

15 September 2026

English only

Human Rights Council

Sixty-third session

Human rights standards and guidelines on the use of digital technologies in electoral processes

OHCHR – Privacy International – The Carter Center

Summary

The growing reliance on digital and data-driven technologies, including artificial intelligence, across societies, as well as in electoral processes, has significantly transformed election management and political campaigning. This evolving landscape requires attention to how to apply established human rights norms and ensuring effective protection of rights, including the rights to privacy and, freedom of expression including access to information. Against this backdrop, informed by best practice and consultations with representatives from UN bodies, civil society, academia, and election oversight institutions the Office of the UN High Commissioner for Human Rights, Privacy International, and The Carter Center have developed practical guidance for States (including election management bodies and data protection authorities), businesses and political actors on the human rights compliant use of technologies throughout the electoral cycle.

Contents

Introduction.....	3
PART I: Human Rights Standards.....	5
A. Human rights obligations for States to respect, protect and fulfil	5
Right to participation in public affairs	5
Right to freedom of expression including access to information	6
Rights to freedom of peaceful assembly and of association	6
Right to privacy	7
Right to an effective remedy	7
Right to equality and prohibition against discrimination	7
Right to education.....	8
B. Responsibilities of businesses and State obligation to protect human rights from third-party violations	8
PART II. Guidelines on the application of human rights to technologies used in electoral processes	9
Registration and voting processes mediated by technology.....	10
Voter registration, identification and authentication.....	11
Additional safeguards for the use of biometrics data.....	12
Internet voting.....	13
Right to information and transparency in electoral processes.....	13
Transparency, auditability and accountability in the procurement of election technologies	13
Use of personal information by and for political campaigns	14
Political advertising, use of artificial intelligence, micro-targeting, and transparency	15

Introduction

The use of technologies in electoral processes is not merely a technical or administrative choice. Electoral processes involve core acts of governance, and their design and implementation engage a range of human rights. The use of technologies in elections must comply with international human rights law, which provides a legally binding framework that conditions State conduct and guides the actions of other relevant actors.

The growing reliance on digital and data-driven technologies, including artificial intelligence (AI), across societies, as well as in electoral processes, has significantly transformed election management and political campaigning. These technologies increasingly shape voter registration, voting, counting and results transmission, political communication and public participation. At the same time, as electoral technologies become embedded in the wider digital environment, they have blurred traditional distinctions between stages of the electoral process and between electoral infrastructure and the broader information ecosystem. This shift gives rise to new and complex challenges for applying established human rights norms and ensuring effective protection of rights in practice.

Under international human rights law, States are the primary duty bearers and are obliged to respect, protect, and fulfil human rights in electoral processes, including if, when and how technologies are used. These obligations apply to all branches of the State and to State bodies at all levels (federal/ national, provincial, and local), including, among others, election management bodies and data protection authorities. The State obligation to protect human rights against infringement by non-state actors encompasses the duty to regulate and oversee the conduct of business enterprises that may interfere with human rights.

In addition, business enterprises (hereafter businesses) have an independent responsibility to respect human rights, in line with the UN Guiding Principles on Business and Human Rights (UNGPs). This expects them to avoid causing or contributing to human rights abuses and to identify, prevent, mitigate and address adverse human rights impacts with which they may be directly or indirectly involved.

These human rights standards are set out in more detail in **Part I**. This section identifies a selection of central human rights relevant for electoral processes and briefly outlines their core legally binding content as established in international human rights law and interpreted by treaty bodies. It also highlights the responsibilities of businesses and the obligation of States to protect human rights from third-party violations.

Building on this foundation, **Part II** sets out recommended guidelines for States (including electoral management bodies) businesses, and political actors to effectively operationalise these international human rights standards with respect to digital technologies for the purposes of voter registration identification and authentication, use of biometrics data, procurement, use of personal information, political advertising, and addressing disinformation and hate speech.

These guidelines aim to provide practical recommendations on the human rights compliant use of technologies in electoral processes, throughout the electoral cycle. The guidelines are informed by relevant best practices. They should not be interpreted as limiting the application of more protective standards found in other regional or national instruments. Given the breadth and complexity of electoral processes and the range of human rights questions that may arise, this document is not intended to be exhaustive. This document was developed by the Office of the UN High Commissioner for Human Rights, Privacy International, and The Carter Center, in consultation with representatives from UN bodies, civil society, academia, and election oversight institutions. Further background information and an annotated bibliography are included in the [Summary of an Expert Consultation on Human Rights, Digital Technologies, and Elections](#).

