o **Phishing:** Tricking users into providing sensitive information like passwords or credit card numbers;
- o **Ransomware:** Malicious software that

blocks access to files until a ransom is paid;

- o **Denial of Service (DoS/DDoS) attacks:**

Overwhelming a network to make it unavailable;

- o **Online fraud:** Financial scams or fraudulent sales conducted via the internet.

- o **Bot-driven disinformation campaigns:**

The use of automated accounts (bots) to rapidly spread false or misleading information, amplify particular narratives, and manipulate public opinion.

3. Tips

- **Avoid sharing sensitive information**
- **Conduct a simple threat assessment**

Question	Example
What am I trying to protect?	My personal information, photos, contacts or work documents
Who might want access to it?	Harassers, abusive partners, scammers or malicious actors
How could they gain access?	Weak passwords, phishing emails, shared devices or public Wi-Fi
What can I do to reduce the risk?	Strong passwords, Multi Factor Authentication, limiting personal information shared online



4. Security for women and girls online

Addressing online threats (harassment, privacy breaches):

Online harassment, hacking, identity theft, and phishing are among the types of cybercrime that can affect individuals, including women and girls.

Experiencing online harassment or abuse can be distressing, but there are practical steps you can take to protect yourself, preserve evidence, and seek support. Legal redress, cyber security and psychosocial support may be available through relevant organisations and services, which can provide assistance, advice and support to people experiencing online harassment or abuse.

1. Report and block abusive content

Most social media and messaging platforms provide tools to report abusive content and block users who engage in harassment.

If you experience online gender-based violence:

- Report abusive posts, messages or accounts using the platform's reporting tools.
- Block or mute users who continue to harass or threaten you.
- Review your privacy settings to control who can contact you or view your content.
- If the abuse involves credible threats of violence or criminal behaviour, report it to the appropriate law enforcement authorities where it is safe to do so.

2. Preserve evidence

Before deleting abusive messages or blocking an account, preserve evidence that may be needed if you decide to report the incident.

Useful evidence includes:

- Screenshots of abusive messages or posts.
- The date and time of the incident.
- URLs (web links) to posts or profiles.
- Usernames or account handles.
- Emails or text messages containing threats.

Store this information securely in case it is needed later

3. Secure your accounts and devices

If you think someone has gained access to your accounts:

- Change your passwords immediately and use a strong password.
- Enable multi-factor authentication (MFA) where available.
- Check recovery email addresses and phone numbers.
- Review active login sessions and sign out of unfamiliar devices.

Update your device and applications to the latest versions

4. Recover a compromised account

If your account has been hacked:

1. Use the platform's account recovery process.
2. Reset your password.
3. Remove unknown devices connected to the account
4. Notify trusted contacts if your account has been used to send fraudulent messages.

More practical tips for interacting with digital technologies

- **Limit the personal information you post on social media:** Avoid sharing your location, financial details, or other private data that could be used to compromise your security through identity theft or cyber attacks;
- **Use strong, unique passwords:** Ensure each of your online accounts has a strong and unique password, combining letters, numbers, and symbols. Use a password manager to keep track of them;
- **Enable two-factor authentication (2FA):** Add an extra layer of security by enabling 2FA on your accounts, requiring a second step like a text message or authentication app code;
- **Keep software updated:** Regularly update your operating systems, apps, and software to protect against vulnerabilities and malware;
- **Be Cautious with Public Wi-Fi:** Avoid conducting sensitive activities like banking on public Wi-Fi networks. If necessary, use a Virtual Private Network (VPN) to encrypt your connection;
- **Avoid phishing scams:** Be wary of unsolicited emails or messages asking for personal information or login credentials. Double-check the sender's email and avoid clicking suspicious links;
- **Use secure websites:** When shopping or entering sensitive information, make sure the website uses HTTPS (indicated by a padlock symbol in the URL bar);

Tips for protecting your digital footprint

- **Minimize cookies and trackers that collect your browsing data:** You can also regularly clear your browser cookies and history;
- **Review privacy settings:** Regularly check and update the privacy settings on your social media, email, and other online accounts to control who has access to your personal information;
- **Think before you post:** Consider the long-term impact of your posts, comments, and shared content. Once something is online, it can be hard to remove, and it may impact your reputation or job prospects;
- **Minimize tracking:** Use browser extensions like ad blockers or anti-tracking tools (e.g., Privacy Badger, Ghostery) to limit how much of your activity is tracked by websites and advertisers;
- **Regularly audit your accounts:** Review the online accounts you have created over time. Delete any old, unused accounts to reduce your digital footprint and minimize data exposure;
- **Use encrypted messaging:** Opt for messaging services that use end-to-end encryption (e.g., Signal, WhatsApp) to ensure your communications remain private;
- **Opt out of data collection:** Many services allow you to opt-out of certain types of data collection or advertising preferences. Check the privacy policies of the websites and platforms you use;
- **Search yourself online:** Regularly search for your name online to see what information is publicly available. If necessary, request to have outdated or incorrect information removed

5. Understanding and avoiding misinformation and disinformation

■ **Build media and information literacy:**

Develop the knowledge and skills needed to assess online information, recognise unreliable websites and sources, and identify misleading or false content before sharing it.

■ **Understand the difference between misinformation, disinformation and malinformation:**

- Misinformation is false or inaccurate information that is shared without an intention to deliberately mislead or cause harm.
- Disinformation is false or misleading information that is deliberately created or shared to deceive, manipulate or cause harm.
- Malinformation is genuine or factually accurate information that is deliberately shared or presented in a misleading way to cause harm for example, by taking information out of context or deliberately exposing private information.

