PRINCIPLES AND GUIDELINES FOR THE USE OF DIGITAL AND SOCIAL MEDIA IN ELECTIONS IN AFRICA

ASSOCIATION OF AFRICAN ELECTION AUTHORITIES

ASSOCIATION DES AUTORITES ELECTORALES AFRICAINES

FOREWORD

In an era where the role of Electoral Management Bodies (EMBs) in Africa is becoming increasingly vital, the Principles and Guidelines For The Use Of Digital and Social Media in Elections in Africa, spearheaded by the Electoral Commission of South Africa, could not have arrived at a better time. These Guidelines are an invaluable resource, empowering EMBs to share their narratives, connect with stakeholders and safeguard their integrity and credibility.

I emphasize that this document could not have come at a better time; especially now when, EMBs worldwide, are witnessing and experiencing real threats to their very existence.

One of the most pressing challenges for EMB's is the proliferation of fake news and disinformation campaigns on social media platforms. These falsehoods, often designed to manipulate public opinion, can significantly impact electoral outcomes and even lead to social unrest.

Regrettably, the power of social media is like a two-edged sword. While it can be a force for good, it also poses significant risks. Over the last few years we have witnessed instances worldwide where social media has been exploited to undermine EMBs' work, as seen in the events surrounding the January 6th, 2021 insurrection in the USA and post-election events in Germany, Brazil, and the Philippines.

These Guidelines emphasize the importance of harnessing social media to bolster EMBs' standing and foster confidence and trust in their endeavors while engaging their stakeholders effectively. The Guidelines also underscore the dangers of social media misuse and call for responsible journalism and accountability among platform owners and users.

The document encourages African EMBs to adopt a clear and comprehensive plan for the responsible use of social media during electoral periods.

Furthermore, it highlights the vital roles that governments and regulatory bodies can play in safeguarding EMBs and elections in Africa. It empowers them to support EMBs and electoral processes and work to protect and preserve the peace and security of their respective nations.

As we embark on this journey towards harnessing the power of social media for democratic progress, let us remain steadfast in our commitment to the principles of transparency, integrity, and accountability.

We are confident that it will serve as a valuable resource for election stakeholders across the continent.

Mrs. Jean Mensa

President of the AAEA Executive Committee
Chairperson, Ghana Electoral Commission

ACRONYMS

AAEA	Association of African Electoral Authorities
ACHPR	African Charter on Human and Peoples' Rights
AI	Artificial Intelligence
ARF	African Renaissance Fund
AU	African Union
AUC	African Union Commission
CSOs	Civil Society Organisations
DIRCO	Department of International Relations and Cooperation
EMBs	Election Management Bodies
RECs	Regional Economic Communities
UNDP	United Nations Development Programme
UNGP	United Nations' Guiding Principles on Business and Human Rights

PART I: INTRODUCTION

1. These Principles and Guidelines for the Use of Digital and Social Media in Elections in Africa are provided to enhance the capacities of Election Management Bodies (EMBs) and other relevant electoral stakeholders to harness the advantages of social media and tackle the adverse effects of new and emerging digital technologies.

2. The Principles and Guidelines are a human rights-inspired non-binding and persuasive instrument that is meant to address the existing normative gap regarding the use and implications of the digital and social media in elections on the continent.

3. The development of these Principles and Guidelines was inspired by the recommendations of the first-ever Continental Conference for Election Management Bodies that was held in Cape Town in March 2020, South Africa. It was themed **"Safeguarding Electoral Integrity in the Digital Age: Strategies for Combatting Digital Disinformation"**. It was jointly organised by the Electoral Commission of South Africa, the African Union Commission (AUC) and the United Nations Development Programme (UNDP).

4. The Cape Town conference noted that, although disinformation and misinformation have existed in offline media like print or analogue broadcast, the digital and social media have amplified them, shifting the speed at which information is transmitted, how content is structured, and how people consume and relate to content.

5. The conference further noted that disinformation and other potential forms of digital harm to human rights have affected the EMBs' constitutional mandates to organise elections and referenda, and have undermined efforts to promote peaceful and democratic elections.

6. In November 2022, the General Assembly of the Association of African Electoral Authorities (AAEA) held in Maputo, Mozambique, and coordinated by the AUC, endorsed the plan to develop these Principles and Guidelines.

7. The General Assembly mandated the Electoral Commission of South Africa to lead the initiative, working closely with the AUC and AAEA.

8. In undertaking this mandate, the Electoral Commission was financially supported by the South African Department of International Relations and Cooperation (DIRCO) through the African Renaissance Fund (ARF).

Objectives

9. The objectives of these Principles and Guidelines are to do the following:

(a) Contribute to the integrity of electoral processes in Africa by providing guidance to EMBs and other relevant electoral stakeholders for identifying opportunities to promote access to electoral information and address challenges in dealing with harm to digital human rights, in particular potentially harmful digital contents and business practices that threaten the integrity of electoral processes.

(b) Foster policy development on digital and social media in elections by EMBs, Regional Economic Communities (RECs) and member states.

(c) Serve as a resource for digital and social media (including digital messaging services) in their policies and processes dealing with online content relevant to elections in Africa.

(d) Inform regulatory processes under development or review for the digital and social media in the context of elections in a manner that is consistent with international human rights standards and the African Charter on Human and Peoples' Rights.

Key Normative Human Rights Frameworks

10. The key international and continental normative human rights frameworks relevant to the use of digital and social media use during the electoral cycle include:

- The 1948 Universal Declaration of Human Rights (UDHR)
- The 1961 International Covenant on Civil and Political Rights (ICCPR)
- The 1979 Convention on the Elimination of Discrimination Against Women (CEDAW)
- The 1981 African Charter on Human and Peoples' Rights (ACHPR)

- The 2002 Organisation of African Unity (OAU)/African Union (AU) Principles for Democratic Elections in Africa
- The 2007 African Charter on Democracy, Elections and Governance (ACDEG)
- The 2011 United Nations Guiding Principles on Business and Human Rights
- The 2014 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)
- The 2019 African Commission on Human Rights and Peoples' Rights Guidelines on Access to Information and Elections in Africa
- The 2019 Addis Ababa Declaration, World Press Freedom Day 2019, "Journalism and Elections in Times of Disinformation"
- The 2021 Windhoek +30 Declaration on Information as a Public Good, World Press Freedom Day, Namibia
- The 2022 ACHPR Resolution on the Protection of Women Against Digital Violence in Africa
- The 2023 African Commission of Human and Peoples' Rights Resolution on Business and Human Rights in Africa

PART II: PRELIMINARY PROVISIONS

2. DEFINITION OF KEY TERMS

For the purposes of consistency and clarity in this document, the following definitions are provided for the terms relevant to these Principles and Guidelines, based on scientific literature and international agreements.

