RECIPE
Recentering The Civic Internet Through Partner Engagement

Co-funded by the European Union

OXFAM

MZALENDO

DIGITAL GOVERNANCE TRAINING MANUAL

Training Manual for Civil Society Organizations on Digital Governance Framework, Safety, and Emerging Trends

Disclaimer

This publication was co-funded by the European Union. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.

Published by

MZALENDO TRUST
P. O. Box 21765 - 00505 Nairobi, Kenya
Email: info@mzalendo.com
Website: www.mzalendo.com

Design, Layout & Printing by Mzalendo Trust

This publication was co-funded by the European Union. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.

TABLE OF CONTENTS

ABBREVIATIONS

AI	Artificial Intelligence
CAJ	Commission on Administrative Justice
CIPIT	Center for Intellectual Property and Information Technology
COK	Constitution of Kenya
CSOs	Civil Society Organizations
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information, Communication Technology
KICTANet	Kenya ICT Action Network
NGO	Non- Governmental Organization
ODPC	Office of the Data Protection Commissioner
ReCIPE	Re-centering the Civic Internet through Partner Engagement
TFGBV	Technology-Facilitated Gender-Based Violence
ToTs	Trainer of Trainers
WHRDs	Women Human Rights Defenders

ACKNOWLEDGEMENTS

A lot of dedicated effort and commitment has gone into the development of this training manual. Mzalendo Trust takes this opportunity to extend its sincere appreciation to all those who contributed in various ways to the successful completion of this resource.

The shared knowledge, expertise, and perspectives have resulted in a manual that will greatly enhance digital safety and governance practices among civil society organizations. The contributions from diverse stakeholders have enriched the content, ensuring its relevance and applicability in the evolving digital landscape.

Special thanks go to Irungu Houghton and Victor Ndede of Amnesty International Kenya, Linda Obonyo of Lawyers Hub, John Walubengo and Tracy Onyango of the Office of the Data Protection Commission, Nelly Rotich of Strathmore's Centre for Intellectual Property and Information Technology Law (CIPIT), and Benjamin Kahindi of Safe Community for their invaluable insights and unwavering support throughout this process. Their dedication to strengthening digital governance has played a pivotal role in shaping the direction of this manual.

We also extend our appreciation to Gitungo Wamere, Grace Naiserian and Vallary Acholla and Fredrick Ajok of Mzalendo Trust for their significant contributions and dedication in ensuring the successful development and design of this manual. Their guidance and input have played a crucial role in refining the content and aligning it with the needs of civil society organizations.

A heartfelt thank you goes to Kitaka Ngala of APL Consultants for his leadership in spearheading the development of this manual. His expertise, coordination, and dedication have been pivotal in bringing this manual to fruition.

This training manual would not have been possible without the collective efforts of all contributors. We are confident that it will serve as a valuable tool in strengthening digital safety and governance within civil society, fostering a more secure and responsible digital environment.

We look forward to seeing the positive impact this manual will have on its intended audience and remain committed to continued collaboration in advancing digital governance and security. All communication and visibility activities should be carried out in close co-operation between the Mzalendo trust and targeted organizations. The visibility of the document will also be in line with the communication and visibility plan by Mzalendo Trust.

BACKGROUND

About Mzalendo Trust

Mzalendo Trust was founded in 2013, with an endeavor to promote public participation, openness and inclusivity in the decision-making process. Mzalendo seeks to bridge the gap between policy making and citizen participation. Mzalendo Trust seeks to contribute to the implementation of the digital rights and access to information legal regimes. The organization seeks to creatively and constructively inform the evolving digital rights and access to information discourse. It aims to boost civic awareness on digital rights and access to information and to increase civic engagement in improving corresponding regulation. Mzalendo is implementing **ReCIPE (Recentering the Civic Internet through Partner Engagement) project** which is an **Oxfam-led** multi-country and multi-annual project co-funded by the European Union. The project will be implemented for 3 years in 10 countries across the world namely Senegal, Tunisia, Kenya, Somalia, Occupied Palestinian Territories (OPT), Uganda, Cambodia, Vietnam, El Salvador, and Bolivia. The project aims to cultivate a rights-respecting digital ecosystem that is value-based, human-centric and safe for civil society actors and human rights defenders."

The ReCIPE Project's capacity-building interventions aim to address significant knowledge gaps in digital rights through a participatory and inclusive approach. Expected outcomes:

1. **Outcome 1:** Increase collaboration between the 'Global South' and 'Global North' to create vibrant and safe online civic spaces.
2. **Outcome 2:** Improve digital rights mechanisms and policies.
3. **Outcome 3:** Foster equitable access to safe and secure online social and political activities.

State of Access to Digital Arena and Digital Rights for CSOs

Kenya, has in the recent past, gradually experienced a shrinking space for civil society, resulting from laws restricting freedom of expression and information, in the media and emerging digital spaces. Policy implementation at the National Level as well as its connection with public participation and the enjoyment of democratic freedoms in line with regional and global commitments remain a challenge. For instance, activist and journalists reporting on 'sensitive' topics – misappropriation of public funds, politics, security and counter-terrorism issues – have been arrested, questioned, and detained, including for sharing information via social media platforms. Laws on hate speech and defamation (such as the 2018 Computer Misuse and Cybercrimes Act) are used to prosecute critical voices and dissidents online.

The impact of this closing space has been a notable decline in people's participation in decision making and governance processes and the censorship of individuals and CSOs. Human rights defenders who have taken to social media without full realization of the need for digital protection and security and with little regard for physical and digital safety, are increasingly coming under attack online and offline and the internet has become the new frontier for restricting freedom of expression. Additionally, during the 2022 general elections in Kenya, social media fake news and lack of clear policies and legislation on privacy, data protection and access to data posed a major challenge for citizens and human rights defenders to inform themselves, monitor election processes and freely express their opinions online.

Justification for the Development of a Training Curriculum

A study on Political Participation of youth (2016) revealed that only 52% of youth know government initiatives towards youth participation in politics and 76% of them noted they have not benefited from government-initiated youth programs. CSOs experience hostile and restrictive operating environments and increasing reduction of operating space for civil society. Since independence, there have been several attempts by the Kenyan State to constrain the civic and democratic space through punitive and prohibitive governance frameworks (legal, policy and administrative actions) targeting the civil society. In 2021, the National Assembly introduced a new bill (Community Groups Registration Bill) that aim to restrict registration and management of CSOs.

Journalists reporting on violence and human rights violations were silenced and there were increased instances of intimidation and harassment in retaliation for online activities. Political bots were highly influential in shaping the online discourse around the elections: reports on 2022 elections noted that bot armies worked tirelessly to undermine the influence of media outlets, independent bloggers, government entities, and even messages from politicians and candidates.

According to the GLOCEPS, Policy paper 2021: on social media disinformation and Kenya's 2022 general elections: mitigation options, the most noteworthy threat were the upsurge of disinformation and misinformation by political actors as they advance their agenda. This was occasioned by the limited capacity to fact-check, regulate, and prosecute the adversities of social media disinformation and misinformation. Even with a myriad of laws governing various aspects on the social media space, experts opined that their implementations are disjointed, ambiguous, and inadequate to the prevailing realities.

Finally, access to information and vital data for knowledge and advocacy remains a challenge among CSOs. While most CSOs rely on reports/data from national government institutions, county government, development institutions and other CSOs, the same information/data or reports are always complex, bulky and/or delayed.

Mzalendo trust in collaboration with **Oxfam- Kenya** is developing this training manual for civil society organisations on digital governance frameworks, safety and emerging trends. As part of its country strategy, Oxfam in Kenya has committed to a more supportive, facilitative approach that will foster the strengthening of local partners by supporting the localization agenda and shifting the powers to the local Civil Society Organizations.

[1] East African Institute. (2016). The Kenya youth survey report 2016. Aga Khan University. https://shorturl.at/vAgbB

How to Use This Manual

Before using this manual, read through it thoroughly and revisit each module for clarity:

1. **Objectives:** This describes what participants should learn by going through the module. It is suggested that each module be introduced to the participants by informing them of the key points in the module and what is to be covered in it.
2. **Duration:** This is how long training on the module should take, based on experience. This duration is however not fixed and may need to be adjusted in view of the target participants undertaking the training programme.
3. **Facilitator's Notes:** These notes will assist the facilitator to facilitate the module better by identifying and highlighting key points to focus on and prepare for. It is suggested that the facilitator reads these notes before embarking on facilitation.

This manual contains a few legal concepts, words and terminologies that the facilitator may not use often. It is vital to know the meaning of the concepts and terminologies when facilitating the modules in this manual. A legal dictionary is an important resource for interpretation of legal terms. In this context, training refers to; the process of developing specific skills, knowledge, or abilities in individuals to improve their performance, competence, or capacity in a particular area. It often involves structured instruction, practice, and feedback to help individuals or groups achieve desired outcome.

The aim of the 'Facilitator's notes' is to:

1. *Outline and explain the planning and preparation that the facilitator(s) needs to make ahead of any training workshop*
2. *Outline to the facilitator(s) some of the challenges of training*
3. *Disseminate appropriate ideas and tools that can support the facilitator(s) to create an environment in which trainees can acquire knowledge based on the principles of adult learning.*
4. *Formulate 'tailored' questions to enhance learning*
5. *Present a programme plan for the training.*
6. *Present a monitoring tool to evaluate the learning of trainees by comparing knowledge before and after the training session.*

Below are some best practice guidelines for preparing for a training of facilitators (ToT) workshop:

The participants

The participants should ideally be a manageable number if the training is being conducted by one facilitator. The recommended number is twenty-five (25). The participants should be able to at least speak, read and write in English, which is the language used to conduct the course. The participants will then be able to train other CSO members.

Training Methods

To ensure effective learning, a variety of training methods should be employed in each module. These methods include:

- **Group and Plenary Discussions:** Facilitate shared learning and encourage interaction.
- **Brainstorming:** Foster creativity and collective problem-solving.
- **Individual Reflection and Work:** Allow participants to internalize concepts and relate them to their contexts.
- **Case Studies:** Analyze real-world examples to apply theoretical knowledge
- **Role Plays:** Simulate practical scenarios for experiential learning.
- **Buzz Groups:** Enable small-group discussions for more focused interaction.
- **Lectures and Presentations:** Deliver concise and clear information to introduce key concepts.
- **Audio-Visual Materials:** Enhance understanding through engaging multimedia content

When delivering training:

1. Use simple, clear language and avoid technical or legal jargon.
2. Limit the use of lengthy lectures and large group discussions to maintain engagement.
2. Limit the use of lengthy lectures and large group discussions to maintain engagement.

Materials for Participants

The workshop should equip participants with the most relevant resource materials, such as handouts, to support their learning and engagement. These materials should be:

- **Accessible and Relevant:** Ensure that all materials are directly aligned with the training objectives and session topics.
- **Engaging and Informative:** Include content that participants can easily understand and apply to their contexts.