Definitions

Personal data means any information relating to an identified or identifiable individual.

Biometric data is a type of personal data that relates to someone's physical, biological, physiological or behavioural characteristics, such as someone's DNA, voice, facial image, fingerprints, iris patterns, etc.

Digital technologies for the purposes of these guidelines refer to digital and data-driven technologies that play a key role in electoral processes and are used for the purpose of collecting, processing, storing and sharing of data

Electoral Management Bodies refer to organizations or authorities legally responsible for the governance and administration of key aspects of elections, such as compiling voter registers and lists, conducting polling, vote counting and tabulating as well as others.

Micro-targeting refers to profiling enabled through the collection of personal data and its use to target specific messages and context to different groups.

Political campaign organisations refer to electoral coalitions and other permanent or temporary entities, not limited to political parties, conducting political campaigns around elections or referenda.

Scraping refers to automated, unauthorized, large-scale extraction of data from websites, including personal data that is accessible on platforms, into a structured format.

Voter registers are the official lists of all persons eligible to vote and the underlying data processed in these registers; while **voter list** refers to the list of all persons registered to vote in a specific electoral district or constituency for an election.

PART I: Human Rights Standards

A. Human rights obligations for States to respect, protect and fulfil

The notion of democratic elections is anchored in the human right to take part in the conduct of public affairs (Article 25 of the International Covenant on Civil and Political Rights) and rooted in the fundamental principle of self-determination (Article 1 common to the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights). Electoral processes and election management directly involve several interrelated and interdependent human rights standards, which apply both online and offline, throughout the electoral cycle, and guide whether and under what conditions technology should be used and regulated.

This section includes key international human rights standards that form the foundation for the guidelines that follow in Part II.

Right to participation in public affairs

- a) States must respect and ensure the right to take part in the conduct of public affairs, including the right to stand for election and to vote in “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”. (Article 25b, International Covenant on Civil and Political Rights (ICCPR)). The principle of one person, one vote, must apply, and States must guarantee and give effect to the free expression of the will of the electors (Human Rights Committee, General Comment 25, paras. 19, 21). The results of genuine elections should be respected and implemented. Any limitation to the right to vote must be established by law and subject only to reasonable restrictions. (Human Rights Committee, General Comment 25, paras. 10 and 19).
- b) States must take effective measures to ensure that all persons entitled to vote can exercise their right to vote. Where registration of voters is required, States should facilitate it and not impose obstacles to such registration. Where residence requirements apply to voter registration, they must be reasonable and should not be imposed in such a way as to exclude the homeless from the right to vote (Human Rights Committee, General Comment 25, para. 11).
- c) States should establish an independent electoral authority to supervise the electoral process and ensure it is conducted fairly, impartially, and in accordance with established laws that are compatible with the ICCPR. Voters must be protected from interference with registration or voting, as well as intimidation or coercion, including compulsion to disclose how they intend to vote or how they voted. Independent scrutiny of voting and counting processes must be ensured, along with access to judicial review for any human rights violations (Human Rights Committee, General Comment 25, paras. 20, 11).
- d) The right to participate in public affairs cannot be considered in a vacuum. The effective exercise of this right requires an enabling environment where all human rights, in particular the rights to equality and non-discrimination, are fully enjoyed by all individuals.
- e) Election observation is in itself part of the right to take part in the conduct of public affairs. To help ensure voter confidence, independent scrutiny of the voting and counting process is required. Accredited observers must be afforded freedom of movement and access, including to polling stations, and protected from harm and interference in their official duties (Human Rights Committee, General Comment 25, para. 20, Declaration of Principles for International Electoral Observation, paras 16 and 12).

