DIGITAL RIGHTS AND ELECTIONS IN AFRICA

MONITORS TOOLKIT

PRIVACY INTERNATIONAL

PARADIGM INITIATIVE

DIGITAL RIGHTS AND ELECTIONS IN AFRICA MONITORS TOOLKIT (DREAMT)

(FIRST EDITION)

August 2025

Published by
Paradigm Initiative

With support from
Privacy International

Researchers:
Thobekile Matimbe and Sani Suleiman

Digital Security Expert:
Angela Onyegbuna

Design and Layout
Kenneth Oyeniyi

DIGITAL RIGHTS AND ELECTIONS IN AFRICA MONITORS TOOLKIT (DREAMT)

Acknowledgements

This toolkit is a Paradigm Initiative (PIN) publication supported by Privacy International. PIN is grateful for their funding support and collaboration.

Who is the Toolkit for?

This toolkit can guide individuals or organisations identifying as an Election Observer or Election Monitor, in assessing the environment before, during and after an election. *Election monitors* are individuals or organisations who have a mandate to observe an electoral process and to intervene in that process if relevant laws or standard procedures are being violated or ignored.[1] *Election observers* refer to accredited independent, non-partisan individuals who have a mandate to observe an electoral process but not to interfere in the process.[2]The election period (the period) referenced in this toolkit for monitoring digital rights and elections covers the following:

- Pre-Election Phase (0-6 months).
- Election Days
- Post-Election Phase (Up to 3 months).

How to Use the Toolkit?

This toolkit is simple, practical, and easy to navigate. You can read to understand key issues in elections and use the monitoring tools and resources to document and report digital rights threats and violations. If you are a trainer, you can adapt this toolkit to the country context, citing relevant examples from the country. Reference Paradigm Initiative (PIN) when training with this tool and provide monitoring feedback through PIN's various platforms.[3]

[1] https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/guidelines_on_access_to_information_and_elections_in_africa_en.pdf

[2] https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/guidelines_on_access_to_information_and_elections_in_africa_en.pdf

[3] https://paradigmhq.org/

DIGITAL RIGHTS IN ELECTIONS

Overview

The United Nations has established that digital rights are human rights online, as presented in the text box above. They are human rights exercised and enjoyed through the use of digital technologies. Digital rights are cross-cutting, and violations can affect civil, political, and socio-economic rights.

> The 32ND Session of the UN Human Rights Council in 2016 established its position as follows:
>
> *'1. Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;'*

Election periods are critical times when individuals in a country exercise their civil and political rights, demonstrating their choice through voting. Election seasons are times when non-discrimination, freedom of expression, freedom of peaceful assembly and association, privacy and access to information are vulnerable human rights in repressive contexts, which can be violated, among others. Some African countries have now embraced biometric voter registration technologies, allowing citizens to register to vote. Directly or indirectly, elections are now powered by the internet. Some countries that are not largely reliant on digital technologies are still linked to technology in one form or another. Political discourse is now exercised beyond offline spaces, having also migrated to online platforms such as Facebook and X. Political actors can now access the electorate through WhatsApp and other communications platforms.

The digital age has brought immense benefits, increasing access to information during elections through online media, especially when some countries still face the challenge of not having a pluralistic media. Where in the past, ruling political parties monopolised the traditional national broadcaster and media, online media platforms offer a solution to advance media freedom in Africa. The assortment of digital threats to elections is ever-expanding. For this toolkit, we look at the following key thematic areas:

- Internet shutdowns
- Data Protection
- Information Integrity
- Freedom of Expression
- Access to Information

GOVERNING REGIONAL AND INTERNATIONAL STANDARDS

Treaties	Articles
International Covenant on Civil and Political Rights	*19.2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.* *19.3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:* *(a) For respect of the rights or reputations of others;* *(b) For the protection of national security or of public order (ordre public), or of public health or morals.'* *25. Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions:* *(a) To take part in the conduct of public affairs, directly or through freely chosen representatives;* *(b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;*
African Charter on Democracy, Elections and Good Governance	3. 1 Respect for human rights and democratic principles; 3.4. Holding of regular, transparent, free and fair elections; 4.1 State Parties shall commit themselves to promote democracy, the principle of the rule of law and human rights. 6.1 State Parties shall ensure that citizens enjoy fundamental freedoms and human rights taking into account their universality, interdependence and indivisibility.
African Charter on Human and Peoples' Rights	*9.1 Every individual shall have the right to receive information.* *9.2. Every individual shall have the right to express and disseminate his opinions within the law.'*
African Convention on Cyber and Personal Data Protection	*8.1* Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data.