■ **Common forms of disinformation include:**

- False content: Completely false information created to deceive or cause harm.
- Manipulated content: Genuine information, images or videos that have been altered or edited to mislead.
- Context manipulation: Genuine information presented alongside false or misleading context, such as an old image presented as a recent event.
- Impersonation: Content that falsely appears to come from a trusted person, organisation or news source.

- Fabricated or AI-generated content: Content that is entirely fabricated or generated using AI and presented as genuine.

■ **Use media and information literacy and fact-checking:** Check information against reliable sources and use reputable fact-checking tools before accepting or sharing information, particularly when content is sensational, emotionally charged or difficult to verify.

■ **To verify information, ask:**

- Who is sharing the information? Is the source known, credible and identifiable?
- What is their interest or purpose? Are they trying to inform, persuade, sell, provoke or manipulate?
- What evidence supports the claim? Can the information be verified through reliable sources?
- Which other credible sources are reporting it? Do reputable and independent sources confirm the information?
- When was it published? Could the information be old or taken out of context?
- Has the image or video been verified? Could it have been manipulated, altered or generated using AI?

Useful tools for recognising and combating disinformation:

- **Interactive learning:** Harmony Square and Bad News
- **Fact-checking:** Africa Check and PesaCheck
- **Finding local resources:** Africa Facts Network



An abstract graphic in the top left corner of the page, featuring a network of thin, light-yellow lines and dots on a solid mustard-yellow background. The lines form a complex, interconnected web, resembling a circuit board or a digital network, with some lines ending in small circular nodes.

Module 5:

Advocacy for Digital Rights

Objective: Create awareness and foster advocacy for inclusive and fair digital rights policies.

1. The Role of Advocacy in Promoting Digital Rights

- Advocacy for rights-based legislation: Advocating for laws and policies that protect digital rights and ensure that digital technologies are governed in accordance with human rights principles and standards. This includes promoting strong protections for digital rights, while challenging laws that unnecessarily restrict these rights.
- Advocacy can also help to put in place targeted measures to bridge the digital divide shaped by factors such as income, education, geography, and disability and promote inclusion ensuring equitable access to digital technologies for everyone, regardless of background, geographic location, economic status, or abilities.

2. How to Engage with Policymakers and Stakeholders

Consulting and engaging with governments and civil society

- Participate in public consultations where governments seek input on proposed laws and regulations regarding digital rights;
- Engage with relevant policymakers by writing to elected representatives or participating in campaigns urging them to protect digital rights;
- Collaborate with civil society organizations like those listed on page nine to advocate for digital rights.

Identifying key stakeholders in the advocacy process

- Key stakeholders include governments, civil society organizations (e.g., Association for Progressive Communications, Paradigm Initiative, CIPESA, Media Foundation for West Africa), and non-profits working on digital rights;
- Engage with organizations like the Global Network Initiative (GNI), which brings together companies, civil society, and academics to protect free expression and privacy.
- Engage in discussions at national, regional and international levels such as Internet Governance Forums (IGF) which happen at national, regional and global level; the African Commission on Human and People's Rights (ACHPR)'s Ordinary sessions, and UN processes like the Universal Periodic Review.

3. Tools and Strategies for Advocacy

Digital campaigns and media outreach

- Use social media platforms to raise awareness about issues like censorship, surveillance, or online privacy violations;
- Share articles, petitions, or updates that highlight digital rights challenges and solutions.
- Use reliable evidence, statistics, and testimonies to document digital rights issues, support advocacy messages, and demonstrate the need for change.

Community outreach and use of infographics

- Share information about digital rights issues with your network to raise awareness;
- Use infographics and other visual tools to simplify complex digital rights concepts for broader understanding.

Development of policy briefs and recommendations

- Develop guidance notes and recommendations to advocate legislation that respects privacy, net neutrality and other fundamental rights;
- Take part in campaigns to protect Internet freedom, data protection and equal access;

4. Mapping Existing Laws and Policies in Africa

Overview of digital rights-related legislation

- Across Africa, many countries have introduced laws relating to digital technologies, including legislation on data protection, cybersecurity,

cybercrime, access to information and electronic communications.

- Some countries have also adopted policies on digital transformation, artificial intelligence and digital identity. While these laws can help protect people online, they may also contain provisions that restrict rights such as privacy or freedom of expression if they are not consistent with human rights standards (see the annex for instruments that provide important guidance for protecting digital rights).

Identifying gaps and areas for improvement

- Advocate for policies that promote universal access to technology, making it easier for marginalized groups to engage in the digital economy and society;
- Address gaps in digital literacy by offering free or low-cost programs that teach basic skills like internet navigation, cybersecurity awareness, and digital rights awareness to ensure all citizens understand their rights and demand them;



5. Key components of an effective advocacy brief

A strong advocacy brief should be:

- Concise & clear: straight to the point, avoiding technical jargon.
- Evidence-based: Supported by data, case studies, and expert analysis.
- Action-oriented: clearly outlining the changes needed and who should take action

Key components of a policy brief

A policy brief is designed to guide policymakers by presenting research findings and policy recommendations in a digestible format.