2.1 Elections

2.1.1 Election Management Bodies

This refers to the body or bodies responsible for electoral management as defined by the legal framework of African Union member countries.

2.1.2 Relevant electoral stakeholders

This refers to the various categories of stakeholders in the electoral process to whom these Guidelines primarily apply, including EMB networks, political parties

and candidates, election observers and monitors, law enforcement agencies, campaign funders, whether public or private entities or persons, media regulatory bodies, media and online media platform providers, civil society organisations, professional organisations, religious bodies and other relevant state institutions, departments and private entities.

2.1.3 Electoral cycle[i]

This is the continuum of interrelated activities and processes that take place during the pre-election, election and post-election phases.

2.1.4 Electoral fraud

This refers to acts considered illegal interference with the electoral process (including manipulation of election results), and against the Constitution and national laws.

2.1.5 Electoral integrity

This refers to alignment of the electoral cycle with the democratic principles of universal suffrage and political equality as reflected in international norms, standards and agreements.[ii]

2.1.6 Electoral violence[iii]

This refers to any harm or threat of harm to any person or property involved in the election process. In the online context, it refers to the use of computer systems and digital services to intimidate, or to cause, facilitate or threaten violence against individuals or vulnerable groups, and harm electoral integrity.

2.2 Communications activities and institutions

2.2.1 Content curation[iv]

This refers to the underlying technologies and practices of the design and operation of digital and social media, which influence how they scope and order content, including the use of proprietary and often secret parameters to determine the reach, prominence, sharing and amplification of content.

2.2.2 Content moderation[v]

This refers to any form of enforcement or editorial action taken by a company with respect to a user's digital content or account, for instance, the removal of content, algorithmic down-ranking, setting limits on sharing, and the temporary or permanent suspension of accounts.

2.2.3 Digital intermediary (plural: digital intermediaries)

These are providers of network infrastructure that allow people and companies to build platforms or provide other services on the internet. This includes internet service (i.e. connectivity) providers, which host services such as cloud computing and web hosting, domain name registrars, online marketplaces, and app stores and artificial intelligence (AI) foundation models[vi].

2.2.4 Media technologies and institutions

Media refers to the various means of communication or tools used to reach mass audiences. In these guidelines:

2.2.4.1 The phrase "the media" refers to news institutions operating online and offline, where editors oversee the production of content.

2.2.4.2 The phrase "social media" refers to companies that provide digital tools for users to create and share content with each other, such as by means of video-sharing services or messaging services.

2.2.4.3 "Other digital media" refers to content producers active on their own digital platforms and infrastructure, as well as in the deployment of AI in communications.

2.2.4.4 The phrase "the digital and social media" points to the combined way in which operators of social media and other digital media impact on online content that is of interest to electoral integrity.

2.2.5 Media and information literacy, and digital literacy

Media and information literacy refers to the knowledge, attitudes and skills of people to engage critically and effectively with media technologies and institutions, and related content. In this context, digital literacy involves the specific competencies for using digital technologies. Both literacies are important for elections.

2.2.6 Paid-for-content and micro targeting

2.2.6.1 Paid-for content refers to content, whether it is explicitly so or not, which is designed to persuade and influence people. It may include advertising and sponsored content, including endorsements by social media "influencers" who may not disclose that they are receiving material benefit for particular messaging.

2.2.6.2 Micro targeting is a form of online targeted advertising that analyses personal data to identify the interests of a specific audience or individual to influence their actions. Micro targeting may be used to offer a personalised message or personalised content to an individual or targeted audience using an online service such as social media.[vii]

2.2.7 Recommender systems

A "recommender or ranking system" means an automated system used by an online platform to suggest specific content to recipients of the service, or to prioritise or deprioritise that content, as well as recommend individuals, groups and trends to follow.

2.3 Data

2.3.1 Algorithms

An algorithm is a set of rules used to solve a mathematical problem in a finite number of steps. In computing, algorithms are used to access and organise information taken from large data sets. The order or preferences embedded within the algorithm will determine how the information is ordered or presented.

2.3.2 Artificial Intelligence (AI)

An artificial intelligence system (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and can generate output such as predictions, recommendations or decisions that influence physical or virtual environments.[viii] AI technologies are shaped by developers, deployers, intermediaries and end-users of the applications, all with implications for voters.

2.3.3 Personal data

Personal data means any information relating to a natural person that can lead to the person's identification. The information may include a name, identification number and characteristics referring to the individual's physical, physiological, mental, economic or social identity.

2.3.4 Data abuse

2.3.4.1 Personal data broadcast

This is the passing of personal data (including individuals' online behaviour, their location in the real world and codes to identify them) to external entities by advertising technology companies. This exposes voters to profiling and manipulation.

2.3.4.2 Unauthorised personal data reuse

This is where personal data that was initially collected or generated for one specific purpose is processed within a company (or controlling undertaking) for other purposes without the permission of the person concerned or an alternative proof of legality or legitimacy.

2.3.5 Potential digital harm

This refers to harm to the integrity of elections and human rights during elections, the safety of citizens and electoral officials, as well as materials and processes that arise from digital technologies.

2.3.5.1 Misinformation

Misinformation is false, inaccurate or misleading information that is disseminated regardless of intent to cause harm, and that may cause harm with or without the disseminators' knowledge[ix]. Misinformation may not be illegal under international standards, unless it serves to harm human rights, including those essential to the integrity of elections.