Right to freedom of expression including access to information

f) Freedom of opinion and expression and freedom of peaceful assembly and of association are essential conditions for the effective exercise of the right to vote and must be fully protected (Human Rights Committee, General Comment 25, paras. 12, 8).

g) Article 19(2) of the ICCPR guarantees the right to freedom of expression, including access to information. Restrictions on freedom of expression must meet the high threshold of Article 19(3) which requires that they be provided by law and be necessary and proportionate for the legitimate aim of respecting the rights or reputations of others, or for protecting national security, public order, public health, or morals. The principle of legality means that the scope, meaning and effect of the law must be clear, precise and public (Human Rights Committee, General Comment 34, para. 25).

h) The State must protect the free communication of information and ideas about public and political issues between citizens, candidates and elected representatives, including through:

- Promoting free and independent media able to comment on public issues without censorship;
- Taking measures to prevent such control of the media as would interfere with the right of everyone to freedom of expression, including by not exercising monopoly control and promoting plurality of the media, as well as addressing undue media dominance or concentration by privately controlled media groups in monopolistic situations that may be harmful to a diversity of sources and views. (Human Rights Committee, General Comment 34, paras 13 and 40)

i) In line with relevant international standards, the State must ensure transparency in campaign financing (United Nations Convention against Corruption, art. 7 (3)). Reasonable limitations on campaign expenditure may be justified where this is necessary to ensure that the free choice of voters is not undermined or the democratic process distorted by the disproportionate expenditure on behalf of any candidate or party (Human Rights Committee, General Comment 25, para. 19).

j) While guaranteeing the right to express unpopular/ offensive/critical and alternative views, States must prohibit advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (art. 20(2), ICCPR). Any prohibition should be consistent with the right to freedom of expression and the Rabat Plan of Action (A/HRC/22/17/Add.4).

Rights to freedom of peaceful assembly and of association

k) States must respect, protect and fulfil the right to freedom of peaceful assembly (art. 21, ICCPR) – including online – not only in relation to political campaign rallies and gatherings, but also as an enabling right for ensuring the broad and inclusive participation in the electoral process and exercise of the right to vote in genuine elections.

l) Any restrictions on the right to freedom of peaceful assembly must be consistent with article 21 of the ICCPR which requires they be provided by law, necessary in a democratic society, and proportionate to the legitimate aim of national security or public order, or to protecting public health or the rights and freedoms of others. The imposition of any restrictions should be guided by the objective of facilitating the right, rather than seeking unnecessary and disproportionate limitations on it (Human Rights Committee, General Comment 37, para. 36).

m) Given the significant role that political campaign organisations and civil society organisations play in the conduct of public affairs and the election process, States must not only respect the exercise of the right to freedom of association and not unduly interfere with

its exercise but must also actively protect and facilitate exercise of this right (art. 22, ICCPR). This includes the right to establish and join associations, carrying out their legitimate election-related and political participation activities, including the ability to seek, access and use resources, free from intimidation, retaliation and undue restrictions.

n) Political parties and party membership play a significant role in the conduct of public affairs and the electoral process. States should ensure that in their internal management, political parties respect the applicable provisions of article 25 of the ICCPR (Human Rights Committee, General Comment 25, para. 26). Any restrictions on political parties should strictly be in compliance with article 22(2) of the ICCPR.

Right to privacy

o) States must respect, protect and fulfil the right to privacy, guaranteed in article 17 of the ICCPR. The right to privacy is fundamental in a democratic society and increasingly important in a data-driven world. The right to privacy includes the principles of data protection, including in jurisdictions and under international instruments that do not recognise data protection as an independent right.

p) Any interference with the right to privacy is permissible only if it is neither arbitrary nor unlawful, and meets the requirements of legitimate aim, legality, necessity and proportionality (art. 17, ICCPR and Human Rights Committee, General Comment 16, paras. 3-4, and 8).

q) The right to privacy guaranteed under international human rights law covers informational privacy and extends to correspondence and personal information on computers, data banks, and other devices, whether held by public authorities or private individuals or bodies (Human Rights Committee, General Comment 16, paras. 8 and 10).

r) Data collection and processing of data relating to personal information or a person's private life involves the right to privacy, including in the context of micro-targeting and large-scale data extraction, and, absent the individual's consent or another valid legal basis, constitutes an interference with it. States must take effective measures to ensure that such information does not fall into the hands of persons who are not authorized by law to receive, process, and use it, and is never used for purposes incompatible with the ICCPR (Human Rights Committee, General Comment 16, para. 10). Where unauthorized access nonetheless occurs, States must act promptly to halt the interference, contain its effects, and notify the affected individuals. The duty to protect privacy does not end at prevention; it extends to remediation once a breach has taken place. States must further ensure accountability for any breach of privacy, including an effective investigation into how the unauthorized access occurred, sanction of those responsible, and an effective remedy for the individuals whose data was compromised (ICCPR, art. 2(3); Human Rights Committee, General Comment 31).