Encourage participants to:

- **Pre-read Materials:** Review the provided resources before the training to familiarize themselves with key concepts.
- **Engage During Training:** Use the materials actively throughout the sessions for deeper understanding.
- **Refer to Session-Specific Content:** Continuously relate the materials to the topics discussed during the workshop.

Venue and Room Layout

Ensure the training organizers choose a venue that fosters both learning and team-building. The space should be well-lit, properly ventilated, and comfortable for all participants. Arrange seating in a semicircle or horseshoe shape to facilitate clear visibility and interaction among participants and the facilitator.

Workshop Programme

A three-to-five-day workshop is ideal; however, the programme should be tailored to meet the specific needs of the participants. Adjustments to the content or structure should be made as needed to ensure relevance and effectiveness.

Each day should follow a structured flow:

1. **Morning Recap:** Begin with a review of the previous day's key points to reinforce learning and set the stage for the day.
2. **Programme Overview:** Introduce the day's agenda and invite participants to share their input or expectations.
3. **Session Delivery:** Conduct sessions as planned, ensuring they align with participants' needs and objectives.
3. **Daily Wrap-Up:** Conclude with a summary of the day's key takeaways, encourage participants to commit to actionable steps, and provide acknowledgments for contributions.

Training Module Layout

Each module is structured to ensure clarity and ease of facilitation. The layout includes:

1. **Overview:** A brief introduction to the module's focus and purpose.
2. **Learning Objectives:** Clear statements outlining what participants are expected to achieve by the end of the module.
3. **Learning Objectives:** A breakdown of the sessions, specifying:

    - The time allocated for each session (with flexibility to adjust based on facilitation needs).
    - The methods or processes to be followed, presented step by step.

Modules are designed to build sequentially, with each one building on the knowledge and skills covered in the previous module. Sessions should be followed in the prescribed order for optimal learning outcomes. The sections are divided into four areas (modules) namely:

- Introduction section: This builds the background to digital landscape. Specifically it looks at understanding of the digital rights and governance, its importance, identifying challenges, and developing strategies for addressing challenges faced by CSOs.
- Module 1: looks at the legal frameworks for digital governance. The module discusses key legal frameworks governing digital governance in Kenya and their implication to CSOs.
- Module 2: addresses digital safety and security. This section details concepts and principles of digital safety and security, as well as, criminality in online communication and speech.
- Module 3: Discusses the emerging trends and opportunities for CSOs.

At the end of each module, facilitators should administer wrap-up questions designed to reinforce key learning points and encourage reflection. This ensures participants consolidate their understanding before progressing to the next module.

Evaluation

At the end of each session, invite participants to provide oral feedback on their experience and key takeaways. Take note of their suggestions where necessary to improve the ongoing sessions and overall training process. After each module, conduct a more comprehensive evaluation where participants assess the content, delivery, and relevance of the training. Use a written evaluation tool, such as the Workshop Evaluation Questionnaire, to gather structured and detailed feedback. These evaluations ensure the training remains responsive to participants' needs and continuously improves for maximum impact.

INTRODUCTION: UNDERSTANDING THE DIGITAL LANDSCAPE

SESSION OBJECTIVES

By the end of this session, participants will:

- Understand the concept of digital rights and governance.
- Recognize the importance of digital rights for civil society organizations (CSOs).
- Identify the challenges faced by CSOs in advocating for digital rights.
- Explore strategies for addressing these challenges and promoting digital inclusion.

SESSION PLAN

Introduction (15 minutes)

1. **Icebreaker Activity:** Ask participants to reflect on how technology has impacted their advocacy work and share one example of a digital challenge they've faced
2. Define Digital Rights:
   - Explain that digital rights are fundamental human rights adapted for the digital age. These include freedom of expression, privacy, and access to information.
   - Highlight that these rights apply online just as they do offline.

Facilitators Guide

Introduction to Digital Rights and Governance (10 minutes)

Facilitator Key Points:

- *Define digital rights:* The rights to freely use, share, and access information on the internet without fear of censorship or surveillance. (*The UN General Assembly and the UN Human Rights Council have adopted several resolutions on digital rights, including resolutions on privacy, internet access, and children's rights.*) The UN defines digital rights as human rights that apply in the digital world. These rights include privacy, security, and freedom of expression. They also include the right to access and use technology.
- *Define digital governance:* Policies, laws, and frameworks regulating digital technologies and the internet.
- *Highlight why governance is critical:* Ensures accessibility, security, and freedom in the digital space.

Discussion Question:

- *How do digital rights mirror or differ from traditional human rights?*

Activity:

- Ask participants to share examples of digital rights violations they've encountered or heard of.

2. Core Components of Digital Rights (15 minutes)

Facilitator Key Points:

- Digital rights are extensions of basic human rights to the online world.
    - *Right to freedom of expression.*
    - *Right to access information*
    - *Right to privacy.*
- Privacy as a cornerstone for activists, journalists, and CSOs
    - *Prevents unwarranted surveillance and intimidation.*
    - *Protects networks and communication.*

Case Example:

Facilitator Key Points:

- Discuss incidents in Kenya where activists have faced digital surveillance.

Activity:

- Small group discussion: "Why is privacy critical for the work of human rights defenders? How can we safeguard it?"

3. Digital Threats in Kenya (15 minutes)

Facilitator Key Points:

- *Surveillance threats: Monitoring of activists and journalists.*
- *Data misuse: Unauthorized collection and use of personal data for political manipulation.*
- *Cyber -security gaps: Breaches exposing sensitive information.*

Case Example:

- *Highlight recent instances of data breaches or misuse of digital tools in Kenya.*

Activity:

- *Introduce encryption tools or secure messaging apps. Briefly demonstrate how to use them.*

4. Kenya's Legal Framework and Challenges (20 minutes)

Facilitator Key Points:

- Progress made: Enactment of the Data Protection Act (2019).
    - *The right to privacy in Kenya is protected by Article 31 of the Constitution. This article states that everyone has the right to privacy, which includes the right to not have their person, home, or property searched.*
    - *Framework for collection, processing, and storage of personal data.*
    - *Role of the Data Protection Commissioner.*
- Challenges:
    - *Low public awareness of digital rights.*
    - *Weak enforcement of laws.*
    - *Political interference in regulatory bodies.*

Discussion Question:

- What can be done to increase public awareness of digital rights in Kenya?

Activity:

- Role-play: One group represents CSOs advocating for digital rights; another represents the government defending its surveillance measures.

5. Strengthening Digital Rights in Kenya (20 minutes)

- Raise awareness:
    - *Educate citizens about their rights.*
    - *Train CSOs on digital security tools.*
    - *Political interference in regulatory bodies.*
- Strengthen legal frameworks:
    - *Enforce existing laws.*
    - *Update frameworks to address emerging threats.*

- Promote collaboration:
    - *Encourage partnerships between government, civil society, and private sector.*
- Foster international cooperation:
    - *Align Kenya's policies with global standards.*

Activity:

- Brainstorm in pairs: "What practical steps can CSOs take to strengthen digital rights in their communities?"

5. Closing and Call to Action (10 minutes)

Facilitator Key Points:

- Emphasize the importance of digital rights as fundamental to democracy.
- Advocate for proactive engagement to protect and promote these rights.

Call to Action:

- Participants identify one action they will take in the next month to advocate for digital rights or improve their digital security practices.

Materials Needed:

1. Presentation slides summarizing key points.
2. Case studies or examples of digital rights violations.
3. Access to encryption or secure messaging apps for demonstration.

Additional Notes for Facilitator:

1. Be mindful of participant knowledge levels; simplify jargon where necessary.
2. Foster an inclusive and interactive environment to encourage participation.
3. Provide handouts summarizing key legal frameworks and tools for digital security.

What are Digital Rights and Governance?

Digital rights encompass the rights of individuals and organizations to freely use, share, and access information on the internet without fear of censorship or surveillance. Governance in the digital space refers to the policies, laws, and frameworks that regulate the use of digital technologies and the internet. These frameworks are essential for protecting the rights of human rights defenders, activists, and journalists, ensuring their physical and online safety when working on sensitive topics.

Digital governance frameworks ensure that the online space remains accessible, secure, and free from censorship. For CSOs, these frameworks offer the tools necessary to engage citizens, share information, and advocate for policy changes, even when addressing politically sensitive or security-related issues.

Importance of Digital Rights for CSOs

1. CSOs, including human rights defenders and activists, rely on the internet for:
    - *Communication*
    - *Advocacy*
    - *Collaboration*
2. Digital rights ensure that these organizations can::
    - *Operate without undue interference or threats*
    - *Promote transparency, accountability, and democratic participation*
    - *Address sensitive issues such as: Misappropriation of public funds, Political accountability etc.*

The importance includes:

a. **Protecting digital rights:** CSOs can monitor internet standards to ensure that they uphold fundamental rights like privacy, free expression, and access to information.

b. **Building trust:** CSOs can help build trust by demonstrating a commitment to transparency, openness, and participatory governance.

c. **Freedom of expression:** CSOs can use digital rights to protect their ability to advocate for citizens' rights, even in challenging political environments.

d. **Accountability:** CSOs can use digital tools to monitor government actions and public expenditure, and to identify and report corruption.

The importance includes:

e. **Transparency:** CSOs can use digital tools to increase transparency by making data accessible to citizens.

f. **Empowerment:** CSOs can use digital tools to empower users to understand and navigate the digital landscape.

g. **Preserving democratic values:** Investing in digital rights is critical for preserving democratic values and ensuring civil society's capacity to hold power to account.

Challenges Faced by Civil Society Organizations

i. Misinformation on online platforms

The rapid growth in misinformation on online platforms; leading to backlash from states, who attempt to regulate it with broad 'fake news' regulations. Defining and protecting journalists and the media in an environment now saturated with bloggers and social media writers, and defending them from online harassment, particularly women who are disproportionately subject to online harms.

ii. Access to Digital Platforms and Information

The challenge of enabling free and equal access to Digital Platforms and Information, including overcoming the challenges of inequalities in acquisition of digital tools, while preventing distortion. CSOs, particularly those addressing sensitive topics such as misappropriation of public funds, politics, and counter-terrorism, face significant challenges in accessing reliable information. These challenges are increased by restrictive laws, delayed government reports, some information in government websites unavailable, and competition within the CSO sector on digital governance.

iii. Shrinking Civic Space in Kenya

In recent years, there has been a gradual shrinking of civic space in Kenya, worsened by restrictive laws like the Computer Misuse and Cybercrimes Act of 2018. This has made it increasingly difficult for CSOs, human rights defenders, and activists to operate freely, especially when addressing sensitive topics such as human rights violations, corruption, and political issues. According to Civicus, the primary indicators for assessing the state of civic space include: freedom of association, freedom of peaceful assembly, freedom of expression, and the state's duty to protect civil society; essentially measuring how well a country respects these fundamental rights in law, policy, and practice, allowing citizens to participate freely in public life without undue restrictions.

iv. The Impact of Restrictive Laws and Regulations

Laws like the Computer Misuse and Cybercrimes Act have been used to suppress online criticism, particularly from journalists, human rights defenders, and activists. Such laws create an environment of fear, hindering open dialogue and engagement, and complicating advocacy efforts on sensitive issues such as security, counter-terrorism, and political transparency. Noted, online content regulation through overly broad and vague cybercrimes legislation intending to counter genuinely criminal activity online, such as child pornography, but often misused by governments to stifle criticism and free speech.