2.3.5.2 Disinformation

This is all forms of false, inaccurate or misleading information designed, presented and promoted to intentionally cause public harm or for profit. This definition unites three critical criteria:

(a) deception
(b) potential for harm
(c) an intent to harm[x]

Disinformation may or may not be subject to restrictions under international standards.

2.3.5.3 Hate speech

This is any kind of communication in speech, writing or behaviour that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor. This is often rooted in, and also generates, intolerance or hatred, and in certain contexts can be demeaning or offensive, and incite violence.[xi]

2.3.6 Attacks on human rights

This refers to threats to the right to freedom of expression, safety, privacy, reputation and political participation, or any other human rights, including freedom of expression, which may be conducted through digital technologies.

2.4 Internet disruptions, telecommunications disruptions

These are disruptions to digital communications instigated by state or non-state actors that do not meet international standards of legality, proportionality and legitimate purpose for limiting freedom of expression and access to information. The interventions that follow are considered disruptions if they are non-compliant with international standards:

2.4.1 Distributed denial of service attacks (DDoS) and hacking, which are service interruptions achieved through criminal hacking or denial of access to online networks, resources and services.

2.4.2 Website blocking or content filtering, which refer to the practice of preventing users from accessing specific websites, types of content or keywords.

2.4.3 App blocking or the digital and social media shutdowns that occur when a particular platform or internet service is blocked, restricted or throttled.

2.4.4 Network throttling refers to the decision to slow down web speeds at the service provider level by making less bandwidth available for internet traffic. Slow web speeds are used to harm freedom of expression by frustrating users who may subsequently reduce the amount of time they spend online.

2.4.5 Mobile network shutdown is when mobile telecommunications services such as voice calls, SMS, mobile data connectivity and mobile money services are suspended.

2.4.6 Partial internet shutdowns occur when internet access is denied to a portion of society, usually delineated by geographical boundaries. This usually occurs at the level of the connectivity service providers.

2.4.7 Full internet shutdowns occur when an entire population is denied access to the internet for a time.

PART III: GENERAL PRINCIPLES

3. GENERAL OBLIGATIONS

3.1 Application and interpretation

3.1.1 All persons enjoy the same human rights online as they do offline, and the restriction of any right is only justifiable to the extent that it strictly complies with the three-part test established under international law: (i) it is prescribed in law; (ii) it serves a legitimate aim; and (iii) it is necessary and proportionate to achieve the stated aim in a democratic society. Restrictions that do not correspond to the test can be described as “arbitrary”.

3.1.2 Fundamental rights can be directly and indirectly enhanced by access to the internet, including access to digital and social media.

3.1.3 While states are the primary duty-bearers to ensure that human rights are respected, protected, promoted and fulfilled, all relevant electoral stakeholders have shared obligations towards the full and meaningful realisation of these rights as may be applicable with particular consideration due from private sector entities.

3.1.4 Relevant electoral stakeholders must take specific measures to address the needs of marginalised or vulnerable groups in a manner that guarantees the full enjoyment of fundamental rights on an equal basis with others, including in respect of access to digital and social media, the protection of safety online and the provision of media and information literacy.

3.1.5 The rights-based framework set out in this document should be read in line with the principle of complementarity, specifically as complementing and enhancing existing international, continental and domestic laws and regulations, encouraging the development and implementation of such laws and regulations where they are absent, and promoting a unified approach to avoid regulatory fragmentation.

3.1.6 This document should also be read and interpreted through a rights-based lens that is intended to foster the respect, protection, promotion and fulfilment of human rights for all, including the fundamental rights of human dignity, equality and universal adult suffrage.

3.1.7 Where a conflict arises between any domestic and international human rights law, the most favourable provision for the full exercise of the right in question shall prevail.

3.2 The right to equality and non-discrimination

3.2.1 All persons are equal before the law and are entitled to equal protection from the law.

3.2.2 All persons are entitled to the enjoyment of the full range of fundamental rights both online and offline under international human rights law without distinction, and any restriction should comply with the three-part test for a justifiable limitation.

3.3 Free, fair and credible elections

3.3.1 All citizens are guaranteed the right and opportunity, without discrimination, to participate in the conduct of public affairs either directly or through freely chosen representatives, to vote and be elected at genuine periodic elections with universal and equal suffrage held by secret ballot, guaranteeing the free expression of the will of the electors.

3.3.2 All reasonable measures must be taken to ensure that the democratic principles of transparency, accountability and the rule of law are implemented, both online and offline, to ensure electoral integrity and the conduct of free, fair and credible elections for all persons without discrimination.

3.3.3 Specific measures must be taken to ensure the safety of vulnerable, marginalised persons, including gender-specific concerns faced by female candidates and journalists engaged in the electoral process such as through sexual and gender-based violence, intimidation and harassment.

3.4 Freedom of opinion and expression

3.4.1 Freedom of opinion, including the right to form and change such opinion at any time and for whatever reason, is a fundamental and inalienable right and should not be subject to interference. Freedom of expression protects the right of individuals to share opinions.

3.4.2 The right to freedom of expression, both online and offline, includes the right to seek, receive and impart information and ideas regardless of the form of communication or medium, and digital and social media should be available to be used as a space for all persons to receive and impart information or ideas.

3.4.3 The right to express oneself, both online and offline, shall not be subject to arbitrary restrictions (meaning those that do not meet the three-part test for justifiable limitations as referred to in clause 3.1.1).

3.4.4 Measures must be taken to prevent and/or provide redress to any person for attacks directed towards their freedom of expression, including via digital and social media.

3.5 Access to information

3.5.1 The right to information is guaranteed in accordance with the following principles:

3.5.1.1 Every person, including a person with disabilities, has the right to access the information of public bodies expeditiously, inexpensively and in accessible format.

3.5.1.2 Every person has the right to access information about private bodies that may assist in the exercise or protection of any right expeditiously and inexpensively.

3.5.2 All information held by relevant electoral stakeholders in respect of the electoral process is presumed to be subject to full disclosure without the need to make a request. Stakeholders are entitled to access the information they seek on an equal basis, both online and offline, in an appropriate and accessible format.

3.5.3 Information may legitimately be withheld only where the potential harm to the interest protected under the applicable exemption demonstrably outweighs the public interest of disclosure, and only for the period in which the harm could occur.