Right to an effective remedy

s) States must, as required by article 2(3) of the ICCPR, put in place a framework that prevents human rights violations, holds those responsible to account, and provides remedies for both actions and omissions by the State and non-State actors. In line with this obligation as well as under international standards on business and human rights, States must ensure that those affected by business-related human rights abuses within their territory/jurisdiction have access to remedy.

Right to equality and prohibition against discrimination

t) Article 26 of the ICCPR guarantees the right to equality, and article 2 entrenches the prohibition against discrimination. While the State can limit the right to participation in public affairs to citizens, it must guarantee all other rights, including the rights to privacy, freedom of expression, peaceful assembly, and freedom of association, without distinction of

any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Right to education

u) Education is both a human right in itself and an indispensable means of realizing other human rights (Committee on ESCR, Comment 13, para. 1). This includes the right to participation in public affairs. Voter education and registration campaigns are necessary to ensure the effective exercise of the right to participate in public affairs by an informed community (Human Rights Committee, General Comment 25, para. 11).

B. Responsibilities of businesses and State obligation to protect human rights from third-party violations

States

a) Under its duty to protect, the State is required to protect individuals from human rights abuses by third parties, including businesses, and to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication. When abuses occur, States must take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that those affected have access to effective remedy (art. 2(3), ICCPR, UNGPs Principle 1, 25-29).

b) States have a duty to ensure that businesses, political parties and other political campaign organisations respect human rights.

c) States should establish and enforce regulatory frameworks requiring businesses, political parties, political campaign organisations and other entities involved in electoral processes to conduct human rights due diligence in relation to their development and use of digital technologies. Such due diligence should enable them to identify, prevent and mitigate actual and potential human rights impacts throughout the technology lifecycle. Regulatory frameworks should also require enhanced due diligence for high-risk use cases and contexts. In addition, they should require adherence to high standards of transparency, accountability and robust data governance.

Businesses

d) Businesses have responsibilities under the UNGPs and other international standards to identify, prevent, mitigate, and redress adverse human rights impacts that they cause or contribute to through their own activities, or that are directly linked to their operations, products, or services by their business relationships, including when they design, develop, manufacture, configure, and operate election technologies. They should carry out human rights due diligence, including assessing actual and potential human rights impacts. (UNGP, Principle 11, 13, 17, 18, 19).

e) As part of this responsibility under the UNGPs, businesses should safeguard against government overreach by having policies and practices in place to address State demands that carry a risk of breaching human rights law and norms. The responsibility to respect human rights may mean that businesses should challenge such requests as appropriate.

f) Businesses, including online platforms, should adopt meaningful transparency measures to communicate their election integrity efforts in relevant local languages in addition to English.

g) Businesses, including online platforms, should consult and engage proactively with stakeholders including Election Management Bodies, the media, civil society organisations and the United Nations human rights system, on a regular basis and especially prior to major policy changes.

PART II.: Guidelines on the application of human rights to technologies used in electoral processes

Technologies used in electoral processes must be designed, configured, deployed and regulated in a manner consistent with international human rights law. This requires clear legal frameworks, effective oversight and remedies to prevent, stop, and redress human rights violations arising from digital voter registers, biometric identification, electronic voting, results transmission systems and online campaigning tools. To give effect to their obligations under international human rights laws (see Part I), States should conduct human rights due diligence, including human rights impact assessments, before and during the use of digital technologies, and engage in broad outreach and meaningful consultations with a range of stakeholders, including civil society and affected groups. In view of developments in both the technology and human rights impacts, State entities, including Election Management Bodies and other bodies, should continuously re-assess and evolve the measures needed to ensure an enabling environment for political participation. The use of technologies that violate human rights or the use of technology for intimidation – including of civil society actors, election observers, political opposition, as well as voters – must be prohibited.

Non-discrimination and the right to privacy are particularly salient for technologies used in electoral processes because such technologies directly mediate access to political participation and can reshape power relations among the State, voters and private actors.