1. Background to Digital Access and Inclusion

Overview of the Digital Landscape in Kenya

- **Internet Use and Social Media:**

  a) Kenyans spend an average of 3 hours 43 minutes daily on social media, surpassing the global average by 1 hour 13 minutes.

  b) Internet penetration in Kenya is approximately 56.03%.

  c) Rural areas experience limited internet access due to infrastructure and economic barriers.

  d) Urban-rural divide persists, with most internet users concentrated in urban areas. (A "rural and urban digital divide" refers to the significant gap in access to and usage of information and communication technologies (ICTs) between people living in urban areas, who typically have much greater access to the internet and digital tools, compared to those residing in rural areas, where infrastructure limitations and economic factors often hinder connectivity.)

  e) There is also prevalence of internet shutdowns in Kenya. For instance Surfshark recorded 116 cases of internet disruptions globally in 2024, with Kenya among the affected countries.

- **Connectivity Infrastructure:**

  a) Kenya is connected to six submarine fiber cables (SEACOM, TEAMS, EASSy, LION2, DARE1, PEACE) that enhance international bandwidth.

  b) Electricity interruptions and ageing infrastructure disrupt home internet services in rural and urban areas.

- **Rural and Underserved Populations:**

  a) 71% of Kenyans live in rural areas with limited internet access and services.

  b) Economic barriers prevent access to devices and affordable internet.

- **Youth and Education:**

  a) Limited access to digital platforms affects education opportunities for rural and marginalized communities.

- **Financial Inclusion:**

  a) Exclusion from digital financial services increases vulnerability to cybercrime.

2. Barriers to Digital Access and Inclusion

- **Affordability:**

  a) High cost of internet access excludes lower-income and rural populations.

  b) Launch of Starlink in 2023 has offered lower-cost internet but faces opposition from local mobile network operators (MNOs) it also has high cost of initial setup

- **Gender Digital Divide:**

  a) 39% of women and 59% of men have internet access, highlighting a significant gap.

- **Disability Inclusion:**

  a) Persons with disabilities face barriers in accessing financial services and internet platforms due to lack of accessibility features.

- **Digital Literacy and Energy Access Challenges**

  a) Digital literacy remains a significant barrier, particularly for older populations and individuals in rural areas.

  b) Limited energy access, such as the lack of electricity in rural regions, poses a fundamental challenge to internet connectivity.

- **Government Websites:**

  a) Many government websites score poorly on accessibility, according to the KICTANet Accessibility Scorecard 2023.

  b) Marginalized counties such as Mandera, Turkana, Wajir and Kwale still face challenges in provision of online county government information.

3. Barriers to Digital Access and Inclusion

4. Digital Rights and Human Rights

- **International Frameworks and Policy Alignment:**

  a) Kenya is a signatory to key UN resolutions on digital rights, including those that emphasize internet access as a fundamental right and call for restrictions on internet shutdowns and censorship.

  b) The African Declaration on Internet Rights and Freedoms provides a regional framework for promoting digital rights, emphasizing privacy, access, and freedom of expression.

  c) There is a need for stronger alignment between Kenya's digital policies and international human rights standards, particularly in content moderation, data protection, and cybersecurity.

- **Impact of Public Protests and Government Crackdowns**

  a) During the #RejectFinanceBill2024 protests, internet shutdowns, geospatial tracking, and censorship were widely reported, restricting digital rights.

  b) These measures contributed to a downgrade in Kenya's Freedom on the Net rating, which is now classified as "Partly Free" (64/100) in 2025 by Freedom House.

- **Hate Speech and Misinformation**

  a) The August 2022 elections saw a rise in hate speech and misinformation online, which contributed to political tensions and instability.

  b) Social media platforms faced challenges in content moderation, struggling to balance free speech protections while curbing harmful content.

- **Digital Privacy Concerns**

  a) Government-led digital ID initiatives, such as Maisha Namba digital ID and the digitization of public services, have raised concerns about data protection, privacy, and the risk of exclusion.

  b) Automated decision-making in digital ID verification could disproportionately marginalize vulnerable communities, particularly Somali and Nubian populations who face documentation challenges.

- **Cybersecurity Threats**

  a) Activists, journalists, and civil society organizations in Kenya face increasing cybersecurity threats, including:

  b) Hacking and phishing attacks targeting sensitive communications.

  c) Doxxing and digital harassment aimed at silencing dissent and human rights defenders.

  d) The lack of robust cybersecurity protections leaves many vulnerable to digital surveillance and data breaches.

5. Progress and Recommendations

- *Achievements:*

  a) Kenya's Vision 2030 prioritises expanding ICT infrastructure.

  b) Over 5,000 government services digitised by mid-2023.

- *Recommendations for CSOs:*

  a) Advocate for policies addressing affordability, accessibility, and inclusion.

  b) Promote gender-sensitive approaches to bridge the digital gender divide.

  c) Support initiatives enhancing digital literacy for marginalised groups.

  d) Engage in collaborative efforts with the government to strengthen data protection frameworks and the overall digital governance frameworks

6. Role of CSOs in Digital Access and Inclusion

- **Advocacy and Awareness:**

  a) Advocate for the right to access affordable internet, safe and secure digital spaces for all people.

  b) Raise awareness on the digital divide and its effects on marginalised communities.

- **Capacity Building:**

  a) Provide training on digital literacy, especially for underserved populations.

  b) Collaborate with grassroots organisations to promote inclusive digital solutions.

- **Monitoring and Accountability:**

  a) Monitor government policies and advocate for transparency in digital initiatives.

  b) Ensure inclusivity in the digitisation of public services.

  c) Doxxing and digital harassment aimed at silencing dissent and human rights defenders.

  d) The lack of robust cybersecurity protections leaves many vulnerable to digital surveillance and data breaches.

7. Key Takeaways for CSOs

a) A secure, inclusive, and accessible digital environment is essential for sustainable development.

b) Fostering inclusivity ensures that no one is left behind in the digital age.

MODULE 1: **LEGAL FRAMEWORKS FOR DIGITAL GOVERNANCE**

Session Objectives

By the end of this session, participants will:

- *Understanding Legal Frameworks: Familiarize participants with constitutional provisions, acts, and policies governing digital governance in Kenya.*
- *Enable CSOs to align their operations with legal requirements and advocate for digital rights.*
- *Equip participants with knowledge on cybersecurity laws and strategies to protect organizational and personal data.*
- *Guide CSOs on leveraging the Access to Information Act for transparency and accountability.*
- *Discuss the ethical implications and governance of AI in Kenya's digital landscape.*

Session Plan

Introduction (15 minutes)

Icebreaker Activity: Ask participants to reflect on how policies and laws has impacted their advocacy work and share one example of a digital challenge or benefit faced due these legal frameworks.

Define legal framework on digital governance:

- *Explain that "legal framework in digital governance" refers to the set of laws, regulations, and policies that govern the use of digital technologies in government operations, including aspects like data privacy, cyber security, electronic signatures, digital identity management, and online service delivery, ensuring legal compliance and accountability in the digital sphere;*

Session 1. Introduction to Legal and Strategic Frameworks in Kenya (15 minutes)

Facilitator Key Points:

- Provide an overview of the constitution of Kenya
- Give example of digital rights

Discussion Question:

- What are the national values and principles related to digital governance?

Activity:

- Put participants into groups and ask them to identify key legal provisions affecting CSOs in relation to digital governance.

Session 2. Kenya National Digital Master Plan 2022-2032 (15 minutes)

Facilitator Key Points:

- Give an overview of the National Digital Plan
- Discuss objectives and pillars of the Digital Master Plan
- Discuss key provisions and weakness

Facilitator Key Points:

- How CSOs can leverage the Master Plan for advocacy?

Activity:

- Brainstorm in pairs the implication of the Master Plan to CSOs and community engagement

Session 3: **Access to Information Act No. 31 of 2016 (15 minutes)**

Facilitator Key Points:

- Provide access to information Act
- Discuss objectives and pillars of the Digital Master Plan
- The right to information
- Challenges and barriers to information

Discussion Question:

- What role do CSOs play in promoting transparency and accountability?

Activity:

- Drafting access –to information requests.

Session 4: **Data Protection Act No. 24 of 2019 (20 minutes)**

Facilitator Key Points:

- Overview of the data protection Act
- Principles of data protection and privacy
- Key provisions and weaknesses

Discussion Question:

- What are the responsibilities of data controllers and processors

Activity:

- Scenario-based discussion: Ensuring compliance in CSO activities

Session 5: **Kenya's Cyber-security and Digital Rights (15 minutes)**

Facilitator Key Points:

- Key provisions of the Computer Misuse and Cybercrimes Act

Discussion Question:

- How can CSOs identifyand mitigate cyber threats?

Activity:

- In groups engage the participants in developing a digital security plan for their CSO

Session 6: **AI Governance and Ethical Considerations (20 minutes)**

Facilitator Key Points:

- Overview of the Kenya National Strategy 2025-2030
- Key strategies affecting CSOs

Discussion Question:

- What are the ethical implications of AI in governance and service delivery?

Activity:

- In groups engage the participants in developing a digital security plan for their CSO

Session 7: **Closing and Call to Action (10 minutes)**

Facilitator Key Points:

- Emphasize the importance of understanding these legal frameworks.
- Emphasize the importance of compliance to these acts

Call to Action:

- Participants identify one action they will take in the next month to advocate for change or implementation of a legal framework of their choice.

Materials Needed:

1. Presentation slides summarizing key points.
2. Case studies or examples of failure to adhere to legal frameworks especially in Kenya.

Additional Notes for Facilitator:

- Be mindful of participant knowledge levels; simplify jargon where necessary.
- Foster an inclusive and interactive environment to encourage participation.
- Provide handouts summarizing key legal frameworks and tools for digital security.

Session 1: Introduction to Legal and Strategic Frameworks in Kenya

Facilitator's notes.

- Ensure familiarity with Kenya's Constitution, especially provisions on digital rights.
- Highlight the role of CSOs in advocating for digital governance reforms.
- Use real-world examples to make concepts relatable.

The Constitution of Kenya, 2010

The Constitution of Kenya, 2010 (COK, 2010) is the 'supreme law of the Republic (of Kenya), and binds all persons and all State organs at both levels of government (National and County governments). Any law that is inconsistent with the constitution is void to the extent of the inconsistency. The document safeguards fundamental rights and freedoms as stipulated in the Bill of Rights, and is touted as one of the most progressive and liberal regimes of human rights in the region. These rights, including the right to privacy and right to access to information must be respected, upheld and protected by all organs and agencies of the government as well as individuals.