3.6 Freedom of association and assembly

3.6.1 Every person has the right to freedom of association and freedom of peaceful assembly, which includes the protection of the wide variety of ways in which persons can associate and assemble through digital and social media.

3.6.2 Digital and social media should be recognised as a virtual space for enhancing networking, relationships and for the organising of interested groups to share mutual interests and benefits, including in relation to election-related matters such as campaigns, candidacy and voting.

3.6.3 Freedom of association and peaceful assembly can directly and indirectly be enhanced by access to digital and social media. Any restriction of access to such technology that can negate these rights should be subject to the application of the three-part test for a justifiable restriction.

3.7 Right to privacy

3.7.1 The right to privacy guarantees the protection of communications and personal information for all persons, both online and offline.

3.7.2 Every person has the right to autonomy over their personal information across any platform both online and offline, and the processing of personal information is only permissible in compliance with international laws and standards.

3.7.3 Communication surveillance, including on digital and social media platforms, must strictly comply with the three-part test as defined in clause 3.1.1 for a justifiable limitation, and be subject to adequate safeguards that protect the right to privacy.

3.8 Protection of the rights of women in the context of elections

3.8.1 All women have the right to fully participate in political life and to take part in the conduct of public affairs in line with the principles of non-discrimination and equal enjoyment of human rights.

3.8.2 Electoral stakeholders should take appropriate measures to counter online and offline violence and intimidation that have a negative impact on women's enjoyment of their rights.

3.8.3 Women's participation in elections should be understood not only in reference to voting and securing seats, but also to a wide range of other activities, including working with election management or related bodies or interfacing with civil society,

online and offline media, as well as political parties in relation to national and local elections. All relevant electoral stakeholders should support women in the full enjoyment of this participation.

3.9 Protection of ethnic, cultural and linguistic rights

3.9.1 Linguistic, ethnic and cultural diversity is a hallmark of public life in Africa. All relevant stakeholders have an obligation to protect and promote the rights of African communities to enjoy their own culture and use their own language when participating in electoral processes.

3.9.2 No member of an ethnic, religious, or linguistic minority community should be excluded from participating in the electoral process, either online or offline, because of their belonging to one or more of these communities.

3.10 Right to remedy

3.10.1 Individuals and communities whose rights are violated online or offline should have the means to seek and receive remedies.

3.10.2 The government must ensure that those whose rights are violated have accessible and effective remedies through an effective and independent recourse mechanism.

3.10.3 Private operators, such as internet service providers, telecommunications operators and the social media have the responsibility to ensure that the procedures for seeking remedies are clear, well known to citizens, easy to access and capable of providing appropriate redress.

4. STRENGTHENING DEMOCRACY AND DEMOCRATIC PRINCIPLES

4.1 All relevant electoral stakeholders have an obligation to implement measures that ensure respect, promotion and the fulfilment of electoral integrity, where the rule of law is respected, protected, promoted and fulfilled throughout the electoral cycle.

4.2 Engagement between the digital and social media companies, and EMBs and other electoral stakeholders is essential to protecting electoral integrity and to guard against online harm. This requires the development and implementation of

adequate measures and metrics to assess the effectiveness of the engagements to protect the integrity of a credible election.

4.3 All electoral stakeholders, including members of the media, must be allowed full access to relevant information and processes during the electoral cycle without intimidation or undue restrictions to publishing this information on any platform.

5. EQUALITY, FAIRNESS AND TRANSPARENCY

5.1 All relevant electoral stakeholders, including the digital and social media, commit to the highest standards of equality, non-discrimination, fairness and transparency in accordance with international human rights standards and comparative best practices.

5.2 In general, digital and social media should be accessible to all persons who desire and have the means to use them within the existing protections of equality, fairness and redress channels, and without discrimination of any kind.

5.3 Relevant electoral stakeholders must ensure that all relevant information pertaining to the electoral cycle and other related matters is available to the public in a timely and accessible manner for the media, researchers and other interested members of the public to review, scrutinise and object to as may be appropriate.

6. PROMOTING FREEDOM OF EXPRESSION

A central tenet of the right to freedom of expression and central to elections is the right to seek, receive and impart information and ideas across any form of communication or medium both online and offline.

6.1 Freedom of expression should be interpreted as including all content, provided that it complies with international human rights standards. This standard should be borne in mind by all relevant electoral stakeholders, including the digital and social media operators, when determining whether such content should be restricted.

6.2 The right must also be interpreted as protecting peaceful assemblies and campaigns that occur online, including through the different digital and social media.

6.3 The news media are subject to electoral codes and self-regulatory standards. As transparent actors in the public domain producing verified news, they should be an important antidote against electoral misinformation, disinformation and hate speech on digital and social media.

6.4 Digital and social media should be safe and accessible for all users to enjoy without discrimination or infringement of their rights. Users should abide by the terms of service for these spaces insofar as these terms do not undermine or contradict international human rights' standards.

6.5 The propagation of abusive, violent or similarly harmful election-related content on digital and social media on election-related matters during the electoral cycle infringes on the right to freedom of expression. Where there is doubt over whether content rises to the standard of abusive, violent or otherwise harmful, the content should be evaluated through the standards of international human rights law, including the three-part test if limitation is justified.

6.6 In order to protect persons' safety and the right to freedom of expression on digital and social media, specific measures must be developed and implemented to address the safety of vulnerable or marginalised persons, as well as relevant categories of stakeholders, including journalists, candidates and electoral officials.

6.7 Relevant electoral stakeholders must cooperate to ensure that all persons have access to universal, equitable, affordable and meaningful access to the internet to be able to access election-related information disseminated online. This includes, but is not limited to, adherence to the following principles of non-interference:

6.7.1 Relevant electoral stakeholders shall not engage in or condone any internet disruption of access to the internet and other digital technologies for segments of the public, nor an entire population during the electoral cycle.

6.7.2 Any interference with any person's right to seek, receive and impart information through any means of communication and digital technologies during the electoral cycle, such as the removal, blocking or filtering of content, is not permissible unless it is justifiable in the terms of the three-part test.