Template structure:

- Title & subtitle: Clearly stating the focus of the policy brief.
- Introduction: Why this policy issue matters.
- Current policy landscape: Analysis of existing digital rights policies in the country or region.
- Gaps & challenges: Identifying weaknesses in current regulations.
- Policy recommendations: Practical steps for governments and stakeholders.
- Conclusion & call to action: A strong closing argument and appeal for action

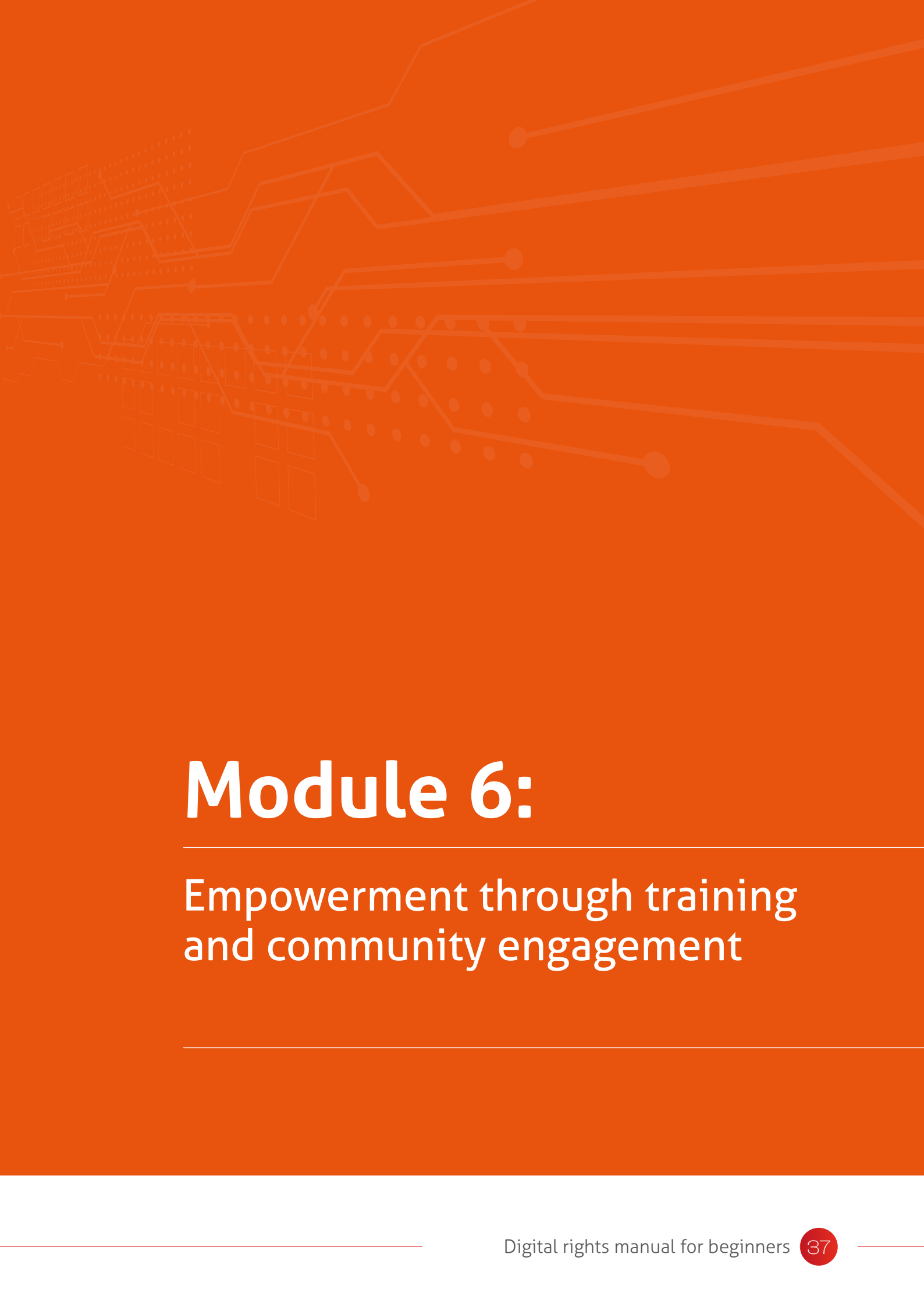
Advocacy & policy areas in digital rights

These templates can be used for pressing digital rights issues in Africa, such as:

- Internet freedom & censorship: Protecting access to information and freedom of expression;
- Data protection & privacy laws: Strengthening policies on personal data security.
- Cybersecurity & digital safety: Ensuring safe online environments for individuals and businesses;
- Women & Digital Rights: Addressing online gender-based violence and access barriers.
- AI & ethical tech regulation: Developing responsible policies for AI governance.







Module 6:

Empowerment through training and community engagement

Objective: Equip participants to empower others through training, awareness, and collaboration.

1. Knowledge-Sharing Techniques

How to organize workshops and training sessions?

1. Define Objectives and Target Audience

- ✓ **Identify participant levels:** Beginners, intermediates, or experts;
- ✓ **Set clear learning goals:** For example, raising citizens' awareness of digital rights, build young people's ability to protect themselves online or supporting media organisations to address disinformation

2. Design a Suitable Program

- ✓ Structure training into **short, interactive modules** and provide real world examples;
- ✓ Use diverse formats: **Presentations, demonstrations, and hands-on exercises;**
- ✓ Allocate time for **questions and discussions.**

3. Choose the Right Format and Tools

- ✓ **Face-to-face:** Encourage interactive learning using **computers or smartphones;**
- ✓ **Online:** Use platforms to reach more people and take sufficient security measures to secure your meetings
- ✓ **Hybrid:** Combine face-to-face and online learning for greater **flexibility.**

4. Make the Workshop Interactive and Engaging

- ✓ Use **case studies and real-life scenarios;**
- ✓ Encourage **collaboration** through **group work, role plays, and quizzes;**

- ✓ Include **practical demonstrations and role-playing exercises.**

5. Ensure Monitoring and Evaluation

- ✓ Assess skills through **exercises or practical projects;**
- ✓ Create a **discussion group** for post-training follow-up and knowledge sharing.
- ✓ Measure learning by conducting a short assessment before and after the training to identify changes in participants' knowledge, skills and confidence.

2. Building Community Engagement

Promoting local initiatives for digital literacy:

1. Development of community digital training programs

- ✓ Creation of free or low-cost workshops on the use of digital tools;
- ✓ Teacher training in digital rights education to be integrated in civic and moral education.