Key provisions on or affecting digital governance

- Article 22 provides for the enforcement of these rights and states that: *"Every person has a right to institute court proceedings claiming that a right or fundamental freedom in the bill of rights has been denied violated or infringed, or is threatened."*
- Article 23 *also gives more weight to the upholding and enforcement of these rights and grants jurisdiction to the High Court to hear and determine applications for redress of a denial, violation or infringement of, or a threat to, a right or fundamental freedom in the Bill of Rights.*
- Article 10 *further provides for national values and principles of governance such as rule of law, democracy, participation of the people, integrity, transparency and accountability, which are all key in the implementation of access to information and privacy right.*

Other rights and freedoms provided for in the Bill of Rights, inter alia, include:

- Right to life;
- Equality and freedom from discrimination;
- Human dignity;
- Freedom and security of the person;
- Slavery, servitude and forced labour;
- Privacy
- Freedom of conscience, religion, belief and opinion;
- Freedom of expression
- Freedom of the media;
- Freedom of association;
- Right to assembly, demonstration, picketing and petition;
- Protection of right to property;
- Labour relations
- Environment;
- Economic and social rights;
- Language and culture;
- Consumer rights;
- Fair administrative action;
- Access to justice;
- Rights of arrested persons;
- Fair hearing;
- Rights of persons detained, held in custody or imprison.

Session 2: **Kenya National Digital Master Plan 2022-2032**

Facilitator's notes.

- Break down complex policy details into practical, actionable insights.
- Encourage participants to share experiences on digital initiatives.
- Facilitate discussions on how CSOs can integrate digital strategies into their work

The Kenya National Digital Master Plan 2022-2032

This Kenya National Digital Master Plan is a continuation of the aspirations of the Kenya Vision 2030. It dovetails the initiatives and achievements of the Kenya National ICT Master Plan 2014 – 2017, builds on the pillars of the Kenya Digital Economy Blueprint, and re-focuses the country on the transformative trajectory towards a digital economy. In the conceptual model given in chapter 3, the purpose of this Master Plan is the provision of quality, accessible, affordable, reliable, quality, and secures ICTs in government, with a positioning of Kenya as a globally competitive digital economy.

This Master Plan has four pillars that are responsible for the provision of digital services to citizens, businesses and other stakeholders:

- **Digital Infrastructure:** For equitable access to national service through a pervasive and ubiquitous national ICT infrastructure;
- **Digital Government Service, Product and Data Management:** For provision of e-Government information and services for improved productivity, efficiency, effectiveness and governance in all sectors. It also considers technology related products and services.
- **Digital Skills:** For the development of a digitally skilled workforce and citizenry that is grounded on ethical practices and social cultural values to implement and operationalize this master plan; and;
- **Digital Innovation, Enterprise and Digital Business:** For enhancing the innovation value chain in order to turn innovative ideas into sustainable businesses and operating models. The pillar also aims to shift businesses onto the digital platform.

Challenges:

- While the plan emphasizes quality and secure ICT, there is limited discussion on addressing cybersecurity threats and AI ethics comprehensively. This may leave the digital economy vulnerable to emerging technological risks such as cyberattacks and data breaches affecting key public and private infrastructure.
- Many e-government platforms and digital tools are not available in local languages, limiting accessibility for non-English or Kiswahili speakers.
- Despite a focus on equitable access, marginalized groups, such as people with disabilities or those in remote areas, may face barriers to benefiting from digital services. Inequalities in digital access and literacy could persist, undermining the plan's inclusivity goals.

Session 3: **Access to Information Act No. 31 of 2016**

Facilitator's notes.

- Clarify legal provisions on information access and guide participants in developing effective information requests.
- Discuss challenges and barriers to information access in Kenya.
- Provide strategies for overcoming obstacles in obtaining public information

The Act was enacted to give full effect to Article 35 of Constitution of Kenya (COK), 2010 on the right of access to information, and empower the Commission on Administrative Justice with oversight and enforcement functions. Read together with Article 10 on national values and principles of governance, the Act seeks to promote good governance through efficient, effective, transparent and accountable government by providing full effect to the constitutional right to access information. The objects of the Act include, inter alia: To give effect to the right of access to information by citizens as provided under Article 35 of the Constitution;

Key provisions

- Enhances accountability and aims to reduce corruption by allowing citizens to scrutinize public operations.
- Implements Article 35 of the Constitution of Kenya, which guarantees every citizen the right to access information.
- Reinforces constitutional rights and strengthens the rule of law. The Act allows access to information held by private bodies if it affects public interest. Broadens the scope of transparency, ensuring private entities with public functions are also held accountable.
- Stipulates a clear timeframe of 21 days for public entities to respond to information requests. Encourages timely provision of information and reduces unnecessary delays.
- Empowers the Commission on Administrative Justice (CAJ) to oversee implementation and address complaints related to information access. Provides a formal redress mechanism for citizens when access is denied.
- Mandates public entities to proactively publish information of public interest without waiting for requests. Reduces the burden on citizens to request information and ensures regular dissemination of relevant data.

- Offers protections to individuals disclosing information in good faith. Encourages reporting of wrongdoing without fear of retaliation.

Challenges:

- The Act allows for withholding information under broad exemptions, such as national security, which are not clearly defined. Creates room for misuse and arbitrary denial of information requests.
- Low public awareness of the right to access information and the mechanisms provided for by the Act. Citizens may not utilize the Act effectively to demand accountability.
- The penalties for non-compliance by public officials are weak and rarely enforced. Discourages adherence to the Act's provisions and weakens its impact.
- The Act does not sufficiently address challenges related to accessing information in a digital context, especially for marginalized groups without internet access or digital skills. Limits inclusivity, particularly in rural areas and among disadvantaged populations.
- The Commission on Administrative Justice (CAJ) is underfunded and understaffed, limiting its ability to enforce compliance and address complaints effectively. Reduces the effectiveness of the oversight mechanism. This has led to lack of critical information in the public domain affecting adequate participant in governance matters.

Session 4: **Data Protection Act No. 24 of 2019**

Facilitator's notes.

- Differentiate between personal data, sensitive data, and public information.
- Explain legal obligations for organizations handling data.
- Use practical case studies to illustrate data protection challenges.

Pursuant to the constitutional requirement of Article 31(c) and (d), the right to privacy is given detailed effect by The Data Protection Act No.24 of 2019. This Act governs the protection of personal data. Personal data is information that can be used to identify a natural person and this includes:

- Name
- Phone number
- Birth Certificate
- Location.

Hence the Act requires consent from individuals before using or collecting personal information. The rights of Data Subjects are:

1. To be informed of the use of their personal data
2. Access of their persona data in the custody of data controller,
3. Object to processing of their personal data
4. Correction of misleading or false data
5. Deletion of false or misleading data
6. Right to erasure.

The Act also establishes the Office of the Data Protection Commissioner appointed by the Public Service Commission responsible for regulation of the processing of personal data and providing for the rights of data subjects and obligations of data controllers and processors. Data Controllers are defined as the persons or entities that determine the purpose and means of processing of personal data, while data processors are the persons or entities that process data on behalf of the Data Controller. The Act also details the procedures for rectification and erasure of personal data.

Lastly, the Act has an enforcement section which among other provisions provides for a procedure for complaints and offences for unlawful disclosure of data. A complaint is dissatisfaction with the way personal data has been handled. The complaint is lodged with then Office of the Data Protection Commissioner (ODPC).

Who can lodge a complaint?

- To be informed of the use of their personal data
- Person acting on behalf of the complainant.
- Any other person authorized by law to act on behalf of a data subject.
- Anonymously.

The Act provides for and summarizes the principles of personal data protection as follows: That personal data is-

- Processed in accordance with the right to privacy of the data subject;
- Processed lawfully, fairly and in a transparent manner in relation to any data subject;
- Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes",
- Adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
- Collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- Kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected;
- Not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

These principles are consistent with internationally recognized principles and standards espoused in the documents such as the European Union (EU) Guidelines on Data Protection Rights (GDPR), the United Nations Principles on Personal Data Protection and Privacy and principles developed by the Organization for Economic Co-operation and Development (OECD).

A key case study illustrating both successes and challenges in implementing a Data Protection Act is Kenya's experience with its Data Protection Act, where notable achievements include registering data handlers, conducting audits, and issuing enforcement notices, but ongoing challenges remain regarding awareness, enforcement capacity, and addressing cross-border data flows, particularly in sectors like mobile money services like M-Pesa where personal data is heavily used and potentially vulnerable.

Session 4: **Cyber-security and Digital Rights**

Facilitator's notes.

- Demonstrate cyber-security best practices and discuss real cyber threat cases affecting CSOs.
- Guide participants in creating simple, effective security measures.
- Provide actionable steps for improving digital security within organizations.

The Computer Misuse and Cybercrimes Act No. 5 of 2018

The Act was enacted to provide for offences relating to computer systems, to enable timely and effective detection, prohibition, prevention, responsive investigation and prohibition of computer and cybercrimes and to facilitate international co-operation in dealing with computer and cybercrime matters. The law addresses offences such as cyber espionage, computer forgery, computer fraud, false publication, child pornography, cybersquatting, phishing, identify theft, cyber terrorism among others.

Challenges:

- Instead of placing more emphasis on crimes found in the cyberspace and those crimes related to ICT systems, transactions and communications, the Act goes above and beyond to deal with free speech. Section 22 and 23 in particular are offending provisions in this regard.

Section 22:

"A person who intentionally publishes false, misleading or fictitious data or misinforms with intent that the data shall be considered or acted upon as authentic, with or without any financial gain, commits an offence and shall, on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both."

Section 23:

"A person who knowingly publishes information that is false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence among citizens of the Republic, or which is likely to discredit the reputation of a person commits an offence and shall on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding ten years, or to both."

- There is no scientific formula of determining what is false or 'fake news'. For example, it will be difficult to determine the authenticity of what is 'fake news' as set out in Sections 22 and 23 of the Act which prohibits publishing false, misleading or fictitious data or information that is intended to cause others to act on them as authentic.
- Both sections can also act to deter potential whistle-blowers and journalists from coming out in the open against big personalities, as fear of facing charges in addition to fear for their lives, may weigh heavily in their final decision.
- There is also the lack of a digital forensic laboratory hence the inability by the government to process digital evidence and consequently, the state can take advantage of this loophole to bring trumped up charges against human rights defenders and journalists.

Session 4: **AI Governance and Ethical Considerations**

Facilitator's notes.

- Simplify AI concepts for non-technical participants.
- Discuss ethical dilemmas in AI governance, including data privacy and bias. Use real-world scenarios to explore the impact of AI on digital governance

Kenya National AI Strategy 2025–2030:

This strategic document outlines Kenya's approach to harnessing AI's transformative power to drive sustainable development, enhance public services, and improve social and economic equity.