6.7.3 To the extent that any such interference arises during the electoral cycle or in relation to any election-related matter, digital and social media companies' digital intermediaries and other relevant stakeholders must ensure that human rights safeguards are mainstreamed into their responses. They must also ensure that there is transparency regarding any requests for removal of content or other restrictions, and there are established appeal mechanisms and effective remedies if the right to freedom of expression or any other right is violated.

7. PROMOTING ACCESS TO INFORMATION

7.1 The right to information is an invaluable cross-cutting right in a democratic society and plays a crucial role in facilitating participation in electoral process. This right is guaranteed under the following principles:

7.1.1 Any policy or practice creating a right of access to information shall be interpreted and applied based on a duty to disclose. Non-disclosure shall be permitted only in exceptionally justifiable circumstances as contemplated under the three-part test.

7.1.2 All relevant electoral information is subject to full disclosure within the boundaries of the law, including the duty to publish essential information of public interest.

7.2 All relevant electoral stakeholders are obliged to create, keep, organise, maintain and manage information relating to the electoral cycle in a manner that facilitates the right of access to information, and to keep and record information for a reasonable period of time on electoral cycle activities as determined by law.

7.3 In realising the right of access to information, relevant electoral stakeholders are required to take measures that facilitate the full enjoyment of the right, including, for instance:

7.3.1 Voluntarily and proactively disclosing relevant information related to the electoral cycle.

7.3.2 Promptly responding to access to information requests prescribed by law in line with international law and standards.

7.3.3 Making such information readily accessible to the public in relevant languages and different formats, across different technical options both online and offline.

7.3.4 Assisting persons in requesting or accessing information.

8. PROTECTING THE RIGHT TO PRIVACY

8.1 The right to privacy is an essential component of ensuring free, fair and credible elections, particularly concerning to any person's exercise of their right to vote.

8.2 While the digital and social media may serve as a means of mass communication (including when messaging services are used to reach large numbers of people), they must not be used to invade the privacy of other users and non-users, unless there is a public interest justification that meets domestic and international standards on the protection of private data.

8.3 Any processing of personal information by a relevant stakeholder must comply with the lawful conditions as established within international human rights law and standards.

8.4 Relevant electoral stakeholders shall not engage in nor condone any harmful and unlawful sharing of personal data, such as the unauthorised disclosure of personal details regarding a voter or candidate or the sharing of intimate images without informed consent, subject to the three-part test for a justifiable limitation.

8.5 Surveillance activities by electoral stakeholders, including acts of indiscriminate data collection, storage, analysis or sharing through the digital media and social during the electoral process are broadly prohibited. Any exceptions to this prohibition must comply with international human rights law and standards and be subject to the three-part test for a justifiable limitation.

8.6 Any form of communication surveillance undertaken during the electoral cycle is only permissible to the extent that it is justified in law, complies with international human rights law and standards, and is subject to adequate safeguards such as prior authorisation of a judicial authority and the implementation of measures ensuring due process. Encrypted communication should be respected.

8.7 All relevant stakeholders shall cooperate to ensure that all persons are protected from any harm that infringes on their human rights, and mechanisms are to be established to provide for effective remedies where there has been a violation of a person's privacy or unlawful processing of their personal information.

PART IV: GUIDELINES

9. THE STATE

9.1 The state should create an enabling environment to protect rights online and offline, and take measures that give equal protection to all stakeholders in the electoral processes, including opposition parties, candidates, citizens and vulnerable or marginalised persons. This includes addressing gender-specific concerns faced by women candidates and journalists engaged in the electoral process, such as sexual and gender-based violence, intimidation and harassment.

9.2 The state should ensure a robust legal and regulatory framework for the digital and social media that upholds the principles of democracy. This includes ensuring that there are no arbitrary limits to freedom of expression and media freedom during the electoral cycle.

9.3 The state should provide for the independent transparent regulation of digital and social media so that all stakeholders have clear guidelines on what constitutes the permissible and impermissible use of these services during the electoral cycle.

9.4 The state and its agencies must impartially apply laws used to counter potential online harm, particularly in cases of disinformation, hate speech and electoral offences targeting EMBs, critics of the state, the media, the political opposition, and human rights groups and other actors.

9.5 The state should ensure that personal data is protected, that data holders protect and secure the data in their possession or under their control, that such data is not unlawfully shared with any third party, and that its use, availability and longevity is in line with data protection standards.

9.6 The state should ensure effective data protection under an independent data protection authority. All parties have a duty to comply with legislation on privacy and personal data protection throughout the electoral cycle and using the following international data protection standards:

(a) Purpose limitation
(b) Fairness, lawfulness and transparency
(c) Data minimisation
(d) Storage limitation
(e) Accuracy
(f) Confidentiality and integrity
(g) Accountability

9.7 The state should require digital and social media to have structures and processes for reporting action related to election integrity, including for content curation and moderation, user appeal and redress.

9.8 The state and its agencies should refrain from imposing measures that might disrupt access to the internet, and to digital and social media. Any limitations must be necessary, proportionate, lawful and temporary, in line with international human rights standards. The state and its agencies should respond to providing digital intermediaries, and digital and social platforms with written reasons why such measures are sought, including justifications based on the three-part test for the measures being sought.

9.9 The state and its agencies, in collaboration with civil society and other relevant stakeholders, as may be appropriate, should provide effective civic education on electoral laws, citizen participation, media and information literacy, and digital literacy, and proactively provide open access to information to the electorate, including on the progress of the electoral cycle, in the multiple languages of the country through multiple online and offline channels.

9.10 The state should promptly investigate and prosecute individuals who use digital and social media to infringe on the privacy of others, or engage in online harm such as the spreading of hate speech, misinformation and/or disinformation that violates human rights and may undermine the integrity of the elections.

9.11 The state should ensure that EMBs and other oversight bodies are properly resourced to effectively conduct their digitally relevant activities online during the electoral cycle.

9.12 The state should address the digital divide to facilitate participation in electoral processes, and develop strategies to extend access to the internet to various communities in an affordable and meaningful manner, including media and information literacy, and its digital literacy dimensions.