Digital technologies are not just transforming what we see online. They are transforming the conditions under which voters decide. Electoral technologies frequently involve the large-scale collection, processing and storage of highly sensitive personal data, including biometric data, political opinions, voter behaviour and location information. In the electoral context, violations of privacy carry heightened risks: misuse or unauthorized access to voter data can enable surveillance, profiling, intimidation, or chilling of political participation and freedom of expression and association. Weak data protection safeguards may also enable undue micro-targeting, or unlawful interference by State or non-State actors. Where voter data is repurposed beyond its original electoral function, or shared with security, intelligence or commercial actors, the secrecy of the ballot and the autonomy of voters are fundamentally compromised. Robust privacy protections are therefore essential to preserve the integrity of democratic processes themselves. States must safeguard the right to privacy by ensuring that personal data is lawfully collected only when necessary and proportionate to legitimate electoral purposes, securely processed, stored in a manner that does not link the voter to their vote, and not retained or repurposed in ways that enable surveillance or intimidation of voters.

States must also prevent discrimination, including indirect or algorithmic discrimination, by ensuring that technologies do not disproportionately exclude or disadvantage groups on prohibited grounds. Non-discrimination is critical because digital voter registration systems, biometric identification, algorithmic voter verification and automated constituency mapping can systematically exclude or disadvantage certain groups when poorly designed, inadequately tested or deployed without appropriate safeguards. Groups in often marginalized situations, including older persons, persons with disabilities, ethnic or linguistic minorities, women, persons without stable documentation or those living in poverty or remote areas, may face disproportionate barriers due to unequal access to technology, lower digital literacy, data quality gaps or biased datasets. Ensuring non-discrimination requires active assessment of disparate impacts, inclusive design, accessibility measures and mechanisms for correction and redress.

Businesses have a responsibility to respect human rights wherever they operate, in line with the UN Guiding Principles on Business and Human Rights. Businesses involved in supplying or operating electoral technologies should fulfil this responsibility by conducting rigorous human rights due diligence, including human rights impact assessments, throughout the

technology lifecycle, and cooperating with public authorities to enable transparency, accountability and effective remedy where violations occur. States must adopt and enforce regulations requiring businesses to respect human rights, periodically assess whether those regulations are adequate and address any gaps, and ensure access to effective remedies when violations occur (UNGPs, Principles 1, 3, 25).

The below guidelines are practical recommendations – informed by best practice – aimed at supporting States (including electoral management bodies), businesses, and political actors to ensure that any use of technologies in electoral processes is consistent with the international human rights standards detailed in Part I.

Registration and voting processes mediated by technology

States

1. The process for adopting new technologies for an electoral process can be lengthy. Election Management Bodies should develop a clear timeline in relation to the timing of the election where the technology would be deployed and should include adequate opportunities for consultations, quality assurance and risk assessments.
2. Election Management Bodies should consult with specialized human rights agencies, such as national human rights institutions or independent experts, to perform a human rights impact study to assess the potential risks of exclusion, discrimination or possible disadvantages that technology may pose for specific regions, communities or groups, including rural communities, indigenous people, minorities, people with disabilities and others.
3. Election Management Bodies should ensure that the design and deployment of election technology promotes accessibility and universal suffrage. This includes easy, user-friendly instructions and procedures, disability access, and multilingual support for linguistic minorities. In addition, where voting is digitalized, alternative, non-digital options should be provided to guarantee the inclusion of all eligible voters.
4. Election Management Bodies should ensure that election technology guarantees the accurate tabulation of votes and provides results that reflect the expressed will of the electors according to the one person, one vote principle.
5. Election Management Bodies should ensure that clear mechanisms for addressing complaints of violation of electoral rights, including those related to data protection and privacy, discrimination or unequal treatment, are clearly established and easily accessible to voters and organizations.
6. Election Management Bodies should put in place contingency plans for election technologies. Contingency plans should include alternatives that are independent of the technology used and are tailored towards addressing gaps that may be occasioned by limited infrastructure such as limited internet connectivity, or power. This should include, physical backup systems, analog systems, and paper options, with data protection procedures for the transfer of data and information between the alternatives and the technology-based systems that Election Management Bodies deploy.
7. Election technologies should be designed to protect the secrecy of ballots during voting, vote processing, transmission, and storage, including throughout any period of data retention after the vote, to ensure that ballots cannot be linked with the voters who cast them and that voters are able to vote freely without fear of coercion, intimidation, or discrimination.
8. Voter education and awareness-raising processes should include all eligible voters without discrimination based on race, colour, sex, language, religion, political opinion, origin, physical or mental ability, sexual orientation or gender identity, property, birth, or

other status. Voter education should include information on procedures for voters to address violations of the full range of rights implicated in electoral processes. Information about voters' rights and the mechanisms and procedures for remedies should be available in languages that voters can understand and use effectively. Particular efforts should be made to include individuals and groups that are marginalized or discriminated against.