Kenya aims to become a leading AI hub both in Africa and within the East Africa region. This strategy focuses on creating an enabling environment for responsibly developing quality AI applications that leverage local datasets and talent, ensuring safety, responsibility, and alignment with international human rights standards.

Kenya's National AI Strategy 2025-2030 aims to establish Kenya as a leading African hub for Artificial Intelligence research and innovation, utilizing AI to drive sustainable development, enhance public services, and promote social and economic equity across the country, with a focus on ethical and inclusive AI development tailored to Africa's specific needs; the strategy prioritizes leveraging AI to address challenges like food insecurity, healthcare access, and inefficient public service delivery, while fostering collaboration between government, private sector, and civil society to achieve these goals.

Key points:

- **Vision:** Position Kenya as a regional AI leader in Africa.
- **Focus areas:** Healthcare, agriculture, education, public services.
- **Ethical considerations:** Emphasize responsible AI development with transparency, accountability, and inclusivity.
- **Stakeholder involvement:** Encourage collaboration between government, private sector, academia, and civil society.
- **Economic impact:** Drive economic growth through AI-powered innovation and job creation.

Some of the strategies relevant in this discourse are:

1. **Data Sovereignty and Privacy:** This is directly related to articles 31 and 35 of the Constitution of Kenya regarding Privacy and Access to information. There is fear of data misuse, unauthorized access and a lack of control over personal information.

2. **Ethical AI, Human Rights and the Promotion of Public Trust:** There is the potential use of AI for surveillance on people who criticize the government for illegal purposes. There is also need to ensure that AI developments respect human rights and aligns with Kenyan values. For example, the recent depiction of public personalities has sparked a lot of outrage from people supporting and opposed to the same and hence the need to find a common ground on the use of AI to create almost real images of a person or situation and control of the same to make sure it is within the law.

3. **Regulatory Preparedness:** As it is still a virgin area, there are no laws yet to govern AI in the country, hence the reliance of laws such as the Computer Misuse and Cybercrimes Act to govern the same. Despite some relevance to AI, it is still far from addressing the unique concerns and challenges brought up by AI. For example, if a state agency is able to doctor a image and frame a person as having manufactured the same for illegal intent and decides to prosecute them, there is a very high possibility of proving it hence the need to come up with AI legal frameworks to safeguard against what may turn out to be executive witch hunts against government critics.

Module evaluation quiz

1. What are the main legal frameworks addressing digital governance?
2. Discuss the ethical implications of AI in Kenya's digital landscape?
3. Identify legal frameworks addressing the following
    - Data Piracy
    - Cyber-security
    - Personal data
    - Online service delivery
4. What role do you play in addressing access to information within your region or nationally?
5. How can CSOs take advantage of existing legal frameworks in Kenya to advance digital governance?

MODULE 2: **DIGITAL SAFETY AND SECURITY**

Session Objectives

By the end of this session, participants will:

- *Understand the concepts and principles of digital safety and security*
- *Understand criminality in online speech*
- *Internalize the existing opportunities of online freedom of speech*

Session Plan

Introduction (15 minutes)

Icebreaker Activity: Ask participants to reflect on how they ensure data safety and security

Define digital safety and security:

- *Explain that Digital safety and security, is the practice of protecting digital assets, data, and systems from unauthorized access, attacks, or destruction*

Facilitator's notes.

Session 1: Introduction to digital safety and security (25 minutes)

Facilitator Key Points:

- Overview of data safety and security.
- Discuss the essence of personal and organizational data safety and security
- How to improve CSOs safety and security

Discussion Question:

- How does your organization handle digital safety and security?

Activity:

- Brainstorming: mechanisms that CSOs/HRDs can use to ensure Digital safety and security.

Session 2. Criminalization of Online Speech (15 minutes)

Facilitator Key Points:

- Overview of Online Speech Restrictions in Kenya
- Balance between free speech vis a vis hate speech
- Discuss threats and opportunities for criminalization of online speech
- Give practical examples

Discussion Question:

- Discuss examples indicating criminalization of online speech?

Activity:

- In pairs discuss notable current effects of online speech.

Session 3. Challenges to Online Freedom of Expression (15 minutes)

Facilitator Key Points:

- Discuss opportunities and challenges of online freedom of expression
- Give examples of notable cases.
- Discuss the role of CSOs /HRD in promoting HRDs

Discussion Question:

- Do you think the Kenya government appreciates the online freedom of expression?

Activity:

- In Pairs ask participants to discuss scenarios they have been involved in their freedom of speech? Online or otherwise?

Session 4. Key Recommendations for CSOs and case studies (15 minutes)

Facilitator Key Points:

- Discuss recommendations towards enhancing digital safety and security.
- Provide notable cases of digital safety and security.
- Provide notable cases of digital safety and security.

Discussion Question:

- Do you think the Kenya government appreciates the online freedom of expression?

Activity:

- In Groups ask participants, to develop action plans for digital safety and security.

Session 5. Closing and Call to Action (10 minutes)

Facilitator Key Points:

- Advice on CSOs adopting Digital safety and security mechanisms.
- Appreciating current initiatives/ tools CSOs can use.
- Emphasize on lessons learnt and way forward.

Call to Action:

- Participants identify one action they will take in the next month to advocate for digital safety and security.

Materials Needed:

- Presentation slides summarizing key points.
- Case studies or examples.

Additional Notes for Facilitator:

- Be mindful of participant knowledge levels; simplify jargon where necessary.
- Foster an inclusive and interactive environment to encourage participation.
- Provide handouts for ease of reference.

Session1: **Introduction to Digital safety and security**

Facilitator's notes.

- Provide clear examples of data safety and security, including implications and benefits accrued
- With examples, showcases where digital safety and security was crucial (positive and negative)
- Provide case scenarios of the critical role of CSOs in ensuring data safety and security.

1. Data safety and security

In the CSOs world there are a range of digital safety and security risks to privacy risks to behavioral cyber-risks. There exist various ways in which privacy and security can be compromised by criminal, corporate or state activity which are multiplying and becoming more and more complex. CSOs adopting new strategies and plan they can become less vulnerable to digital insecurities.

Digital security refers to the protection of personal and organizational data from threats like hacking, surveillance, and online harassment. For human rights defenders, journalists, and activists, ensuring digital security is essential to protect sensitive information and ensure safe advocacy, particularly when dealing with sensitive topics such as politics, corruption, and counter-terrorism.

Digital threats can be grouped into three key categories:

a) **Technical Risks:**

- **Hacking:** Unauthorized access to personal or organizational data.
- **Ransomware Attacks:** Malicious software that locks files until a ransom is paid.
- **AI-Driven Surveillance:** Use of artificial intelligence for facial recognition and tracking.

b) **Behavioral Risks:**

- **Phishing:** Deceptive emails or messages tricking users into revealing sensitive information.
- **Social Engineering Attacks:** Use of artificial intelligence for facial recognition and tracking.

b) Behavioral Risks:

- **Doxxing:** Publishing private or identifying information online to intimidate individuals.

c) Legal and Policy Risks:

- **State Surveillance:** Government monitoring of online activities, often justified by national security concerns.
- **Censorship and Content Takedowns:** Suppression of political dissent and human rights activism.
- **Criminalization of Digital Expression:** Use of cyber laws to target journalists and activists.

d) Emerging Digital Security Threats

- **Deepfakes:** AI-generated synthetic media used for disinformation and political manipulation.
- **AI-Driven Surveillance:** Expansion of facial recognition and predictive policing.
- **Ransomware Attacks:** the growing threat of cybercriminals targeting institutions for financial extortion.

Digital security is important for civil society organizations (CSOs) because they increasingly use digital tools for communication, fundraising, and operations. Here are some tips for CSOs to strengthen their digital security:

- Create safety measures: Outline safety measures for staff, facilitate safe online interactions, and ensure the safety of the organization.
- Use strong passwords: Use strong passwords and don't use the same password for all accounts.
- Check URLs: Always check the URL before entering a password.
- Avoid suspicious links: Don't click on links that are irrelevant or seem suspicious.
- Encrypt drives: Encrypt the drives of all computers.
- Avoid attachments: Avoid downloading attachments, and if you do need to view them, do so in a well-protected environment.
- Use digital security controls: Use digital security controls like usernames and passwords, two-factor authentication, antivirus software, and firewalls.

It is important for CSOs to take holistic and relevant measures to ensure that the online engagements and overall operations of the organisation are safe from cyber-attacks. A principal and preliminary action CSOs can take to strengthen their digital security is to conduct a comprehensive risk assessment. This involves identifying potential vulnerabilities and threats, evaluating the impact of a breach or attack, and developing a plan to mitigate risks. This assessment can be done internally if the organisation has the appropriate skill set and or tools or with the help of a digital security consultant.

2. Addressing Personal Digital Safety and Security

Currently, CSOs digital safety depends on how exposed the staff is digitally equipped. Ensuring high personal digital safety and security is crucial to the process of strengthening digital security of CSOs. Here are some ways to improve and ensure \Staff's personal online security:

- *Passwords:* The use of strong passwords: Creation of a strong and unique password for corporate emails and online accounts is essential entails use of a mix of upper and lowercase letters, numbers, and symbols. A key recommendation is to use relatively long passwords.
- *Safe Wifi use and Computers:* Having an original version of softwares and keeping them up to date: Regularly update your operating system, antivirus software, and other applications to ensure that security vulnerabilities are minimized.
- *Safe Emailing:* Email is an essential communication tool, but it also poses some risks, such as phishing scams, man-in-the-middle scams, malware, denial of access and identity theft. There is a need to be cautious of suspicious emails. Be wary of emails that ask for personal or sensitive information, contain suspicious links or attachments, or come from unknown senders. Do not click on links or download PDF attachments unless you are sure they are safe. Sweep through and verify emails monthly for hacks and attempts to illegally penetrate your digital space.
- *Safe Social Media Use and Interaction:* Social media platforms are powerful tools for activists, journalists, and civil society organizations (CSOs) in Kenya to engage communities, amplify advocacy efforts, and expose human rights violations. However, these platforms also come with risks, including cyberattacks, surveillance, misinformation, and online harassment. This guide provides practical steps to ensure safe, responsible, and effective social media engagement.

3. Safe Social Media Use and Interaction:

What to Watch Out for in Kenya:

- **Phishing attacks** disguised as messages from banks, M-Pesa, or government agencies.
- Fake job offers or grants targeting journalists and CSO staff.
- **Scam links in WhatsApp and Facebook groups** offering financial aid, loans, or scholarships.
- **Hacked activist/journalist accounts** sending malicious links.Social engineering tactics designed to extract sensitive information.

What You Can Do:

- Use secure messaging apps like Signal or Telegram (Secret Chats feature) for sensitive discussions.
- Enable two-factor authentication (2FA) on all accounts to prevent hacking.
- **Verify links using tools like Google Safe Browsing before clicking.**
- **Do not share personal data (ID numbers, phone numbers, locations) publicly or with unverified contacts.**
- Report and block suspicious accounts on social media platforms.