10. THE ELECTION MANAGEMENT BODIES

10.1 EMBs should cooperate in developing strategies and implementing measures to address specific forms of online harm occurring on digital and social media during the electoral cycle.

10.2 Throughout the electoral cycle, EMBs should deepen their internal capacity to understand and effectively use digital and social media, while partnering with relevant research and academic stakeholders to monitor and understand the technologies.

10.2.1 Ahead of elections, EMBs should conduct advanced assessments of opportunities and risks to their mandate arising from digital and social media.

10.2.2 EMBs are encouraged to maintain a presence on social media as permitted by law, and keep their presence as up to date and responsive as possible to avoid information gaps. This presence should be conducted with the highest standards of cyber security, including the use of strong passwords and encryption where relevant.

10.3 EMBs should have transparent cooperation agreements with digital and social media, focused on protecting the digital rights of users.

10.4 EMBs should develop partnerships, mechanisms and capacities to monitor the digital and social media throughout the electoral cycle through relevant partnerships and collaborations with regulatory bodies, including monitoring

adherence by candidates and parties to the guidelines on the use of digital and social media in elections.

10.5 EMBs should develop guidelines on the transparency of online political advertising on digital and social media (including social media "influencers") in the interest of electoral transparency, fairness and integrity, while respecting citizens' privacy and data protection rights.

10.6 EMBs should facilitate and monitor the implementation of these Guidelines, on such aspects as sources and levels of advertising funds applicable to digital outputs, the nature of adverts, the advert's beneficiaries, the targeting methodology and the transparency of "adtech" companies about political advertisements.

10.7 EMBs, in cooperation with all relevant electoral stakeholders, must ensure that the public is provided, through all types of media, with all information pertaining to the electoral cycle across different channels, including information relating to registration deadlines, voting dates, polling stations and election results, in a timely and consistently updated manner throughout the electoral cycle.

10.8 EMBs and all stakeholders should collaborate to ensure that digital and social media are not used to propagate false information regarding electoral irregularities or any election-related information throughout the electoral cycle that may unlawfully undermine the integrity of the election.

10.9 EMBs should take gender equality into consideration and facilitate equal access to elections-related information for men and women, and develop mechanisms to monitor and ensure the accountable use of digital and social media to prevent and sanction election-related attacks on women.

10.10 EMBs must consider people with disabilities while transmitting election-related messages through the digital and social media, and ensure the use of appropriate communication channels and accessible formats for all disability groups, mindful of the affordability of the chosen communication medium.

10.11 EMBs should consider partnerships with relevant stakeholders to harness the youth potential as digital and social media creators and consumers, and

empower them with media and information literacy skills, including digital dimensions, and voter education.

10.12 EMBs must develop mechanisms that integrate digital and social media as a platform to prevent and manage election-related conflict.

10.13 EMBs and oversight bodies should work with the media, academia, civil society organisations, social media and security forces to detect challenges arising from digital and social media that could threaten the electoral process before they occur, and develop risk mitigation strategies to address them.

10.14 EMBs should consider developing strategies and action plans to harness the benefits and respond to misinformation and other harm arising from digital and social media. These strategies should ensure that the election is not undermined by online harm throughout the election cycle.

11. DIGITAL AND SOCIAL MEDIA

11.1 In line with the United Nations' Guiding Principles on Business and Human Rights (UNGPs), the digital and social media must put in place processes for human rights due diligence and human rights impact assessment to identify, prevent, mitigate and account for how they address their impacts on human rights during the electoral cycle, and disclose these processes for transparency and accountability.

11.2 Social media operators should treat political parties and candidates equitably, provided their messages do not undermine electoral integrity and contravene human rights.

11.3 Social media operators should proactively contribute to elections by encouraging voter registration and voting by promoting sources of reliable and verified electoral information, and by supporting media and information literacy as relevant to elections.

11.4 Social media operators should provide information that is clear, understandable and accessible during the entire electoral cycle regarding the following:

11.4.1 Political advertising, including information relating to the political advertisements themselves, the origin and the funding of such advertisements and a repository of such advertisements

11.4.2 Measures to protect users from any malicious or harmful use of the applicable technologies to target users with, for instance, misinformation, disinformation, mal-information and hate speech, as well as the measures to be established to respond accordingly

11.4.3 Specific measures to protect marginalised persons, including candidates who are female or who belong to ethnic, religious, sexual or gender minorities

11.4.4 The criteria to be applied when implementing such measures, including in respect to the removal or down-ranking of content, application of labels, de-monetisation or other restrictions on content

11.4.5 The applicable algorithms, including access to the back-end architecture, to allow regulatory bodies to conduct audits

11.4.6 Access to curated relevant data, including by means of application programme interfaces, to enable the independent monitoring of content and networks that may harm election integrity

11.4.7 The designation of “trusted flaggers” and any monitoring activities, proactive removal of content or other treatment of content, and complaints received in the context of the electoral cycle, including the outcomes and appeals lodged

11.5 Social media operators should be transparent and accountable about their corporate policies concerning elections, their content curation, and moderation measures and capacity in local languages, and should work with the media, civil society, EMBs and other key actors to publicise their content curation and moderation standards and reporting mechanisms for potentially harmful electoral-related content. Social media operators should provide effective systems of vetted access to data for research purposes as relevant to electoral integrity.

11.6 Social media operators should conduct periodic reviews of their content curation and moderation policies through broad multi-stakeholder consultations to ensure that those policies remain effective and relevant to their stakeholders in the electoral cycle.

11.7 Social media operators should institute mechanisms and employ sufficient numbers of human content moderators who are knowledgeable about local contexts, languages, slang and sensitivities to enable them to conduct timely identification, and transparent curation and moderation.

11.8 Social media operators must deliberately enhance their software, including recommender systems, to ensure that they do not prioritise and amplify content that is restricted under international human rights law.

11.9 Social media operators must take specific measures to address the needs of marginalised groups in a manner that guarantees the full enjoyment of fundamental rights on an equal basis with others, including in respect of access to online services, safety online, and media and information literacy and digital literacy.