GOVERNING REGIONAL AND INTERNATIONAL STANDARDS

Soft Law	
African Commission on Human and Peoples Rights *Declaration of Principles on Freedom of Expression and Access to Information*	Principle 40(1) *Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information.*
ACHPR Resolution 573 on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa	i.Ensure that all restrictions on the rights to privacy and other fundamental freedoms, such as freedom of expression, freedom of association and freedom of assembly, are necessary and proportionate, and in line with the provisions of international human rights law and standards; ii.Align approaches on the regulation of communication surveillance with relevant international human rights law and standards, considering safeguards such as the requirement for prior authorization by an independent and impartial judicial authority and the need for effective monitoring and regular review by independent oversight mechanisms; iii.Only engage in targeted communication surveillance that is authorized by law, that conforms with international human rights law and standards, and premised on reasonable suspicion that a serious crime has been or is being carried out;
ACHPR Resolution 580 on Internet Shutdowns and Elections in Africa	Taking into consideration the increased use of the internet and social media platforms for the dissemination of information to voters, election observers, election management bodies and other stakeholders, particularly during elections; **The Commission calls on State Parties to:** (i) Ensure compliance with the African Charter, the African Charter on Democracy, Elections and Good Governance and relevant regional and international human rights instruments during the electoral process; (ii) Take the necessary legislative and other measures to ensure open and secure internet access before, during and after elections, including ensuring that telecommunications and internet service providers take adequate steps to provide unrestricted and uninterrupted access; (iii) Refrain from ordering the interruption of telecommunications services, shutting down the internet, and/or disrupting access to any other digital communication platforms before, during or after the elections; (iv) Require telecommunications and internet service providers to inform users of potential disruptions and exercise due diligence to resolve any disruptions expeditiously.

GOVERNING REGIONAL AND INTERNATIONAL STANDARDS

Guidelines on Access to Information and Elections in Africa	3. The presumption is that all information held by relevant electoral stakeholders is subject to full disclosure. Accordingly, relevant electoral stakeholders are obliged to publish key information of public interest about their structure, functions, powers, decision-making processes, decisions, revenue and expenditure in relation to the electoral process. 26. The body responsible for regulating the broadcast media and any other relevant national security, public or private body involved in the provision of telecommunication services shall refrain from shutting down the internet, or any other form of media, during the electoral process. 27. In exceptional cases in which a shutdown may be permissible under international law, the reasons for any shutdown shall be proactively disclosed. Such limitation shall: (a) Be authorised by law; (b) Serve a legitimate aim; and (c) Be necessary and proportional in a democratic society. 28. Any decision of the Media or Internet Regulatory Body shall be subject to judicial review, which shall be undertaken on an expedited basis.
ACHPR Resolution 620 on promoting and harnessing data access as a tool for advancing human rights and sustainable development in the digital age	1. Urges States Parties to: a) Ensure that data collection, processing, storage and access practices are transparent, accountable and in line with regional and international standards in this era of digitalization and increasing use of AI;

MONITORING INTERNET SHUTDOWNS

Internet shutdowns are common during elections in countries where governments seek to interfere with the free flow of information. They occur in various forms but are intentional disruptions of the internet or electronic communications, making them inaccessible or unusable.[4] They can be implemented for specific populations or can affect specific social media platforms such as X or Telegram.[5] Internet shutdowns are also referred to as a 'kill switch' due to their inherent ability to disconnect communities from accessing the internet, a deliberate digital exclusionary practice.

1. Amnesty International Togo and Ors v. The Togolese Republic (ECW/CCJ/JUD/09/20)

The Community Court of Justice of the Economic Community of West African States (ECOWAS) holds that freedom of expression is a derivative right and that the Togolese government violated the right to freedom of expression of the applicants by shutting down the internet in September 2017. The Court passes a decision that guarantees the "non-occurrence" of internet shutdowns and orders compensation to the sum of 2,000,000 CFA (approx. 3,500 USD).