2. Encourage local innovation

- ✓ Support for local entrepreneurs developing digital educational solutions tailored to community needs.

3. Accessibility and connectivity for all

- ✓ Provide free or low-cost Internet access in public spaces (schools, libraries, community centers);
- ✓ Create public and accessible spaces where people can safely access digital resources, including digital libraries and community technology centres.



- ✓ Support community networks and locally driven connectivity initiatives that help underserved and remote communities access affordable and reliable Internet, particularly where commercial networks are unavailable or unaffordable.
- ✓ Create safe and inclusive spaces for women and girls to access and use digital technologies, including spaces where they can access devices, connectivity, digital skills training and support free from harassment, discrimination and other forms of online or offline abuse.

4. Integration of local languages and cultures

- ✓ Develop local language content and digital literacy to improve digital inclusion;
- ✓ Adapt trainings to different regional sociocultural contexts

5. Awareness of cybersecurity and good digital practices

- ✓ Inclusion of modules on data protection and online security in training;

- ✓ Workshops on digital citizenship and the fight against disinformation.

Engaging youth and women in digital spaces:

Engaging young girls and women in digital spaces can be done in several ways:

- Raising awareness about the importance of digital technology can be a time to encourage young people and women into digital spaces;
- Workshops and training sessions also represent ways to get young people and women interested in digital technology;
- Encourage and support women's associations in digital technology (sponsoring activities, portraits of women leaders, etc.);
- Ensure the effective participation of girls and young women in discussions on regulations, standards and policies, ensuring that their experiences and perspectives are taken into account;
- Create training, programs and awareness campaigns for men to improve their online behavior towards women.





Module 7:

Emerging technologies

Objective: Introduce participants to new technologies and their impact on digital rights.

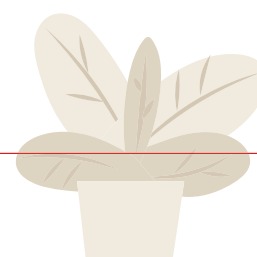
1. Overview of Emerging Technologies and trends

Social media trends

- There is more awareness of the need for fact-checking tools to combat fake news and prevent the spread of misinformation;
- Short videos and interactive content (polls, stories, live streams) are becoming more popular, making information more accessible and engaging.
- Concerns about addictive design and user wellbeing: The use of short videos and highly engaging, personalised content has raised concerns about addictive or compulsive use, particularly among young people. Regulators are increasingly examining whether platforms should change features and practices that encourage excessive use or negatively affect users' wellbeing.

Biometric digital ID systems

- Many governments are introducing digital identity (digital ID) systems to make it easier for people to access public services, vote, open bank accounts, receive social benefits and verify their identity. These systems often use digital records and may include biometric information such as fingerprints, facial images or iris scans.
- Digital ID systems can improve access to services and reduce administrative barriers. However, they can also create digital rights challenges if they are not designed and implemented in a way that respects human rights. For example, if people are excluded from essential services, when they do not have a digital identity or do not have a device to authenticate their digital identity. The collection and storage of biometric data also raises important questions about privacy, data protection and security. Without strong legal safeguards, personal information may be misused or shared without people's knowledge or consent.



SIM registration mandates

Many countries require people to register their SIM cards using official identity documents before they can access mobile phone services. Governments often introduce SIM card registration to help prevent crime, improve national security or reduce fraud. SIM registration can also exclude people who do not have official identity documents, including refugees, stateless persons and some rural or marginalised communities, preventing them from accessing mobile communication and internet services.

AI and digital rights

Accessibility: AI tools such as speech-to-text, language translation, and assistive technologies can enable greater access to digital platforms for people with disabilities or language barriers;

Challenges:

- Governments and companies could use AI for facial recognition, tracking, and profiling, which can infringe on individuals' right to privacy and freedom of movement. AI systems can also amplify disinformation at scale, particularly through automated generation and targeting of misleading or false content.
- Data bias in AI systems can reproduce or reinforce existing inequalities, potentially leading to discrimination in areas such as access to employment, healthcare, education, financial services,

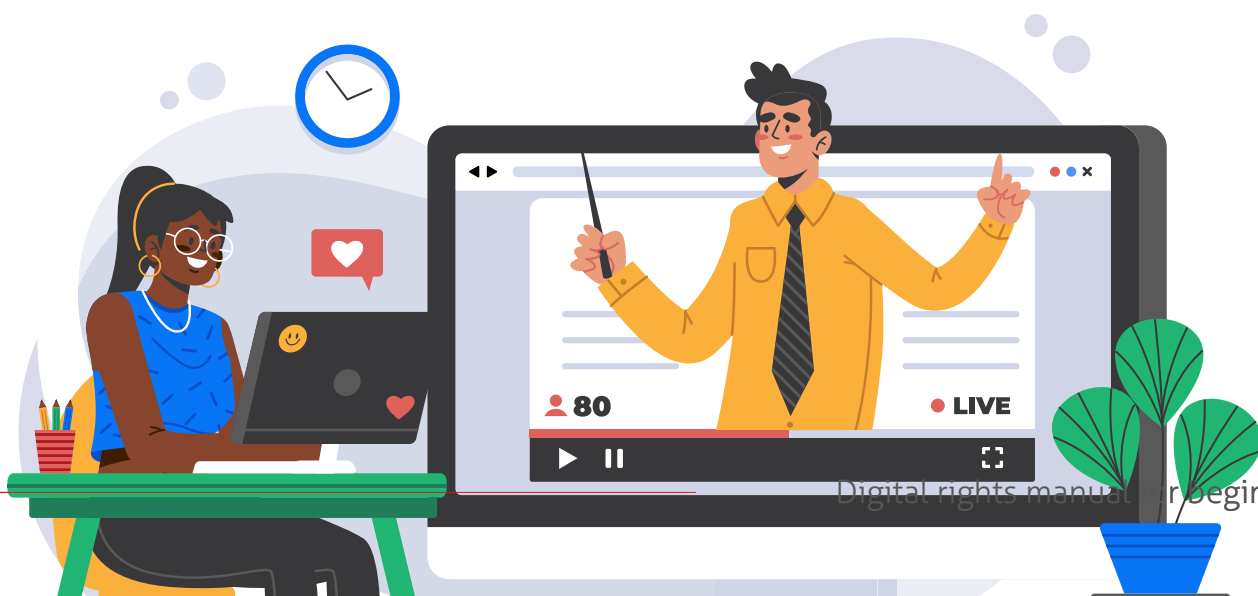
or social protection. Inaccurate or biased automated decision-making can also make it difficult for individuals to understand, challenge, or appeal decisions that affect their rights.