11.10 Social media operators should request regulators and state agencies that issue directives to disrupt the use of digital and social media (such as internet disruptions, social media blockage, website shutdown and internet throttling) to provide written reasons why measures were sought, including justifications for the directives in line with the three-part test for a justifiable limitation to be implemented.[xii]

11.11 Digital intermediaries, the digital and social media, and relevant electoral stakeholders shall neither engage in nor condone the arbitrary disruption of access to the internet and other digital technologies for segments of the public or an entire population during the electoral cycle.

11.12 No actor should obstruct any person's right to seek, receive and impart information through any means of communication, including digital technologies, during the electoral cycle, such as the removal, blocking or filtering of content.

11.13 Recommender systems must not process any data that can be associated with a person and that could categorise their sensitive personal characteristics,

including the following categories of information:

(a) Religious or philosophical beliefs
(b) Race or ethnic origin
(c) Trade union membership
(d) Political persuasion
(e) Health or sex life

11.14 The exception to this prohibition in subsection 11.13 above is where the individual concerned has given their specific consent for the use of the specific category of information. In this case, the digital service provider must present, at all times and places where the recommender system is active, the means for the user to switch off the recommender system again. These means must be highly visible and immediately accessible.

11.15 A person may consent to the use of their data for advertising by a specific digital or social media entity. In this case, the digital service provider should completely anonymise that data before sharing it with any other entity (including entities within the same company) so that it can never be linked to that person again.

11.16 The use of Artificial Intelligence should be transparent. People must be informed when they are interacting with an AI system, unless the context makes this obvious.

11.17 Digital and social media operators have an obligation to monitor the dissemination of manipulated and synthetic media that may affect the electoral processes. To the extent possible, users must be informed if the content being presented to them was not generated by a human.

11.18 All digital or electronic systems monitoring someone's emotions must inform the person of this fact to protect their fundamental digital right to privacy and personal autonomy.

11.19 End-to-end encryption is a crucial tool for protecting privacy rights and, if technology provides for it, encryption should be respected throughout the entire electoral cycle. Where there is a public interest justification for accessing the meta-data generated by encrypted information, the justification should satisfy

international human rights law and the three-part test set for justifiable limitation.

12. REGULATORY BODIES

Recognising that EMBs have a mandate to regulate elections, it is important in regard to digital and social media to ensure coordination with other regulators such as data protection and communications authorities, and self-regulatory bodies such as press councils and advertising industry standards bodies.

12.1 Regulatory bodies should ensure accountability and compliance with the laws and promotion of human rights by digital and social media operators.

12.2 Rules for digital and social media should be developed and monitored through a multistakeholder process that includes, but is not limited to political parties, candidates, the digital and online media, civil society and academia. This process should be led by an independent body that regulates the media, by the EMB or by another statutory media monitoring body. In all cases, basic oversight principles and standards should be respected. Oversight structures should cover, at a minimum, the following:

(a) Explicit legal guarantees of autonomy and independence
(b) Powers and responsibilities clearly set out in law
(c) Members chosen transparently and democratically
(d) Adequate and consistent funding to safeguard independence
(e) Accountability to the public
(f) Empowered to promote fairness, freedom of expression and access to information as relevant to the election

12.3 Independent oversight bodies should work to develop self-regulatory tools that are outside the existing regulatory scope to resolve common problems that arise through such regulatory gaps. This should also be done through further multi-stakeholder cooperation, and should support the capacity of the digital and social media to meet the required legal standards.

12.4 Regulatory bodies should ensure a safe digital space for citizens by instituting clear rules governing the use of the digital and social media in elections, and

implement those laws fairly, timeously and transparently.

12.5 Data protection supervisory authorities should take active roles in relation to elections in upholding citizens' privacy and data protection rights during the entire electoral cycle, and should build on the Malabo Convention 2014 and other international standards to draw up appropriate safeguarding measures.

12.6 Regulatory authorities should require the digital and social media to conduct regular human rights risk and impact assessments before the elections and to implement measures to mitigate any risks.

12.7 Regulatory bodies should develop regulations to deal with political micro targeting and online political advertising. These regulations should govern what candidates and political parties can do and the obligations of digital and social media.

12.8 Regulatory bodies should ensure a robust cyber security stance to ensure that the online systems and resources of EMBs, political parties and other actors are not subjected to technical attacks that may hit their robustness and undermine electoral integrity.

12.9 Regulatory bodies have the duty to censure internet disruptions that occur outside of the three-part test during elections.

12.10 End-to-end encryption is a crucial tool for protecting privacy rights and should be respected throughout the electoral cycle. Where there is a public interest justification for accessing the metadata generated by encrypted information, this should satisfy international human rights standards and the three-part test.

13. POLITICAL PARTIES AND CANDIDATES

13.1 Political parties and candidates that use digital and social media should be aware of the risks and benefits for the entire electoral cycle, as well as the commercial incentives of those who own and run these communication channels.

13.2 Political parties and candidates should not commit, support, encourage or condone any form of potential online harm, including by their supporters during the entire electoral cycle, and should comply with relevant rules and standards.

13.3 Political parties and candidates should ensure that campaigns conducted on digital and social media, including messaging, are transparent and clearly attributed, including the use of paid-for-content, including influencers.

13.4 Political parties, political leaders, members and candidates should uphold data protection and protect fundamental rights, including voters' data protection rights.

13.5 Political parties and candidates should abide by the electoral and other relevant codes of conduct on content generated and distributed online during the electoral cycle, and raise awareness of these provisions to the voters and their membership rank and file. Where such a code of conduct is absent, political parties and candidates should participate in the development of such a code of conduct.

14. AFRICAN TRADITIONAL INSTITUTIONS AND RELIGIOUS BODIES

African traditional institutions and religious bodies should engage with digital and social media to seek to understand the role and function they can play in ensuring the effective dissemination of election-related information, including measures to contribute to the following:

(a) Improve access to information
(b) Dissemination information on all social media in local languages
(c) Collaborate in community-based civic and democracy-related initiatives
(d) Promote peace and security during the electoral period

15. CIVIL SOCIETY ORGANISATIONS

15.1 Civil society organisations should engage with the state, EMBs, the digital and social media and other relevant electoral stakeholders to initiate and implement media and information, as well as digital literacy and fact-checking skills initiatives.