4. Strengthen Privacy and Security Settings

What to Watch Out For:

- **Default social media settings** that expose personal and professional information.
- **Location tracking** revealing movements of activists, journalists, or CSO staff.
- **Metadata leaks** (e.g., EXIF data in images) that can expose a person's location.
- **Unauthorized access** to sensitive communications and documents.

What You Can Do:

⟶ **Review and adjust privacy settings on Facebook, Twitter (X), Instagram, and WhatsApp to restrict public access to posts and profiles.**

⟶ **Disable location tracking in posts and live streams unless necessary.**

- ⟶ **Secure email communications with ProtonMail or Tutanota (encrypted email providers).**
- ⟶ **Use a Virtual Private Network (VPN) like ProtonVPN or Mullvad for added online anonymity.**

5. Avoid Sharing Sensitive or Unverified Information

What to Watch Out For:

- ⟶ Misinformation and disinformation campaigns, especially during elections or protests.
- ⟶ Fake news websites impersonating legitimate media to spread propaganda.
- ⟶ Deepfake content used to discredit activists, journalists, and CSOs.
- ⟶ Government surveillance and cyber threats targeting human rights defenders.

What You Can Do:

- ⟶ Verify facts using PesaCheck, Africa Check, or the Media Council of Kenya before sharing.
- ⟶ Avoid sharing unverified, inflammatory, or sensitive information that could endanger individuals or organizations.
- ⟶ Use encrypted cloud storage (e.g., ProtonDrive, Tresorit) instead of sharing sensitive files via email or social media.
- ⟶ Train team members and communities on digital literacy and security best practices.
- ⟶ If dealing with high-risk content, consider secure publishing platforms like SecureDrop for whistleblowers.

6. Final Recommendations for Activists, Journalists, and CSOs in Kenya:

- Regularly update passwords and use a password manager like Bitwarden.
- Use end-to-end encrypted communication tools like Jitsi Meet for secure online meetings.
- Be aware of digital surveillance and avoid discussing sensitive topics on unencrypted platforms.
- Attend cybersecurity and digital safety training to stay updated on emerging threats.

⟶ **Secure email communications with ProtonMail or Tutanota (encrypted email providers).**

⟶ **Use a Virtual Private Network (VPN) like ProtonVPN or Mullvad for added online anonymity.**

7. Improving and ensuring a CSOs digital security and safety

CSOs digital security and safety are crucial to protect sensitive data and prevent attacks. CSOs can take several measures to improve and ensure their digital security and safety. Some holistic measures can include;

1. *Design and apply online communication policies for staff and organisations:* CSOs should develop clear policies outlining the acceptable and secure use of digital platforms, ensuring alignment with organizational values, legal requirements, and security best practices.
2. *Key Elements of a Digital Communication Policy:*
    - ⟶ Acceptable Use Guidelines: Define how staff can use email, messaging apps, and social media for official communication.
    - ⟶ Secure Social Media Practices: Specify how the organization manages its official accounts, including password security, authorized users, and crisis response measures.
    - ⟶ Digital Identity Protection: Establish rules on how employees handle personal vs. organizational accounts to avoid impersonation risks.
    - ⟶ Incident Reporting Procedures: Outline steps to report cyber threats, phishing attempts, and data breaches.
3. *Policy Frameworks to Include:*
    - Data Protection Policies: Ensure compliance with Kenya's Data Protection Act, 2019, covering the collection, storage, and sharing of personal data.
    - Incident Response Plans: Define who does what in case of hacking, data leaks, or cyberattacks to minimize damage and restore operations quickly.
    - Secure Digital Engagement Policies: Establish rules for interacting with external partners, donors, and media through digital channels.

4. Provide training and support for staff:

- Provide training and support to staff to ensure that they understand policies, guidelines, opportunities and threats associated with online engagements. This could include training sessions, workshops, or facilitating the access to and use of online resources for knowledge acquisition and skills upgrading.

8. Key Training Areas for CSO Staff:

⟶ Understanding Digital Security Policies: Ensure staff are familiar with organizational policies on safe online communication, social media use, and data protection.

⟶ Cyber Threat Awareness: Train staff to identify phishing attacks, malware, hacking attempts, and online misinformation campaigns.

⟶ Use of Secure Digital Tools: Provide hands-on training on encrypted communication (e.g., Signal, ProtonMail), secure file storage (e.g., Tresorit, CryptPad), and safe browsing (e.g., VPNs, Tor Browser).

⟶ Crisis Response Protocols: Teach staff how to respond to hacking incidents, data breaches, or online threats and whom to report to.

9. Psychological Safety: Supporting Staff Facing Online Harassment

- Many activists, journalists, and CSO staff in Kenya face online harassment, doxxing, and targeted cyberattacks. Organizations must provide mental health and legal support to affected individuals.

What CSOs Can Do:

- Develop Response Protocols for handling cyberbullying, hate speech, and doxxing incidents.
- Provide Access to Mental Health Support (e.g., counseling, peer support groups) for staff experiencing online abuse.
- Offer Legal Assistance to help staff report threats, seek legal redress, and document digital harassment.
- Encourage Safe Online Behavior, including limiting personal information sharing and strengthening account security.

- Long-Term Resilience Building: Embedding Digital Security into Organizational Culture
- To sustain digital safety, CSOs must integrate cybersecurity into their long-term planning and daily operations.

Steps to Build Long-Term Digital Resilience:

⟶ Regular Security Audits: Conduct periodic digital risk assessments to identify vulnerabilities and update security measures.

⟶ Institutionalize Digital Security Roles: Assign digital security champions within the organization to monitor threats and coordinate training.

⟶ Ongoing Training: Provide continuous learning opportunities through workshops, online courses, and peer-to-peer learning.

⟶ Foster a Culture of Security Awareness: Encourage staff and partners to proactively engage in cybersecurity best practices and report threats immediately.

Session 2: **Criminalization of Online Speech**

Facilitator's notes.

- Describe online speech and criminalization of the same
- Provide scenarios on criminalization of online speech
- Provide case studies on denial on freedom of speech either online or otherwise.

1. Overview of Online Speech Restrictions in Kenya

Kenya's legal framework contains provisions that restrict online freedom of speech and expression, primarily under the Computer Misuse and Cybercrimes Act, 2018 (commonly referred to as the Cybercrimes Act discussed deeply in the next module)-. While this law was designed to address online abuse, it has been criticized for enabling government-led censorship and infringing on human rights.

2. Highlights and Examples

- Criminalize false publication and content intended to incite panic, chaos, or violence, or that could harm reputations. Offenders face imprisonment of up to 10 years

- **Case Examples:**
  - → **2020:** Blogger Cyprian Nyakundi was charged under Section 23 for posts on Twitter.
  - → **2021:** Blogger Edgar Obare faced similar charges for an exposé on social media.
  - → **2024:** Political activist David Morara Kebaso was charged under Section 27 for critical content posted on X (formerly Twitter).
  - → **In December 2024** Online activists were abductedincluding; Steve Kavingo Mbisi, Billy Wanyiri Mwangi, Peter Muteti, Bernard Kavuli, Naomi aka @Jabertotoo, Gideon Kibet aka Kibet Bull, Rony Kiplang'at
  - → **During the COVID-19 pandemic,** several bloggers and social media users were arrested for allegedly spreading false information online on the status of the pandemic.

3. Broader Implications for CSOs and Human Rights

- **Overbroad Definitions:** Vague terms in the Cybercrimes Act allows discretionary enforcement by State agencies, increasing the risks of censorship and rights violations.
- **Focus of Cybercrime Laws:** Cybercrime legislation should target cyber-dependent crimes like hacking and ransomware rather than broadly criminalizing online expression.
- **May 2021:** Section 66 of the Penal Code, barring false information publication, was invalidated for violating freedom of expression
- **March 2024:** The High Court struck down Section 77 of the Penal Code, which criminalized subversion, as unconstitutional. The court stated that the provision served no legitimate aim and was not strictly necessary in an open and democratic state. Consequently, the court declared sections 77 (1) and (3)(a), (b), (c), (d), (e), (f), and (g) of the Penal Code, Cap 63, unconstitutional.[1]

Session 3: **Challenges to Online Freedom of Expression**

Facilitator's notes.

- Discuss online freedom of expression
- With examples, show case challenges facing online freedom of expression.
- Show case using digital platforms of cases facing HRDs

1. Attacks on Journalists and Human Rights Defenders

- CSOs have documented increasing arrests, abductions, and physical attacks on journalists and activists using online platforms to express dissent.

Notable Cases:

- **Daniel Muthiani** (Sniper), a political blogger, was abducted and killed in 2023.
- Several journalists were assaulted during protests against the Finance Bill 2024. A good example is the case of Anti-IMF loan crusader Mutemi Kiama.

2. Internet Shutdowns and Censorship

- **2023:** Kenya experienced its first internet shutdown during national exams, with further disruptions noted during anti-government protests in 2024.
- Internet controls violate constitutional rights and hinder e-commerce, emergency services, and public discourse.

3. Economic Barriers

- **Digital Tax:** The 2023 Finance Act introduced a 15% tax on digital creators, criticized for stifling freedom of artistic expression.
- **KFCB Regulations:** The Kenya Film Classification Board mandates YouTube content creators to seek classification and licensing, posing economic and bureaucratic barriers.

4. Disinformation and Misinformation

- **Gendered Disinformation:**
  - ⟶ Women leaders face targeted online abuse, often using deepfake technology and TFGBV.
  - ⟶ **Example:** Martha Karua was targeted with disinformation during the 2022 elections.
- **Deepfakes and Manipulated Content:**
  - ⟶ AI-generated content has been used to spread false narratives, such as linking protests to controversial agendas.
- **Information Vacuums:**
  - ⟶ Internet shutdowns exacerbate the spread of disinformation by creating gaps in reliable information.