Voter registration, identification and authentication

States

9. Voter registration, identification and authentication of processes and procedures must be governed by national law and regulations consistent with international human rights obligations and standards.

10. Voter registration, identification and authentication are central to protecting the right to vote. Voter registration should aim to include all eligible voters possible to promote universal and equal suffrage.

11. In consultation with civil society, experts and data protection authorities, Election Management Bodies should adopt and publish regulations or internal policies to clarify the application of data privacy standards and procedures to voter registration, identification and authentication

12. Voter registration must be fair, comprehensive, accessible, secure and inclusive. Election Management Bodies should take effective measures, including voter education and awareness raising, to provide people with clear, simple and accessible information about the registration process and the steps they can take to participate. This includes providing adequate time for eligible voters to register.

13. The voter registration process should not include information beyond what is necessary to identify a voter and to determine the person's eligibility to vote. Where the collection of sensitive information, such as ethnicity, race, and political party affiliation, is required by law, such information should be strictly confidential and should not be shared with third parties.

14. Election Management Bodies should implement strong security safeguards, including cybersecurity protocols, to ensure that voters' confidential information is stored and processed securely. These safeguards should meet the standards of applicable data protection law and, where that law exempts or only partially covers electoral or government data processing, should apply equivalent protections regardless. Confidential information should not be stored longer than necessary for the specific purpose pursued and should be promptly and securely destroyed. The safeguards applied should include training of Election Management Bodies personnel on data privacy, security and protection. Safeguards should further include appropriate responses to technical errors, security breaches and cyber-attacks; access controls, confidentiality agreements; and controls on physical access to places and equipment where personal data is stored.

15. The systems and software used for computerized voter registration, voter lists and certification should allow for and be subject to independent scrutiny by authorized oversight bodies, specialized agencies and experts.

16. Election Management Bodies should ensure that candidates, political parties and accredited election observers are able to access and verify the accuracy of the voter lists without undue restrictions in advance of elections. Voter lists should be provided and available in accessible formats. In addition, the procedure for sharing the voter lists with candidates and political parties should be governed by law and should be limited to the purpose of transparency and verification of the process without undue cost.

17. Election Management Bodies should publish or publicly display and provide an adequate timeline for inspection of the voter list. This should include clear procedures for voters to correct, object, and challenge information relating to the registration process or the voter list prior to election day. Procedures put in place for inspection, corrections and challenge should not be unduly burdensome or require financial charges to voters. Appropriate safeguards should also be in place to address frivolous or bad-faith challenges, and to protect voters from arbitrary removal or disenfranchisement.

Additional safeguards for the use of biometrics data

States

18. Biometric systems raise distinct privacy risks: biometric identifiers are permanent and cannot be reissued if compromised; a breach is therefore effectively irreversible. Given these risks, biometric systems should be used in voter registration or verification only when their use is based on law and is necessary and proportionate to a clearly identified electoral need.

19. Election Management Bodies should bear primary responsibility for technologies procured to obtain, store, and process biometric data used for electoral processes. The adoption, procurement, and deployment of biometric technologies should be managed by Election Management Bodies with support from cybersecurity and data protection agencies.

20. Election Management Bodies should consult with parliaments or legislatures, civil society, political parties, experts, and data protection agencies in the adoption of biometric data technologies, allowing adequate time for meaningful consultations as well as the adoption, testing and deployment of biometric technology.

21. Before adopting biometric technology, States should establish the specific needs the technology will address and clearly identify the technical specifications required. States must ensure that any biometric technology they adopt complies with international human rights law and is designed to be transparent, accountable, and auditable. Businesses supplying such technology should design and document it to enable that compliance.

22. As with other technologies used in electoral processes, the process of adopting new biometric data technologies or systems can also be lengthy. Election Management Bodies should develop a clear timeline for adopting biometric technology. This should be in relation to the timing of elections and should allow adequate opportunities to collect biometric data from all eligible voters and to conduct feasibility studies, pilots, testing and certification by relevant agencies.