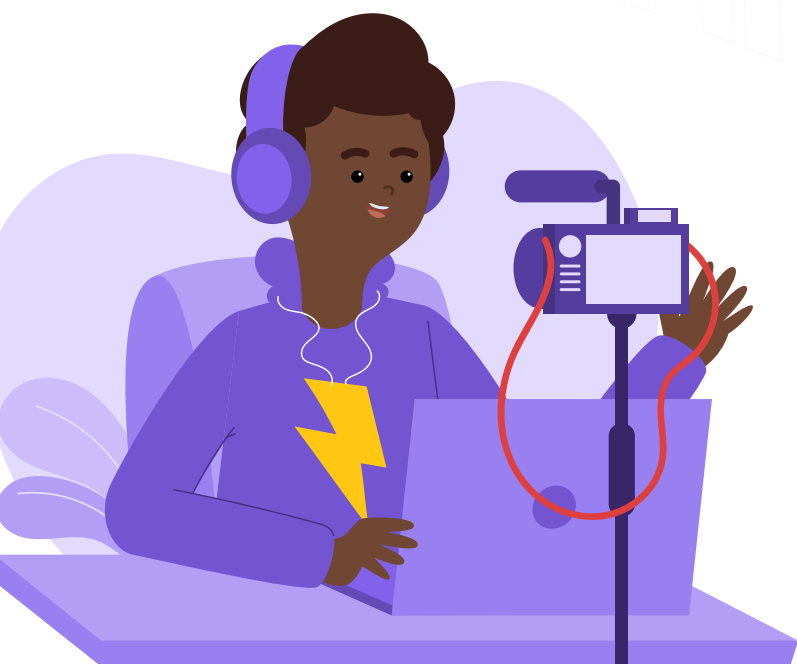
Ethical AI development: AI systems need to be designed with built-in fairness, transparency, and accountability to avoid bias and discrimination. Initiatives like AI Ethics Guidelines and regulation such as the EU's AI Act can help steer AI development toward upholding digital rights;

Regulation of AI surveillance technologies: Governments and international bodies need to create legal frameworks that regulate the use of AI to protect individual privacy and prevent abuse;

Human oversight in decision-making: AI should be used as a tool to assist humans in decision-making, not as the sole arbiter. Ensuring human oversight and review of AI-generated decisions will help safeguard fairness and accountability;

AI transparency: There is a need for transparency in how AI algorithm's function and the data they are trained on. This will help individuals understand how decisions affecting them are made and provide opportunities for redress. AI systems should be audited regularly to prevent discrimination and to ensure that their decisions are transparent and explainable.





2. Best practices for staying informed

How to Keep Up with digital trends?

Stay Informed: Regularly follow technology updates to keep up with changes in social media and digital tools;

Continuous Learning: Take part in online or in-person training to develop digital skills and better understand the challenges of the digital world.

Following digital trends

In an ever-evolving digital world, staying informed about the latest trends is essential for understanding opportunities but also risks, improving digital skills, and making informed decisions. Below are some best practices for keeping up with digital trends effectively.

Engage in continuous learning

Online courses & webinars: Platforms like ulearn.enabel.be, Coursera, Udemy, and Atingi offer courses on emerging technologies, AI, cybersecurity, and more;

Tech blogs & websites: Follow reputable sources like TechCrunch, Wired, Numerama (Francophone), or MIT Technology Review for industry insights;

Podcasts & YouTube channels: Listen to digital experts on podcasts like The Vergecast or La French Tech for the latest innovations.

Subscribe to the mailing lists or newsletters of organisations listed in page nine.

Resources and Appendices

I. Case Studies

1) Challenging internet shutdowns through the ECOWAS court

What happened?

In 2017, the Government of Togo shut down internet and messaging services during large-scale anti-government protests, limiting people's ability to communicate, access information and report on events. Civil society organisations (CSOs) argued that the shutdown violated the rights to freedom of expression and access to information. In 2021, the Nigerian government also suspended access to Twitter nationwide after the platform removed a presidential tweet, disrupting communication for millions of users, businesses and CSOs. These actions reflected a growing trend of governments restricting digital communications during periods of political tension.

What was the response?

CSOs used strategic litigation to challenge these restrictions before the ECOWAS Community Court of Justice. In the Togo case, Amnesty International Togo, together with other human rights organizations and individuals, argued that the internet shutdown violated regional and international human rights protections. After Nigeria's Twitter suspension, the Socio-Economic Rights and Accountability Project (SERAP), supported by other organizations and an amicus brief from Amnesty International, brought a similar challenge before the ECOWAS Court. Rather than treating internet restrictions as purely technical or political issues, civil society framed them as violations of fundamental human rights protected under the African Charter on Human and Peoples' Rights.