Session 4: **Key Recommendations for CSOs and case studies**

1. **Advocate for Reforms:** Engage in policy dialogue to narrow overly broad provisions in the Cybercrimes Act.
2. **Strengthen Digital Literacy:** Equip communities with tools to identify and counter misinformation and disinformation.
3. **Promote Legal Awareness:** Educate citizens about their rights under the constitution and international law.
4. **Support Journalists and Activists:** Establish rapid response mechanisms for victims of harassment or attacks.
5. **Enhance cyber security measures:** Establish institution policies and guidelines..
6. **Monitor and Document Violations:** Regularly report instances of censorship, internet shutdowns, and attacks to ensure accountability.
7. **Engagement with private sector actors:** on their role in ensuring online safety and/or implications in facilitating state surveillance/ violation of privacy rights

Case scenarios for discussion

- *During the #RejectFinanceBill2024 protests, Safaricom, Kenya's dominant telecommunications provider, was blamed for sharing data with law enforcement agencies to facilitate surveillance and potential abduction of protestors.*
- *A recent study[1] on the use of surveillance and counterterrorism measures found that Kenya has in place elaborate measures, infrastructure and mechanisms to facilitate communication interception and surveillance that have a significant impact on civic space. The study notes the role of enablers in this surveillance, for example the implementation of mass data collection programmes such as the National Integrated Identity Management System (Maisha Namba digital ID programme), mandatory SIM card registration, national CCTV systems and other social media monitoring measures.*

https://ir-library.ku.ac.ke/items/d9eb66e4-bb30-4a8f-9ec8-f4b75366d788

Case scenarios for discussion

- *These enablers, along with broad provisions allowing surveillance by government in laws such as the Prevention of Terrorism Act and the National Intelligence Service Act, combined with weak oversight of state surveillance practices, have allowed unchecked surveillance by agencies with little accountability. There are also documented instances of the use of such surveillance to target human rights defenders.*

Module evaluation quiz

1. What is digital safety?
2. How does digital safety differ from cyber-security?
3. What are the main threats to digital safety?
4. Why is online privacy important?
5. What are the potential consequences of poor digital safety practices?
6. Discuss how CSOs can address personal and organizational data safety and security?
7. What mechanism can be put in place to ensure fair and justice in Criminalization of Online Speech?
8. What challenges do HRDs/CSOs face on digital safety and security?

MODULE 3: **EMERGING TRENDS IN DIGITAL GOVERNANCE ADVOCACY**

Session Objectives

By the end of this session, participants will:

- *Understand the current emerging trends and there implication to organization operation and advocacy*
- *Understand methodologies and ways of adopting to the current emerging trends*
- *Understand the implications and challenges faced for failure to adopt to the emerging trends*

Session Plan

Introduction (15 minutes)

Icebreaker Activity: *Ask participants to reflect on any changes that have occurred in the recent past regarding digital advocacy*

Define emerging trends in digital governance:

- *Explain that emerging trends in digital governance are the latest ways that governments use technology to improve their services, increase transparency, and empower citizens*

Facilitator's notes.

Session 1: Introduction to emerging trends in digital governance (15 minutes)

Facilitator Key Points:

- Brief on emerging trends in digital governance
- Examples of emerging trends
- Impact of emerging trends

Discussion Question:

- What are the challenges or benefits brought about by emerging trends in digital governance?

Activity:

- Put participants into groups and ask them to identify emerging trends that are affecting CSOs and the mitigating measures they have adopted

Session 2. The General Data Protection Regulation (GDPR) (15 minutes)

Facilitator Key Points:

- Give an overview of the GDPR
- Discuss the rights offered by GDPR
- Discuss data protection principles as per the protection laws
- Explain essence of legal ways of processing personal data
- Consent

Discussion Question:

- How do CSOs ensure adoption of effective data protection methods?

Activity:

- In pairs discuss how your CSOs have ensured data protection for its clients.

Session 3. Gender Perspective (15 minutes)

Facilitator Key Points:

- Discuss Technology-Facilitated Gender-Based Violence (TFGBV)
- Give examples of TFGBV
- Give recommendation to CSOs on TFGBV

Discussion Question:

- What role can CSOs play in addressing cases of TFGBV?

Activity:

- In groups the participants to discuss real scenarios they have experienced in relation to TFGBV.

Session 3. Gender Perspective (15 minutes)

Facilitator Key Points:

- Emphasize the importance of the adoption of emerging trends.
- Emphasize the importance of advocacy against TFGBV.

Session 3. Gender Perspective (15 minutes)

Call to Action:

- Participants identify one action they will take in the next month to advocate for actions against emerging trends affecting the society.
- Give recommendation to CSOs on TFGBV

Materials Needed:

- Presentation slides summarizing key points.
- Case studies or examples.

Additional Notes for Facilitator:

- Be mindful of participant knowledge levels; simplify jargon where necessary.
- Foster an inclusive and interactive environment to encourage participation.
- Provide handouts

Session 1: **Introduction to Emerging Trends and opportunities for CSOs**

Facilitator's notes.

- Discuss the emerging trends providing examples
- Enable participants to clearly understand the implication of the trends
- Discuss potential challenges and mitigation measures that they can use

Introduction

CSOs are the main point of contact between government and people, businesses and organisations. The qualities of community services have a profound impact on people's lives and are often pivotal in ensuring citizens have access to opportunities and realize their full potential.

The digital divide has had real effects on rural versus urban CSOs from the aspects of affordability, accessibility, e-literacy, et cetera. The research revealed that technology, which tends to reproduce inequalities experienced on the ground, (gender, and rural/urban disparities), serves to transpose the same issues plaguing the sector to the digital space. The research showed that the question of who has access to technological resources is tied to overall resource constraints which are more deeply felt by smaller NGOs and more so CBOs in Kenya.

1. Current Emerging Trends

- **Future-oriented and co-created Community services:** CSOs are working with users and stakeholders to co-design solutions and anticipate future needs, creating public services that are flexible and responsive to change, and are therefore more resilient and sustainable in the long term.
- **Digital and innovative foundations for efficient services:** CSOs are investing in scalable digital infrastructure, experimenting with emergent technologies (such as automation, AI and modular code), and expanding innovative and digital skills to make community services more accessible and efficient.
- **Personalized and proactive services for accessibility and inclusion:** CSOs are making services more personalized and proactive to better meet people's needs and expectations, reduce psychological costs and administrative frictions, ensuring they are more accessible, inclusive and empowering, especially for persons and groups in vulnerable and disadvantaged circumstances.

- **Data-powered public services for better decision-making:** CSOs are drawing on traditional and non-traditional data sources to guide public service design and execution. They are increasingly using experimentation to navigate highly complex and unpredictable environments.
- **Public services as opportunities for public participation:** · CSOs are seeing services as an opportunity to engage citizens in exercising their rights, building trust, and holding government accountable for upholding democratic values such as openness and inclusion.

Session 2: The General Data Protection Regulation (GDPR)

Facilitator's notes.

- Clearly explain the role played by GDPR and the implications it brings
- Use clear examples on failures and powers of GDPR
- Discuss CSOs need to implement data protection and consent rules

1. Introduction

The General Data Protection Regulation (GDPR) is significant in data protection because it establishes a comprehensive and robust legal framework for how organizations can collect, store, and process personal data of individuals within the European Union, giving individuals greater control over their personal information and holding companies accountable for how they handle that data, setting a global standard for privacy practices.

The General Data Protection Regulation (GDPR) is the data protection law in the European Union (EU), while the Data Protection Act (DPA) is the data protection law in Kenya; they list the rights:

2. Rights of individuals

- The need for an individual's clear consent to the processing of his or her personal data
- Easier access for the data subject to his or her personal data
- The right to rectification, to erasure and 'to be forgotten'
- The right to data portability from one service provider to another.

3. Data protection principles

- **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
- **Purpose limitation** — one must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization** — one should collect and process only as much data as absolutely necessary for the purposes specified.
- **Accuracy** — one must keep personal data accurate and up to date.

- **Storage limitation** — one may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- **Accountability** — the data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

3. Data processing

GDPR lists the instances in which it's legal to process person data.

- The data subject gave specific, unambiguous consent to process the data. (e.g. They've opted in to your marketing email list.)
- Processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party. (E.g. need to do a background check before leasing property to a prospective tenant.)
- You need to process it to comply with a legal obligation of yours. (E.g. receive an order from the court in your jurisdiction.)
- One needs to process the data to save somebody's life. (E.g. know when this one applies.)
- Processing is necessary to perform a task in the public interest or to carry out some official function. (E.g. a private garbage collection company.)
- Have a legitimate interest to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data. (It's difficult to give an example here because there are a variety of factors you'll need to consider for your case.
- Once determined the lawful basis for data processing, one need to document this basis and notify the data subject (transparency!).

4. Consent

There are strict new rules about what constitutes consent from a data subject to process their information.

- Consent must be "freely given, specific, informed and unambiguous."
- Requests for consent must be "clearly distinguishable from the other matters" and presented in "clear and plain language."
- Data subjects can withdraw previously given consent whenever they want, and you have to honor their decision. You can't simply change the legal basis of the processing to one of the other justifications.

- Children under 13 can only give consent with permission from their parent.
- You need to keep documentary evidence of consent.

Session 3: **Emerging Citizen Participation and E-Governance in Kenya**

Kenya has made significant strides in digital governance and civic engagement through e-governance platforms, social media activism, and CSO-led digital advocacy initiatives. This session contextualizes these developments, highlighting tools, innovations, challenges, and opportunities within Kenya's governance landscape.

1. Digital Tools for Civic Engagement in Kenya

Kenya's digital transformation has facilitated greater public participation in governance. Key tools include:

- **E-Citizen Platform:** The government's one-stop portal for accessing services like business registration, tax filing (iTax), land records, and passport applications. This enhances transparency and reduces bureaucratic inefficiencies.
- **Huduma Namba, Maisha Namba & Huduma Centers:** A biometric digital identity system aimed at streamlining service delivery, though concerns about data privacy and exclusion persist.
- **Online Petitions:** Platforms such as Parliament's e-petition system allow citizens to voice concerns and demand policy changes.
- **Social Media Advocacy:** Twitter (X), Facebook, and WhatsApp have become powerful tools for mobilization, as seen in movements like #LowerFoodPrices, #RejectFinanceBill, #LindaKatiba, and #JusticeForKianjokomaBrothers.

2. CSO Innovations in Digital Advocacy

Civil society organizations (CSOs) in Kenya use digital tools to promote good governance, civic rights, and social accountability. Notable innovations include:

- **Mzalendo Trust's Hansard democracy tool:** A parliamentary watchdog platform that tracks MPs' contributions, bills, and policy positions, enhancing legislative transparency.
- **Ushahidi:** A Kenyan-born crowdsourcing tool used for election monitoring, human rights reporting, and crisis response.

- **Okoa Uchumi:** A citizen-led campaign coalition advocating for responsible public debt management and accountability in government spending.
- **SautiYaBajeti** is an AI-Powered WhatsApp Chatbot designed and developed by ColMusk Ltd for the Institute of Public Finance. The Platform goal is to provide factual PFM Information that educate citizens on how taxes are collected and spent for service delivery and to promote the principles of Public Finance which include Transparency, Accountability, participation, Efficiency, effectiveness and Equity
- **Digital Whistleblowing Platforms:** Initiatives like Sema Kenya provide anonymous reporting channels for corruption and rights violations.

3. Challenges and Opportunities in E-Governance in Kenya

Challenges

- **Digital Divide:** Many rural and marginalized communities lack internet access, limiting their participation in e-services initiatives.
- **Cybersecurity & Data Privacy Concerns:** Cases of government surveillance, data breaches, and hacking incidents raise fears about digital rights.
- **Misinformation & Disinformation:** Fake news and propaganda, especially during elections, undermine trust in digital advocacy efforts.
- **Government Resistance & Censorship:** Crackdowns on online activists, restrictive cyber laws (e.g., the Computer Misuse and Cybercrimes Act), and internet shutdowns in some regions threaten digital civic space.
- **Low Digital Literacy:** While Kenya has a growing tech-savvy population, a significant portion of citizens, especially the elderly and those in rural areas, struggle with digital platforms.