2. Internet Shutdown in Guinea-Conakry

In a similar case to Amnesty v Togo mentioned above, the ECOWAS Court, following a case of the government of Guinea-Conakry shutting down the internet in March and October 2020 held that the conduct violated freedom of expression and access to information and that freedom of expression. Is a derivative right.

Monitoring Steps

To track whether there is a total internet shutdown, you can rely on the tools developed by the organisations in the measurement community, such as NetBlocks[6] and Ooni.[7]

Indicators of Internet Shutdowns

- No access to major websites
- Connectivity slows down during major events such as political rallies, election protests, election days, and the announcement dates of election results.

How to remain connected during elections?

- Use of Virtual Private Networks (VPNs), see Ayeta[8] for guidance.
- Install OONI Probe at least 6 months before the election to enable data collection to gather evidence of internet censorship, since it shows how, when and where it is implemented. Information on internet censorship trends can be found on OONI's Detection Analysis (IODA), which monitors the internet and detects internet connectivity

[4] https://www.accessnow.org/issue/internet-shutdowns/
[5] https://www.mediadefence.org/
[6] https://netblocks.org/
[7] https://ooni.org/install/
[8] https://paradigmhq.org/wp-content/uploads/2024/04/AYETA-Digital-Rights-Toolkit-1.pdf

outages in real time on an interactive internet outages dashboard, which allows users to track internet outages globally.

- Is there a slowdown in internet access or a total blackout?
- When did it start and end? (If ongoing, you can indicate it as still pending. Also, report this occurrence on Ripoti.)
- If so, what websites are affected? (All websites or specific platforms like X or Facebook?)
- Did the government communicate a blocking of internet access or order it?
- If so, can you share a link to the communication/order?
- Which government agency ordered it?
- Which law did they rely on?
- Did the internet service providers (ISPs) communicate that they will block internet access?
- If so, any links to this?

DATA PROTECTION AND ELECTIONS

Privacy International has published a Data and Elections Checklist[9] that outlines the importance of the right to privacy during elections. National constitutions promote the right to privacy and some have data protection legislation. However, in countries like Kenya[10] and Zimbabwe,[11] there have been violations of privacy, where political parties access the contact numbers of voters and send text messages soliciting votes or requesting voters to attend political rallies. This practice contradicts most data protection laws in countries where they exist.

- Are citizens getting any unsolicited political messages through text messages or other communications technologies?
- Which networks are these messages being sent from?
- Has there been any data breach of the voters' roll or other personal data in elections online?

Biometric Technologies

Biometrics involves measuring and analysing unique physical or behavioural characteristics, especially to verify and identify an individual. The broad range of biometric traits that can be measured includes fingerprints, palm prints, retina and iris scans, voice patterns and

[9] https://privacyinternational.org/sites/default/files/2023-11/Data%20and%20elections%20checklist_Update_Final_21Nov_Reduced.pdf

[10] https://privacyinternational.org/sites/default/files/2018-06/Biometric%20Technology-Elections-Privacy.pdf

[11] https://www.techzim.co.zw/2018/07/econet-denies-selling-customers-data-to-3rd-parties-refutes-zecs-allegations-so-who-sold-data-to-zanu-pf/

DNA profiles[12]The most commonly captured biometric features for electoral purposes are fingerprints for automatic fingerprint identification systems (AFISs), facial images of voters for facial recognition systems (FRSs), and sometimes also scanned signatures. Regulation is required regarding the purposes for which biometric data can be used and the individuals to whom this data can be disclosed. Citizens whose data is collected should be able to obtain information about how this data will be used, and they should have an opportunity to access their data and correct any inaccuracies.

Countries like Kenya use several technologies in the electoral process, including Biometric Voter Registration (BVR) systems, posing data protection concerns for the right to privacy. In Malawi, the Malawi Electoral Commission procured new technologies for use in the 2025 election from Smartmatic, with concerns[13] raised over the integrity of the election management systems. In Nigeria, failure to report election results resulted in protests during the 2023 elections. The Independent National Electoral Commission (INEC) result viewing portal (IREV) failed to upload the presidential results of the 25 February 2023 election promptly, despite the seamless working of the bimodal voter accreditation system (BVAS), posing concerns of bias and manipulation. Apart from data protection concerns, misinformation and disinformation thrive where there is no adequate information concerning the use of biometric technologies during elections. See an extract below on Zimbabwe.