23. Tests conducted should include security and accuracy tests and should be supported by cyber security, data protection, and other specialized agencies. This should include ongoing monitoring for possible breaches and addressing such breaches in line with international human rights standards. Civil society, candidates and political party representatives should be provided with the opportunity to monitor security and accuracy tests and subsequent application monitoring during rollout as well as regular audits.

24. There should be clear security measures to ensure data protection and data loss prevention. This should include procedures for data control, transfer and duplication checks where offline registration systems, such as physical storage devices, are used to transfer data to an online database due to infrastructural or connectivity limitations that prevent access to the online database. Security measures should ensure procedures to prevent the use of biometric identifiers from identifying and tracking individuals across unrelated systems.

Internet voting

States

25. Internet voting – defined here as the casting of ballots over public networks from uncontrolled environments – raises distinct concerns that set it apart from most other electoral technologies. As with mail-in voting, the remote nature of internet voting makes it difficult to ensure the voter is free from observation, coercion or undue influence at the moment of voting. Verifiability is also significantly harder to as the recording and counting of votes relies on complex technical systems that require advanced levels of technical expertise to assess and verify. Internet voting systems may also expand opportunities for interference by State and non-State actors, including by increasing the number of potential points of vulnerability across voter devices, networks, or the voting infrastructure itself.

26. States considering internet voting should therefore proceed with careful consideration of its specific risks and ensure that the necessary safeguards are effectively implemented and independently verified. Where used, internet voting should be accompanied by robust independent security audits, end-to-end verifiability mechanisms where feasible, alternative voting channels for voters who cannot or do not wish to vote online, and clear procedures for invalidating compromised votes. Internet voting must fully ensure the integrity, secrecy and equality of the vote.

Right to information and transparency in electoral processes

States

27. Election Management Bodies should ensure that information regarding the entire electoral process, including voting operations, are accurate and publicly accessible. This should include information about the technologies used in the electoral process.

28. The vote counting process should be verifiable and subject to future review and audits. The use of voting machines should be grounded in law or Election Management Bodies regulations.

29. Results should be publicly announced and published in a timely manner and should be publicly announced and posted at the polling station level.

30. Political party representatives, candidates, and accredited election observers should be able to access and comment on all parts of the electoral process, including pre-election day processes, polling, tabulation, and transmission of results.

Transparency, auditability and accountability in the procurement of election technologies

States

31. The process of procuring election technologies should be transparent and conducted in accordance with applicable procurement laws designed to prevent corruption and to promote the use of competitive processes and public tenders.

32. Election Management Bodies decision-making about procurement should promote transparency by ensuring public participation, particularly for civil society and political parties, in the procurement process with clear safeguards against reliance on intellectual property, trade secrets and non-disclosure agreements as potential barriers to access to procurement information. Procurement information and documents should also be made publicly available.

33. The technology systems procured, while meeting security, technical and operational purposes, should allow for scrutiny of the electoral process and results by independent experts, auditors and accredited election observers.

34. The roles and responsibilities of technology vendors as well as their relationship with Election Management Bodies and other bodies, such as certification agencies, should be clearly defined, with adequate mechanisms for their management and oversight.

35. Legislation and regulations governing data ownership, access, transfer, and destruction should be clearly incorporated into agreements or contracts with technology vendors with clear prohibitions against using Election Management Bodies data for artificial intelligence training or any other purpose beyond the narrow scope of the authorized use.

36. Election Management Bodies should manage and supervise the execution of contracts with technology vendors to ensure changes to election technologies or access, transfer, and destruction of data by vendors are authorized in advance.

Use of personal information by and for political campaigns

Political actors – at times closely intertwined with both businesses and State actors – are also key stakeholders in this context. Political parties, candidates and other campaign organizations increasingly rely on data-driven technologies to communicate with, influence, and target voters. Human rights standards should therefore guide political actors in their reliance on such technologies, as well as the responsibilities of businesses, such as online platforms and data analytics providers that enable or facilitate these practices.

States

37. States should ensure that data protection laws are fully applicable and applied to the processing of personal data by political parties and other political campaign organisations.