15.2 Civil society organisations should incorporate the capacity for advocating for human rights and freedom in their election observation and civic education initiatives, and develop their capacity to provide oversight over the relevant electoral stakeholders on the use of the digital and social media during elections.

15.3 Civil society should conduct policy advocacy that challenges unfair and

inequitable access to the digital and social media by parties that are seeking to use these technologies.

16. JOURNALISTS AND THE NEWS MEDIA

16.1 Journalists and the news media should, in line with professional ethics and standards, help ensure that the information shared on their digital and social media during elections is verified and factual. They should advance the protection of rights and prevent the promotion of violence, while providing fair and balanced coverage of candidates, parties and issues on their digital and social media.

16.2 Media owners and editors should put measures and systems in place to protect journalists, especially women journalists, online and offline, during the entire election cycle.

16.3 Media owners and editors should create measures and systems to promote gender-sensitive reporting and the equitable coverage of men and women candidates during elections.

16.4 Journalists and the news media should develop election-reporting guidelines relevant to the digital ecosystem, in collaboration with the relevant statutory and self-regulatory bodies.

16.5 News media houses should put in place measures and systems to enhance fact-checking and information verification, including working closely with fact-checkers to identify and expose disinformation and other potentially harmful content in a timely fashion, and building the capacity of journalists and editors to conduct fact-checking.

16.6 The news media should pursue and publish relevant investigative journalism to enhance the integrity of the entire electoral cycle, including, but not limited to understanding the impact of digital and social media on the elections, or the covert financing and spread of content that causes potential digital harm.

16.7 Journalists should raise awareness about the risks of the misuse of digital and social media, including hate speech and disinformation, and the impact on voters' access, to be a vibrant, diverse and fact-based information ecosystem.

17. DIGITAL INTERMEDIARIES

17.1 Digital intermediaries should adhere to the UNGPs, as outlined in section 11 above.

17.2 In line with the UNGPs, digital intermediaries should conduct human rights due diligence, including impact assessments and risk assessments in advance of an election, comply with all applicable laws, respect human rights wherever they operate, and honour all applicable laws and the principles of internationally recognised human rights when faced with conflicting requirements during the electoral cycle.

17.3 Digital intermediaries should put in place transparent policy provisions for elections, as well as clear, timely, well-publicised grievance and remedy mechanisms, and ensure that any affected person is duly informed thereof.

17.4 To the extent that any interference arises during the electoral cycle or in relation to any election-related matter, digital intermediaries and other relevant stakeholders must include human rights safeguards in their processes. They should also ensure that there is transparency regarding any requests for the removal of content or other restrictions, and establish appeal mechanisms and effective remedies if the right to freedom of expression or any other right has been violated.

18. ACCOUNTABILITY MECHANISMS

18.1 All relevant laws should be enforced without discrimination. Accountability and redress mechanisms should be established and effectively implemented by the AU member state and intergovernmental bodies to ensure accountability for the perpetration of any online harm, including, for instance, through judicial and legislative measures, as well as self-regulatory bodies, as applicable.

18.2 All relevant stakeholders should cooperate to ensure that all rights impacted by digital and social media are fully protected and realised during the electoral cycle and that the elections are free, fair and credible. This may include frameworks for cooperation, agreed working methods and protocols, and designated communication channels in the event of urgent matters arising.

ACKNOWLEDGEMENTS

The AAEA is grateful to the South African Department of International Relations and Cooperation (DIRCO) African Renaissance Fund (ARF) for the financial support for developing these principles and guidelines, and the Electoral Commission of South Africa for superintending the process and convening the Technical Working Group. We are grateful to the partnership support provided by the following organisations:

African Union Commission (AUC)
United Nations Development Programme (UNDP)
United Nations Educational, Scientific and Cultural Organization (UNESCO)

The following experts and practitioners constituted the Technical Working Group.
Dr Victor Shale, Ms Nanjala Nyabola, Ms Avani Singh, Ms Idayat Hassan, Professor Guy Berger, Dr Jonny Ryan, Dr Wairagala Wakabi, Mr Robert Gerenge, Ms Hilda Modisane, Ms Albertina Piterbarg, Mr David Onen, Mr Moise Bukasa, Mr Naoufel Frikha, Dr Expedit Ologou.

ENDNOTES

[i] ACHPR, Guidelines on Access to Information and Elections in Africa, 2017.

[ii] Kofi Annan, 2012. Electoral integrity and deepening democracy worldwide, https://www.kofiannanfoundation.org/speeches/electoral-integrity-and-deepening-democracy-worldwide/.

[iii] Ace Project, Preventing Election-related Violence, https://aceproject.org/ace-en/topics/ev/default/mobile_browsing. Also see UNDP.

[iv] Access Now. n.d. 26 recommendations on content governance, a guide for lawmakers, regulators, and company policy makers, https://www.accessnow.org/wp-content/uploads/2020/03/Recommendations-On-Content-Governance-digital.pdf.

[v] Santa Clara Principles, 2021, https://santaclaraprinciples.org/es/open-consultation/.

[vi] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) PE/30/2022/REV/1, *OJ L 277, 27.10.2022, pp. 1–102.*

[vii] https://ico.org.uk/for-the-public/be-data-aware/social-media-privacy-settings/microtargeting/

[viii] See the the AI Act, https://www.euractiv.com/section/artificial-intelligence/news/eu-lawmakers-set-to-settle-on-oecd-definition-for-artificial-intelligence/.

[ix] Deen Frelon and Chris Wells, “Disinformation as political communication”, Political Communication 2020, Vol 37 (2), pp. 145–156, https://doi.org/10.1080/10584609.2020.1723755.

[x] Deen Frelon and Chris Wells, “Disinformation as political communication”, Political Communication 2020, Vol 37 (2), pp. 145–156, https://doi.org/10.1080/10584609.2020.1723755.

[xi] Action_Plan_on_Hate_Speech_EN.pdf. Also see the United Nations Strategy and Plan of Action on Hate Speech.

[xii] Global Network Initiative. Implementation Guidelines for the Principles on Freedom of Expression and Privacy, Clause 3.2, https://globalnetworkinitiative.org/implementation-guidelines/.