> ‘Heal Zimbabwe through its trained Human Rights Monitors (HRMs) has been monitoring the electoral environment ahead of the voter registration exercise and has noted an increase in cases of human rights violations where some overzealous political activists are saying the BVR system is capable of allowing political parties to see how one votes.’
>
> *An extract on a Monitoring Report by Heal Zimbabwe on the Biometric Voter Registration (BVR) in Zimbabwean elections.*[14]

Using biometrics for voter registration and identification does not eliminate the need for transparency measures related to voter registration. Building stakeholder trust in biometrics and avoiding incorrect perceptions requires continuous awareness raising. Information about the systems in use should be provided throughout the election period and cycle. When biometric technologies are adopted in the absence of a robust data protection law, the right to privacy and personal security is at risk..[15]

[12] https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf

[13] https://www.investigativeplatform-mw.org/show-story/mecs-controversial-it-partner

[14] https://kubatana.net/2017/09/08/voter-educators-diffuse-myths-suspicions-biometric-voter-registration/

[15] https://privacyinternational.org/report/2066/investigating-privacy-implications-biometric-voter-registration-kenyas-2017-election

- Is there a Data Protection law in your country addressing using biometric technologies during elections?
- Is the Election Management Body sharing adequate information on the use of biometric technologies to prevent misinformation and disinformation?
- Any misinformation and disinformation about the use of biometric technologies?
- Any links to the reports?

SURVEILLANCE

Surveillance during elections refers to the secret monitoring of people's communications, activities, movement, and personal data. This is done without consent and usually targets journalists, activists, opposition candidates, and sometimes voters. While certain rights and freedoms can be limited, there should be judicial oversight to safeguard the rights of individuals. In the absence of judicial oversight, rights are violated. Surveillance can take different forms, such as:

- Hacking phones or emails to spy on private conversations.
- Tracking social media activity to monitor critics or opponents.
- Using spyware to gather personal information.
- Monitoring public spaces and gatherings with facial recognition technologies and other technologies such as spyware.

- Was there any mention of targeted mass communications surveillance during elections?
- Was there any targeted surveillance on any individuals or specific groups?
- If so, where was this communicated?
- Which government agencies are responsible for this surveillance?
- Was there any procurement or deployment or surveillance tools?
- Was there any deployment of public space surveillance tools during the period ?
- Was there any arbitrary seizure of digital technologies for voters, journalists, human rights defenders, election observers/monitors, civil society organisations etc?
- Any links?

Why It's a Problem in Elections

- ***Silences voices:*** *People may be afraid to speak up or participate if they feel watched.*
- ***Violates the right to privacy:*** *Surveillance can expose private data, campaign plans, or voter choices.*
- ***It is Intimidation:*** *Information from surveillance can be used to threaten or discredit opponents and makes an election unfair.*
- ***It is Abuse of Power by Ruling Parties:*** *It enables those in power to abuse it and target the opposition.*

FREEDOM OF EXPRESSION

Free speech is regarded as fundamental during elections. Any means to curtail this freedom should not unjustifiably interfere with individuals' right to engage in political discourse and share views online.

> *Article 21 of the Universal Declaration of Human Rights and article 25 of the Covenant guarantee the right to participation in public affairs. The Human Rights Committee has affirmed that, in order to ensure the full enjoyment of rights protected by article 25, the "free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion.* UN General Assembly A/77/287 (Paragraph 19)

The ACHPR Declaration[16] defines prohibited speech in Principle 23.1 as any speech that advocates for national, racial, religious or other forms of discriminatory hatred which constitutes incitement to discrimination, hostility or violence. Principle 23.3 stipulates that States shall not prohibit speech that merely lacks civility or which offends or disturbs. Political discourse should not be criminalised.

What to Watch?

- Are there any arrests of individuals for political speech online?
- Who is specifically targeted/affected?
- Is there any disclosure on the charges they are facing?
- Are the arrests in terms of a law in the country discourse (insult laws, false news, inciting public violence, criminal defamation, etc.?
- Which law and provision allows the arrest if known?