Outcome

The ECOWAS Court ruled that Togo's internet shutdown was unlawful and affirmed that internet access is essential to the exercise of freedom of expression. It ordered the government to prevent similar shutdowns in the future and compensate the applicants. In 2022, the Court also found Nigeria's Twitter suspension unlawful, reinforcing that governments cannot arbitrarily restrict access to digital platforms. Together, these decisions established important regional jurisprudence that civil society across West Africa can rely on when challenging future internet shutdowns and other forms of online censorship.

Lessons learned

- Framing internet shutdowns as human rights violations not just technical or economic issues can strengthen advocacy.
- Collaboration between local organizations, regional actors and international partners can increase the impact of advocacy efforts.
- Court victories create valuable legal precedents, even where implementation remains an ongoing challenge.

2) Case study: Shaping regional digital rights standards in Africa

What happened?

As digital technologies became central to communication, participation and access to information, the African Commission on Human and Peoples' Rights (ACHPR) recognised the need to update its regional standards on freedom of expression. The existing Declaration of Principles on Freedom of Expression, adopted in 2002, did not adequately address emerging digital rights issues such as internet shutdowns, online privacy, encryption and access to the internet.

What did civil society do?

African civil society organisations took the lead in developing a shared vision for digital rights on the continent. In 2014, a coalition of organisations launched the African Declaration on Internet Rights and Freedoms (AfDec), setting out key principles for protecting human rights in the digital age.

Rather than treating the Declaration as a standalone document, civil society used it as an advocacy tool. Organisations engaged with the ACHPR—particularly the Special Rapporteur on Freedom of Expression and Access to Information in Africa—through consultations, expert input and sustained advocacy.

Impact

In 2019, the ACHPR adopted the Revised Declaration of Principles on Freedom of Expression and Access to Information in Africa, incorporating many of the issues championed by civil society. The revised Declaration affirms that everyone should have affordable and non-discriminatory access to the internet, prohibits arbitrary internet shutdowns and network disruptions, recognises the importance of privacy, anonymity and encryption, and limits intermediary liability to help protect online freedom of expression.

Today, the Declaration serves as an important regional standard that governments, courts, national human rights institutions and civil society organisations can use to promote and protect digital rights across Africa.

Lessons learned

- Civil society can shape regional human rights standards by developing practical, evidence-based policy proposals.
- Building coalitions across countries and sectors strengthens advocacy and gives recommendations greater legitimacy.
- Sustained advocacy over several years may be needed to achieve meaningful policy change.

3) Case study: Strengthening privacy protections in Kenya's Huduma Namba digital ID System

What happened?

In 2019, the Kenyan government launched the National Integrated Identity Management System (NIIMS), commonly known as Huduma Namba, to create a single digital identity system for all residents. While the initiative aimed to improve access to public services, civil society organisations raised concerns that the system was being implemented without adequate legal safeguards to protect people's privacy and personal data. There were also concerns that marginalised communities could be excluded from registration and that the collection of sensitive personal information could increase the risk of surveillance and discrimination.

What did civil society do?

A coalition of Kenyan civil society organisations, including the Nubian Rights Forum, the Kenya National Commission on Human Rights and the Kenya Human Rights Commission, brought a constitutional challenge against the implementation of Huduma Namba. Their advocacy combined strategic litigation with public awareness campaigns, legal analysis and community engagement to highlight the potential human rights risks of the programme.

Impact

The High Court of Kenya recognised that digital identity systems must comply with constitutional rights and ruled that Huduma Namba could not be made mandatory until appropriate data protection safeguards were in place. The litigation contributed to stronger oversight of Kenya's digital identity programme and reinforced the importance of implementing the country's Data Protection Act. The case has since become an important reference point for digital identity initiatives across Africa, demonstrating that innovation and digital transformation must be accompanied by robust human rights protections.

Lessons learned

- Civil society does not have to oppose digital innovation it can advocate for rights-respecting implementation.
- Building coalitions between human rights organisations, legal experts and affected communities strengthens advocacy.
- Privacy, data protection and inclusion should be considered from the design stage of digital systems, not added later.

4) Case study: Defending freedom of expression online – The Stella Nyanzi Case

What happened?

Stella Nyanzi, a Ugandan academic, poet and human rights activist, became well known for using Facebook and other digital platforms to criticise government policies and political leaders. Between 2017 and 2019, she was arrested and prosecuted under Uganda's Computer Misuse Act for posts that authorities claimed were offensive or constituted cyber harassment. Her case raised concerns that cybercrime laws were being used to suppress legitimate political speech and silence government critics.

What did civil society do?

Civil society organisations in Uganda and across Africa provided legal support, documented the human rights implications of the case and campaigned for Stella Nyanzi's release. Human rights groups issued public statements, monitored court proceedings and used regional and international advocacy to draw attention to the misuse of cybercrime legislation to restrict freedom of expression. The case also mobilised journalists, academics and digital rights organisations to advocate for reforms to laws that criminalise online speech.

Impact

In 2020, Uganda's High Court overturned Stella Nyanzi's conviction, finding that the prosecution had failed to prove the offence. The case became an important example of the risks posed by overly broad cybercrime laws and highlighted the need for legislation that protects, rather than restricts, freedom of expression online. It also strengthened advocacy efforts calling for legal reforms and greater safeguards for digital rights in Uganda and across Africa.

Lessons learned

- Monitoring and documenting digital rights violations strengthens national, regional and international advocacy.
- Defending the rights of individual activists can contribute to broader protections for freedom of expression online.