Opportunities

- **Increased Government Transparency:** Platforms like IFMIS (Integrated Financial Management Information System) and Open Data Kenya promote fiscal accountability.
- **Youth-Led Digital Activism:** Kenya has a vibrant youth-driven civic space leveraging social media for political engagement and human rights advocacy.

- **Cost-Effective Public Participation:** Digital platforms reduce logistical barriers, allowing more citizens to engage in governance processes without physical meetings.
- **Emerging Technologies:** AI, blockchain, and data analytics can improve service delivery, election integrity, and policy formulation.

Session 4: **Technology-Facilitated Gender-Based Violence (TFGBV)**

Facilitator's notes.

- Explain the concepts and technologies TFGBV
- Explain key terminologies in the related to TFGBV
- Trends in Kenya context in terms of TFGBV

Refers to gender-based violence committed, abetted, or aggravated through Information and Communication Technologies (ICTs), including:

- Mobile phones
- Internet
- Social media platforms
- Email

Common examples of TFGBV

- Cyberstalking
- Online harassment
- Doxxing (publishing private information with malicious intent)
- Email

Continuum of Gender-Based Violence:

- TFGBV stems from the same systemic gender inequalities that drive other forms of gender-based violence offline
- Online and offline violence are interconnected; harm in one domain often affects the other.
- Women and gender-diverse individuals experience violence that cuts across their personal, professional, and public lives, with significant social, economic, and psychological impacts.

1. TFGBV in the Kenyan Context:

- Online violence disproportionately targets women and gender-diverse people, particularly those in public life, activism, and leadership roles.
- Women politicians, activists, and journalists face heightened vulnerability to online abuse, especially during key political events like elections.

2. Key Findings from the 2022 Kenyan General Elections (Byte Bullies Report):

- 55% of women candidates reported experiencing online violence, including:
    - Sexual violence
    - Hate speech
    - Trolling
    - Disinformation campaigns
- Comparatively, 35.4% of male candidates reported similar experiences.
- Women were often targeted with explicit threats to their safety and dignity, aimed at discouraging their participation in politics and public discourse.
- Social media platforms, particularly Twitter, Facebook, and WhatsApp, were primary channels for online abuse.

3. Broader Trends and Impacts in Kenya:

Youth and Adolescent Girls:

- Young women and adolescent girls are particularly vulnerable to cyberbullying, revenge porn, and unsolicited sexual advances on social media platforms.
- Online abuse discourages many girls and young women from engaging fully in digital spaces, limiting access to education, networking, and career opportunities.

Women Human Rights Defenders (WHRDs)

- WHRDs in Kenya face relentless online harassment, including threats to their lives and families, which undermine their advocacy work and well-being.

Cultural Factors

- WHRDs in Kenya face relentless online harassment, including threats to their lives and families, which undermine their advocacy work and well-being.

Cultural Factors

- Cultural norms and stigma around women's use of digital platforms exacerbate the effects of TFGBV, often leading to victim-blaming and silencing.

4. Recommendations for CSOs in Kenya

Awareness and Advocacy:

- Conduct awareness campaigns to highlight the prevalence and impact of TFGBV in Kenya.
- Advocate for stronger policies and legislation to address TFGBV, including enforcement of the Computer Misuse and Cybercrimes Act, 2018 in addressing the actual challenges rather as a tool for intimidation by the state.

Support for Survivors:

- Establish and promote reporting mechanisms for survivors of TFGBV.
- Provide psychosocial, legal support and digital safety training to victims.

Digital Literacy and Safety Training:

- Equip women and girls with skills to navigate digital platforms safely, including by understanding privacy settings and reporting abuse.

Capacity Building for CSOs:

- Train CSOs on how to support survivors of TFGBV, advocate for systemic change, and engage technology companies to address online abuse.

Collaborations with Tech Companies:

- Partner with social media platforms to improve the reporting and removal of harmful content targeting women.

Monitoring and Research:

- Track incidents of TFGBV in Kenya to identify trends, document cases, and inform policy advocacy.

Partnerships:

- Partner with academia, other civil society organizations, private sector players, and tech experts to enhance digital security, compliance, and overall impact.

Module evaluation quiz

1. **Identify and explain emerging trends that have:**
    - Positively enhanced CSOs/HRD work?
    - Negatively impacted the community and CSOs/HRD work?
2. **Discuss ways of ensuring data protection principles are followed?**
3. **How has technology affected GBV with the community? – give examples**
4. **Explain the need for CSOs to ensure Consent when engaging community members? – Which areas need consent?**
5. **Explain ways that CSOs/HRD can use to reduce the impact of emerging technologies?**

ANNEX

How to facilitate:

A workshop for participants from a diverse CSO cohort and community leaders need extensive preparation, and the facilitator should ensure that the following is done well in advance:

1. Preparation

Before each day's training, facilitates must review the topics to be covered for that day, by carefully reading the relevant material. This will enhance understanding of the concepts and points raised on each slide and its correlation to the accompanying text. Depending on the skills of the trainer, and their background, they may wish to include examples or case studies to bring further depth and clarity to the topic being presented. The workshop trainers or facilitators should be familiar with experiential and participatory forms of learning. They should have the ability to ask exploratory/probing open-ended questions and should make it a point to involve all the participants. The facilitators should be technically competent to answer various intervention-related questions. The topics included may be adapted to suit local needs and priorities. As there are many hands-on sessions, the facilitators would need to be familiar with all those processes so that they can demonstrate as well as guide the participants correctly in the field. It will be important at all stages for participants to correlate their classroom teachings with field-level learning and vice versa.

1. Preparation

Before each day's training, facilitates must review the topics to be covered for that day, by carefully reading the relevant material. This will enhance understanding of the concepts and points raised on each slide and its correlation to the accompanying text. Depending on the skills of the trainer, and their background, they may wish to include examples or case studies to bring further depth and clarity to the topic being presented. The workshop trainers or facilitators should be familiar with experiential and participatory forms of learning. They should have the ability to ask exploratory/probing open-ended questions and should make it a point to involve all the participants. The facilitators should be technically competent to answer various intervention-related questions. The topics included may be adapted to suit local needs and priorities. As there are many hands-on sessions, the facilitators would need to be familiar with all those processes so that they can demonstrate as well as guide the participants correctly in the field. It will be important at all stages for participants to correlate their classroom teachings with field-level learning and vice versa.

2. Practical tips for facilitators

The following are general tips for the design and facilitation of digital governance training sessions or of meetings to plan or evaluate digital governance initiatives.

3. Before the workshop

a) Define the objectives of the session with leaders or representatives of the organization (or organizations) that will participate in it. This is especially important when the organization has requested that the session take place. A facilitator should be clear about how these fits within the organization's overall structure and programmatic activities. They should try to ensure that it is consistent with the organization's stated mission and objectives.

b) Ensure that the people with whom you are coordinating the event have the backing of the organization and its membership to avoid such problems as manipulation, poor attendance, or lack of credibility.

c) Arrange for the facilitation to be done by a team of facilitators.

d) Make sure that whatever technical equipment is needed for the event is available and functioning properly.

e) Gauge the participants' true level of commitment to and involvement in the group's advocacy initiative.

f) Obtain as much information as possible about the organization: its history, current objectives, structure, activities, and internal dynamics. Information can be gathered through interviews, informal conversations, documents, and minutes.

g) Bear in mind the characteristics of the people who are going to participate: their ages, ethnicity, race, gender, knowledge, and experience related to the issue, level of formal schooling, responsibilities within the organization, and level of political awareness.

h) Deal with logistical aspects of the event: the schedule, time allotted for lunch, where and how to hang up newsprint, the size of the space, the noise and temperature levels, the availability of break-out space for small group work, and so on.

i) Ensure that the specific objectives of the session contribute to the organization's overall objectives.

j) Ensure the logical sequencing of the content to be presented and select training techniques that will fulfill the specific learning objectives of the event.

k) Be familiar with all the materials that will be used during the session, ensuring their appropriateness for the group and issue under discussion.

l) Maintain good communication and coordination within the team of facilitators, agreeing in advance on each person's role and responsibilities.

During the workshop

a) Make good use of the physical space available.

b) Allow participants the opportunity to express their hopes for the session so that they feel as though their opinions are considered from the beginning. Agree upon a schedule and some basic ground rules—the need to be punctual, to listen to other people's opinions, to be brief, to avoid excessive repetition, to respect others, and so forth. In other words, clarify expectations and the "rules of the game."

c) Create work groups of participants that will have specific responsibilities and tasks during the event to assist the team of facilitators.

d) Before presenting content, agree on how to handle the taking of minutes. It is important to be clear about the type of minutes that are needed, who will prepare them, with what inputs, and by what date. Explain that the minutes will serve as a report to be given to the team of facilitators. They should record the interests and needs expressed by the participants, analyze any difficulties that arose, and note which techniques were most helpful and appropriate and which achieved the best results.

e) Maintain fluid communication among members of the facilitation team and model a participatory and democratic work style characterized by mutual respect.

f) Use a variety of presentation techniques (cards, newsprint, transparencies, the blackboard, etc.) to convey information and help participants follow a sequence of topics.

g) At the end of each step in the methodology, summarize it and highlight the main points of the discussion to clearly mark the end of one step and the beginning of another.

h) Make visual contact with all the people in the group of participants. Do not direct your attention at only one person or one subgroup of people. When participants speak, they should speak to the entire group and not just to the facilitator.

i) Be creative and use appropriate new techniques to communicate with the participants. Know when to switch to a different technique (for example, after a long plenary, a serious discussion, a sad or emotional moment, or a break or meal). Varying the techniques helps keep participants energized and alert. Do not, however, go overboard and allow the techniques to distract from the content being presented or to curtail debate among the group participants on contentious issues.

j) Recognize and deal with the conflicts and disagreements that arise during the session. It is counterproductive to continue to present content when it is obvious that conflict is brewing or that feelings are not being expressed.

k) Address comments or statements made by any participant that are racist, sexist, homophobic, or otherwise offensive, by questioning underlying behaviors or attitudes instead of attacking the person. The facilitator should make every effort to create a safe and congenial environment in which all participants feel respected.

l) Maintain a high level of motivation within the group throughout the session. It is important to create a positive and friendly environment by using techniques that allow the participants to get acquainted with one another.

m) Do not be afraid to make mistakes! Group facilitation is not an exact science, but rather a trial-and-error exercise. Popular educators often say that "a person who never makes mistake.

CONTACTS

ACK Garden House, Second Floor
Wing A | First Ngong Avenue
P.O Box 21765 - 00505 Nairobi
Phone: +254 (0)726464063
Email: info@mzalendo.com
www.mzalendo.com

@MzalendoWatch

RECIPE
Recentering The Civic Internet Through Partner Engagement

Co-funded by the European Union

OXFAM

MZALENDO