Tracking Misinformation and Disinformation

Information Disorders

The following are common forms of information disorders during elections:

1. Misinformation stands for sharing false information, but without the intent of causing harm[17]
2. Disinformation stands for knowingly sharing false information with the intent to harm.[18]
3. Malinformation describes genuine information shared with the intent to cause harm, often by disclosing information from the private sphere into the public sphere.[19]

[16] https://achpr.au.int/en/node/902

[17] https://firstdraftnews.org/long-form-article/understanding-information-disorder/

[18] Abid

[19]

What to Watch:

- Spread of false or misleading information targeting candidates, institutions, or voters.
- Use of social media, bots, or networks to amplify narratives.
- Presence (or absence) of fact-checking mechanisms.

> *While the spread of disinformation during such periods may exacerbate adverse impacts on human rights, Internet shutdowns have broad impacts on a full range of rights and may even contribute to human rights violations and abuses, including by limiting their visibility. Given the indiscriminate reach and broad negative impacts of shutdowns, they very rarely meet the human rights requirements of necessity and proportionality.* UN General Assembly A/77/287 (Paragraph 45(e))[20]

Many countries in Africa address disinformation in elections in unclear and broad terms leading to human rights violations. Some adopted approaches by States include the following:

- Vague definitions of false news in Criminal or Penal Codes or Laws.
- Internet shutdowns
- Deployment of targeted mass communications surveillance using technology

In the digital age, technologies like artificial intelligence (AI) and other emerging technologies can be used for bad or good in elections. The rise of deepfakes for instance, are problematic as this misleads the electorate. An example of deepfake usage is seen in the extract below where fake videos mimicked xxxxx. The effect of such content is a misled voting electorate and election monitors should be able to monitor social media platforms such as Facebook, X and WhatsApp to assess the following:

- Was there any use of politically oriented deepfakes and AI-generated misleading content online before, during, and after the elections?
- Who generated the deepfakes or other AI-generated false content?
- Was there any flagging of the content by social media platforms as false of AI-generated?
- Was any takedown of content by social media platforms (SMPs) flagged as violating the Community Standards of the SMPs?
- Any Links to the Content?

Proactive Disclosures

To curb misinformation and disinformation and to address their impact, proactive disclosures are a critical strategy that States should use during elections. When all election stakeholders proactively disclose information, this lays a foundation for a democratic process, reducing the incidence of information disorders. This should be accompanied by raising awareness among the electorate and promoting fact-checking practices. Appointing authorities of members of the EMB, EMBs, Political parties, Candidates, Law enforcement agencies, Election observers,

[20] UN General Assembly https://documents.un.org/doc/undoc/gen/n22/459/24/pdf/n2245924.pdf

election monitors, Media and Social Media Platforms have a role to disclose information proactively. They can leverage technology to ensure a constant free flow of information to the electorate. Failure to proactively disclose information takes away from an election's record, leading to a conclusion of unfairness.

Paragraph 27.

In its resolution 76/227, the General Assembly highlighted the need for "the dissemination of factual, timely, clear, accessible, multilingual and evidence-based information" and emphasized "the need for all relevant stakeholders to address the challenge of disinformation". Maximizing transparency and access to information is a central requirement for building trust in public institutions, governance and processes. When governments, politicians and public officials operate transparently, maintain regular communication with the people they serve, provide timely, evidence based information and are open to scrutiny, they contribute to building legitimate, accountable, effective institutions, which can reinforce public trust in the information system and reduce susceptibility of people and communities to disinformation.[21] UN General Assembly A/77/287

The Guidelines call on *Election Management Bodies* (EMBs) to proactively disclose information at all stages of the electoral process, specifying certain categories of information that should be disclosed before, during and after elections. In tracking proactive disclosures of information, please see what to monitor below from EMBs:

- When did the EMB announce the date of the Elections in relation to the election?
- What platforms did the EMB use to make the disclosure?
- Which platforms were primarily used in the election-related disclosures?
- What information was disclosed explicitly and was it in good time?
- How often was the EMB disclosing Information?
- How precise were the disclosures (clarity of disclosures/avoidance of vagueness)?

In tracking proactive disclosures of information, please see what to monitor below from government agencies:

- Is the government using technology in the Election?
- What technology is being used or deployed?
- For what purposes is the technology being deployed in the Election?
- Is there proactive disclosure on the procurement of the technology being used?
- Did the government proactively disclose to key election stakeholders and voters on the procurement and use of the technology?