II. List of legislations and standards

Instrument	Level	Type	Legal status	Digital rights relevance
Universal Declaration of Human Rights (UDHR)	International	Declaration	Foundational (non-binding, widely regarded as customary international law)	Establishes the foundation for all human rights
International Covenant on Civil and Political Rights (ICCPR)	International	Treaty	Binding	Freedom of expression, privacy, assembly, association, political participation
International Covenant on Economic, Social and Cultural Rights (ICESCR)	International	Treaty	Binding	Digital inclusion, education, science, culture
Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)	International	Treaty	Binding	Gender equality and women's digital rights
Convention on the Rights of the Child (CRC)	International	Treaty	Binding	Children's rights in digital environments
Convention on the Rights of Persons with Disabilities (CRPD)	International	Treaty	Binding	Digital accessibility and inclusion
African Charter on Human and People's Rights (ACHPR)	International	Treaty	Binding	Freedom of expression, access to information, equality and participation
African Charter on the Rights and Welfare of the Child	International	Treaty	Binding	Children's rights online

Maputo Protocol	African	Treaty	Binding	Women's rights and gender equality	Various
Protocol to the African Charter on the Rights of Persons with Disabilities in Africa	African	Treaty	Binding	Accessible ICTs and digital inclusion	Various
AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)	African	Treaty	Binding (for States Parties)	Cybersecurity, electronic commerce and personal data protection	Various
Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019)	African	Declaration	Non-binding (authoritative interpretation)	Interprets Article 9 of the African Charter for the digital age	Principles 1–41
Resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa	African	Resolution	Non-binding	Protects internet freedom and digital expression	Resolution
UN Guiding Principles on Business and Human Rights	International	Guiding Principles	Non-binding	Digital platforms and corporate human rights responsibilities	Principles 1–31
UNESCO Recommendation on the Ethics of Artificial Intelligence	International	Recommendation	Non-binding	Human rights-based AI governance	Recommendation
African Union Data Policy Framework	African	Policy Framework	Non-binding	Data governance and trusted data ecosystems	Framework

African Union Digital Transformation Strategy (2020–2030)	African	Strategy	Non-binding	Digital inclusion and transformation	Strategy
African Union Continental AI Strategy	African	Strategy	Non-binding	Responsible AI governance	Strategy
European Convention on Human Rights (ECHR)	European	Treaty	Binding (for States Parties)	Protects fundamental rights relevant to the digital environment, including privacy, freedom of expression, freedom of assembly and association, and non-discrimination	Arts. 8, 10, 11, 14
European Declaration on Digital Rights and Principles	European / EU	Declaration	Non-binding	Human-centred digital transformation; digital inclusion; freedom of expression and participation; privacy and data protection; safety and security; AI and digital governance	Chapters I–VI

III. Glossary of Key Terms

A

Accessibility: Ensuring that digital services and technologies are inclusive and available to all individuals, regardless of socioeconomic status, location, or disability.

Advocacy: Efforts to influence decision-makers and raise awareness about digital rights challenges, often through campaigns, policy briefs, and community engagement.

Algorithmic Bias: The tendency of algorithms to produce biased outcomes, often due to biased data or design, leading to discrimination or unfair treatment.

Artificial Intelligence (AI): Technologies that enable machines to perform tasks that typically require human intelligence, such as decision-making, language translation, and pattern recognition.

B

Blockchain: A decentralized digital ledger technology that records transactions across multiple computers, ensuring transparency and security.

Big Data: Large and complex datasets that require advanced tools for analysis, often used to uncover trends and patterns.

C

Censorship: The suppression or restriction of access to information, often by governments or private entities, limiting freedom of expression.

Cybersecurity: Measures and practices designed to protect systems, networks, and data from digital attacks, such as hacking and phishing.

Cloud Computing: The delivery of computing services (e.g., storage, servers, databases) over the internet, allowing for scalable and flexible resources.

D

Data Governance: The management of data availability, usability, integrity, and security, often through policies and procedures.

Digital Divide: The gap between individuals who have access to digital technologies and those who do not, often due to socioeconomic, geographic, or educational disparities.

Digital Footprint: The trail of data left behind by a person's online activities, including browsing history, social media posts, and online transactions.

Digital Literacy: The ability to access, analyze, understand, and create information using digital technologies responsibly.

Digital Rights: Human and legal rights that allow individuals to access, use, create, and publish digital media, as well as use electronic devices and networks without unlawful restrictions or surveillance.

Disinformation: False information spread intentionally to deceive or manipulate public opinion.

E

E-Government: The use of digital technologies to deliver government services, improve transparency, and engage with citizens.

Encryption: The process of converting data into a code to prevent unauthorized access, ensuring confidentiality and security.

Ethical AI: The development and use of AI systems that are fair, transparent, and accountable, avoiding bias and discrimination.

F

Freedom of Expression: The right to express opinions, share ideas, and publish content without censorship or unjustified restrictions.

Fake News: False or misleading information presented as news, often spread through social media and other digital platforms.

G

GDPR (General Data Protection Regulation): A European Union regulation that sets guidelines for the collection and processing of personal data, emphasizing privacy and data protection.

Global Digital Compact: A United Nations initiative aimed at developing global standards for digital rights, including data privacy, freedom of expression, and cybersecurity.

H

Hacking: Unauthorized access to computer systems or networks, often to steal data or disrupt services.

Human Rights: Fundamental rights and freedoms that belong to every individual, often protected by international laws and conventions as well as national and regional frameworks.

I

Internet Shutdown: The intentional disruption of internet access by governments, often during political unrest or elections, limiting freedom of expression and access to information.

ICT (Information and Communication Technology): Technologies that provide access to information through telecommunications, including the internet, wireless networks, and mobile devices.

M

Misinformation: False or inaccurate information shared without malicious intent, often leading to misunderstandings.

Mal information: true information taken out of context.