[21]

Accountability Mechanisms

In addition to monitoring digital rights during elections, it is essential to identify the reporting mechanisms for accountability purposes. The following are ways to ensure digital rights violations are addressed in real time.

- Report violations to the national human rights institution in your country.
- Report to reputable human rights organisations that can address concerns through advocacy and litigation efforts.
- Submit reports for immediate action to Paradigm Initiative through the reporting platform - Ripoti.
- Submit a Monitoring Report to Paradigm Initiative and any collaborating partner in Annexure A format on partners@paradigmhq.org .

RESOURCES

1. ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa
2. AU
3. ACHPR Resolution 580 on Internet Shutdowns and Elections in Africa
4. African Charter on Democracy, Elections and Good Governance https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/guidelines_on_access_to_information_and_elections_in_africa_en.pdf
5. Netblocks https://netblocks.org/ and follow on X at https://x.com/netblocks?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor .
6. Ayeta Digital Rights Toolkit A Paradigm Initiative Digital Security Toolkit – Ayeta unpacks digital rights and digital security solutions
7. Report all Digital Rights violations on Ripoti.
8. If you need a VPN, send a request to vpn@paradigmhq.org.
9. Open Observatory of Network Interference (OONI) Probe —Test the blocking of websites and apps and measure the speed and performance of your network using Ooni.
10. Privacy International Data and Elections Checklist https://privacyinternational.org/sites/default/files/2023-11/Data%20and%20elections%20checklist_Update_Final_21Nov_Reduced.pdf

ANNEXURE 1: MONITORING FORM

Name:

Organisation/Affiliation:

Role/sector (Journalist/CSO/Researcher, etc.)

Reporting Period (e.g June 2025 or June -July 2025) :

NB: You can answer in any of the following ways:

□ Yes - Provide details on your response, including links, where possible.

□ No - Provide details where relevant for clarity.

□ No available information—Where there is no way of ascertaining what is asked, you can answer this way and provide details for clarity.

Internet Shutdowns

- Is there a slowdown in internet access or a total blackout?
- When did it start and end? (If ongoing, you can indicate it as still pending. Also, report this occurrence on Ripoti.)
- If so, what websites are affected? (All websites or specific platforms like X or Facebook?)
- Did the government communicate a blocking of internet access or order it?
- If so, is there a link you can share to the communication/order?
- Which government agency ordered it?
- Which law did they rely on?
- Did the internet service providers (ISPs) communicate that they will block internet access?
- If so, any links to this?

Data Protection

- Are there reports of misuse or unauthorised access?
- Are citizens getting unsolicited political messages through text messages or other communications technologies?
- Which networks are these messages being sent from?
- Has there been any data breach of the voters' roll or other personal data related to elections online?
- Is there a Data Protection law in your country addressing using personal data and biometric technologies during elections?
- Is the Election Management Body sharing adequate information on using data and biometric technologies to prevent misinformation and disinformation?
- Any misinformation or disinformation about the use of biometric technologies?
- Any links to the reports?

Hacking, Surveillance & Online Harassment

- Are there reports of hacking or surveillance against journalists, activists, and opposition.
- Reports on deployment of spyware or tracking technologies.
- Are there any reports on coordinated online harassment or intimidation.
- Was there any mention of targeted mass communications surveillance during elections?
- Was there any targeted surveillance on any individuals or specific groups?
- If so, where was this communicated?
- Which government agencies are responsible for this surveillance?
- Was there any procurement or deployment or surveillance tools?
- Was there any deployment of public space surveillance tools during the period?
- What tools were deployed, if any?
- Was there any arbitrary seizure of digital technologies for voters, journalists, human rights defenders, election observers/monitors, civil society organisations etc?
- Any links?

Report on Freedom of Expression

- Are there any arrests of individuals for political speech online?
- Who is specifically targeted/affected?
- Is there any disclosure on the charges they are facing?
- Are the arrests in terms of a law in the country discourse (insult laws, false news, inciting public violence, criminal defamation, etc.?
- Which law and provision allows the arrest if known?