Multi-Stakeholder Governance: A collaborative approach to digital governance involving governments, tech companies, civil society, and international organizations.

N

Net Neutrality: The principle that internet service providers should treat all data equally, without discriminating or charging differently based on content, user, or platform.

O

Online Harassment: The use of digital platforms to bully, threaten, or intimidate individuals, often targeting women and marginalized groups.

P

Phishing: A cyberattack that uses disguised emails or websites to trick individuals into revealing sensitive information, such as passwords or credit card numbers.

Privacy: The right to control one's personal information and how it is collected, used, and shared online.

Public-Private Partnership (PPP): Collaboration between government and private sector entities to achieve shared goals, such as improving digital infrastructure.

R

Ransomware: Malicious software that blocks access to a computer system or data until a ransom is paid.

Right to be Forgotten: The right of individuals to have their personal data deleted from online platforms under certain conditions.

S

Surveillance: The monitoring of individuals' online activities, often by governments or corporations, raising concerns about privacy and freedom.

Social media: Online platforms that enable users to create and share content, connect with others, and participate in social networking.

T

Telemedicine: The use of digital technologies to provide remote healthcare services, particularly in underserved areas.

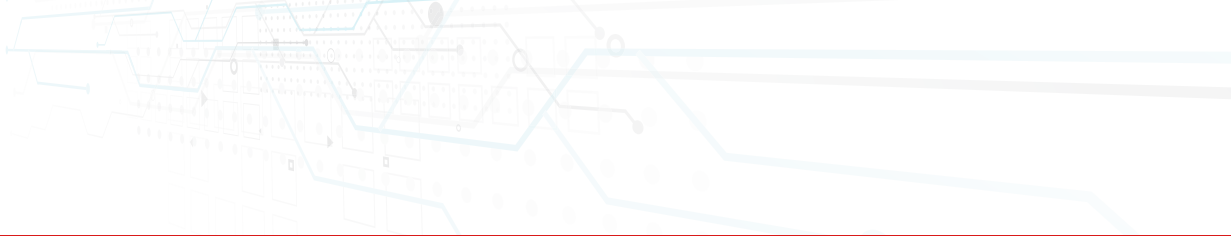
Two-Factor Authentication (2FA): A security process that requires users to provide two forms of identification before accessing an account, enhancing security.

V

Virtual Private Network (VPN): A service that encrypts internet traffic and masks the user's IP address, providing privacy and security online.

W

Web Literacy: The ability to read, write, and participate on the web, including skills like fact-checking, privacy protection, and content creation.



Enabel team

Céline MEWISSEN, Gender and Digital Expert

Cheikh Ahmadou Bamba FALL, Expert Entrepreneurship, Innovation and digitalization

Cristina DE LORENZO BROTONS, Coordinator of D4D Hub African Branch

Florence OTIENO, Intervention Officer Digitalisation Kirsten VAN CAMP, D4D expert

Kirsten VAN CAMP, Digital Transition Expert

Lionel TIENTEGA, Project Manager

Moses OWINY, Digital Rights Expert

Malick TAPSOBA, Digitalisation and Innovation Expert

Nils JANSSENS, D4D Hub Communication and Outreach Officer for Africa

Sebastian OTTE, Digital Transition Expert

Sheetal KUMAR, Consultant on human rights, digital tech policy and internet governance

List of partners and experts that contributed

Name	FAMILY NAME	Position	Organization	Country
Sanyu Agnes	MULUNGI	Communications Director	HER Internet	Uganda
Nakyejwe	SHIRLEY	Senior ICT Officer	Ministry of ICT and National Guidance	Uganda
Peninah Susan	IGAGA	Legal Services Manager and Response Lead	BarefootLaw	Uganda
Patricia	NAMAKULA	Program Manager	ICT Association of Uganda	Uganda
Peace	AMUGE	Africa Regional Strategy Lead	Association for Progressive Communications	Uganda
Esther	NYAPENDI	Technical Support Officer	Women of Uganda Network (WOUGNET)	Uganda
Avis	MOMENI	Secretary General/Digital Rights advocate	Protege QV	Cameroon
Israel	SHEILA	Researcher	Global Rights Alert Uganda	Uganda
Koti Ange Laurentia	DA	Digital Content Creator	Heroines du Faso	Burkina Faso
Charles	BAZIÉ	President	Youth Open Data	Burkina Faso
Rokia Malika	TISSOLOGO	Senior trainer in Media and Information Literacy (MIL)	Fasocheck	Burkina Faso
Amidou	BANDE	Secretary General	CIL	Burkina Faso
Zakaria	SAWADOGO	Researcher / Ex-Vice President	Internet Society BF	Burkina Faso
Arlette	HIEN	Journalist	ABB Check	Burkina Faso
Reine Stephanie	THIOMBIANO	Secretary general	Center of the Burkinabe Association for Family Welfare (ABBEF)	Burkina Faso
Peter King	QUAYE	Executive Director	West Africa ICT Action Network	Liberia
Ababacar	DIOP	Executive Director	JONCTION	Senegal
Jaly	BADIANE	Présidente/Coordonnatrice	Wa Mbed Mi Association / Center for social and environmental innovation	Sene
Demba	Gueye	Members	Africtivistes	Senegal
Serigne Abdou Lahatt	SYLLA	Conseiller Technique	MCTN	Senegal
Yaye Fatou	SARR	Responsable des opérations	Simplon Sénégal	Senegal
Abdourahmane	MARENA	Activistes/ Plaidoyer pour la Paix, la sécurité et les droits de l'homme	S4D Senegal	Senegal
Peace Oliver	Amuge	Africa Strategy Lead	Association for Progressive Communications (APC)	Uganda
Arzu	Geybulla	Co-executive Director	Access Now	Türkiye