Information Integrity

- Was there any use of politically oriented deepfakes and AI-generated misleading content online before, during, and after the elections?
- Who generated the deepfakes or other AI-generated false content?
- Was there any flagging of the content by social media platforms as false or AI-generated?
- Was any takedown of content by social media platforms (SMPs) flagged as violating the Community Standards of the SMPs?
- Any Links to the Content?

Report on Proactive Disclosures of Technology in Elections

- When did the Election Management Body announce the date of the Elections in relation to the election?
- What platforms did the EMB use to make the disclosure?
- Which platforms were mostly used in the election-related disclosures?
- What information was specifically disclosed and was it timely?
- How often was the EMB disclosing Information?
- How precise were the disclosures (clarity of disclosures/avoidance of vagueness)?

Tracking Technology and Elections

- Is the government using technology in the Election?
- What technology is being used or deployed?
- For what purposes is the technology being deployed in the Election?
- Is there proactive disclosure on the procurement of the technology being used?
- Did the government proactively disclose to key elections stakeholders and voters on the procurement and use of the technology?

ANNEXURE B: SECURITY FOR ELECTION OBSERVERS AND MONITORS

	Before Election	During Election	After Election
Digital Safety Tips	- Keep your devices updated. Install antivirus software and ensure firewalls are enabled. - Use Strong Passwords and enable Two-Factor Authentication (2FA) for digital platform accounts. - For secure communication, use end-to-end encrypted messaging apps like Signal for sensitive communications. - Don't click on suspicious links. Double-check who sent you emails and files.	- Avoid using public Wi-Fi. Use mobile data or a trusted Virtual Private Network (VPN). - For data protection, regularly back up documentation (photos, reports) to secure cloud storage or encrypted drives. - Turn off live location sharing on apps and avoid posting your real-time location.	- Encrypt and safely store all data collected. Don't keep it on shared or public devices. - Use secure platforms for reporting and debriefing meetings. - Change passwords for any accounts or devices used during the election.
Physical Safety Tips	- Risk Assessment: Identify high-risk areas and plan observer routes accordingly. - It's essential to have an official observer identification that is valid and accessible. - Save the emergency contact on your device and in a notebook. Share your location and schedule with trusted contacts.	- Stay alert to your surroundings. Avoid confrontation or high-tension crowds. - Survey the area when you arrive and plan an exit route in case of tension or emergency.	- Log and report any threats or incidents encountered during the election. - Plan an exit strategy, especially in regions with post-election unrest.

ADDITIONAL DIGITAL SAFETY TIPS

Google Authenticator (*You can use this tool to generate 2 Factor Authentication (2FA) codes for secure logins.)*

How to use:

- On your mobile device, install Google Authenticator from the Google Play Store or App Store. Visit this link to learn more about Google Authenticator and how to install: Android and iPhone, /iPad
- Open the app and scan 2FA QR codes from your online accounts.
- Use the generated codes to complete logins.

Signal (*For a more secure communication, you can use this platform for encrypted messaging, voice, and video calls.)*

How to use:

1. Go to signal.org and download for your device (Android, iOS, or desktop).
2. Install the app and verify with your phone number.
3. Set a PIN and start messaging securely.

Tor Browser (*For privacy, anonymity, and safe browsing.)*

How to use:

- Download from torproject.org.
- Install and open the browser.
- Browse securely without revealing your identity or location.

ProtonMail (*It sends secure, end-to-end encrypted emails.)*

How to use:

- Go to proton.me.
- Sign up for a free encrypted email account.
- Use web or mobile app to send protected emails.

Proton Drive (*End-to-end encrypted cloud storage from the makers of ProtonMail.)*

- Go to proton.me/drive.
- Create a free Proton account (or log in if you have one).
- Use the web interface or install the app to upload your files.
- Files are encrypted automatically. You can organise them in folders and share securely.
- Turn on two-factor authentication from your Proton account settings for extra protection.

VeraCrypt (*It creates encrypted volumes on your computer or USB.)*

How to use:

- Download VeraCrypt from veracrypt.fr
- Install and open the app.
- Click “Create Volume”, follow the wizard, and choose a strong password.

Have I Been Pwned (*Checks if your email or phone has been exposed in data breaches.)*

How to use:

- Go to haveibeenpwned.com.
- Enter your email or phone number.
- Receive results and change passwords if needed.