38. Laws should ensure that individuals a) can obtain, free of charge, confirmation of the processing of personal data relating to them; b) can access those data in an intelligible form, including any ‘profiling’ and ‘scoring’ that measures voters’ political opinions; c) are informed on how their personal information was obtained and from what source; d) can object to the processing of data on them and request rectification or erasure, if the data is inaccurate, obsolete or incomplete (and, where appropriate, the unconditional erasure or removal of the personal data processed for political marketing purposes); e) are informed about the reasoning underlying the processing of their personal data by political campaigns.

39. Election Management Bodies and/or relevant authorities, in consultation with data protection authorities, experts and civil society organisations, should develop guidelines for political parties and other political campaign organisations on human rights compliant use of technologies in election campaigns.

Political parties, campaign organizations and businesses

40. Political parties and other political campaign organisations should adopt and publish data protection policies and binding internal policies governing the use of digital campaigning activities and tools, including voter profiling, AI, data analytics, prediction, and targeting of (potential) voters.

41. Political parties and other political campaign organisations should carry out human rights impact assessments and data protection audits, to assess the likely impact of intended data processing on the human rights of voters, prior to collection and the commencement of data processing, and should design the data processing in such a manner as to prevent or minimise the risk of interference with these rights. When conducting human rights impact assessments, political parties, political campaign organizations and businesses should also consider whether the processing is in the best interests of broader democratic values and the integrity of democratic elections.

42. Political parties, other political campaign organisations and businesses processing personal data should facilitate the exercise of data rights by individuals (including providing

information about how their data is processed and providing access and allowing for its updating and erasure) and publish mechanisms and procedures for reporting and responding to concerns.

43. Political parties and other political campaign organisations should apply appropriate security measures to ensure voters' data is protected to the highest standards both at rest and in transit, against unauthorized access to or disclosure of personal data. Security measures should consider the current state of the art data-security methods and techniques in the field of data processing. These measures should include training in privacy and security, including how to respond when a technical error occurs or a cyberattack is perpetrated; access controls; confidentiality agreements; and controls on physical access to places and equipment where personal data is stored.

Political advertising, use of artificial intelligence, micro-targeting, and transparency

States

44. States should create an enabling space for freedom of expression, including the right to seek, receive and impart ideas of all kinds and through any media of choice. States should develop multi-stakeholder, human rights-based strategies to address disinformation in electoral contexts, and in this regard promote an independent, pluralistic and diverse media, independent factchecking, and promote the digital and media literacy of the electorate.

45. States, particularly Election Management Bodies and/or relevant authorities, should set up legitimate, accessible, predictable, equitable, transparent, rights-compatible mechanisms for individuals to report political advertising, micro-targeting, disinformation campaigns and other practices that may affect the integrity of elections.

46. States should by law require that political parties and other political campaign organisations carry out full human rights due diligence before using the digital technology services provided by businesses and/or using personal data provided by businesses. Such due diligence should include human rights impact assessments and other measures to ensure the technologies are rigorously assessed and mitigated for bias, and that the data is obtained lawfully with practices compliant with data protection laws.

47. States should consider legislative steps, such as strengthened data protection, to address risks from micro-targeting, including voter discrimination and disenfranchisement, a possible chilling of political participation, and weakening of election integrity.

48. States should by law require political parties and other political campaign organisations to be transparent about their data processing activities, including what personal data they process, how they collect people's data and their profiling practices.

49. Geolocation tracking or geo-fencing to identify the location of a specific individual or for profiling purposes present significant interference with the right to privacy and other human rights. States should legislate to ensure that such services are only deployed pursuant to an appropriate legal basis and are not deployed by default but only on the basis of informed consent freely given by the individuals concerned.

50. States should by law prohibit businesses, political parties and other political campaign actors from engaging in the large-scale, automated collection ("scraping") of personal data from the internet or social media platforms without valid consent or another lawful basis, for the purposes of creating, enriching or inferring profiles of individual voters for political targeting, microtargeting or other campaign purposes.

51. States should by law regulate the use of AI technologies by political campaigns by, prohibiting specific uses of AI that pose a high risk of violating international human rights

law, e.g. where there is use of biometric data to deduce or infer political opinions or other sensitive information.

52. States should further require by law the adoption of measures to mitigate the emerging risks that AI technologies may pose to human rights and the fairness and integrity of the electoral process, such as AI-generated disinformation including deepfakes (realistic but false audio or video content created using AI); and consider mandatory disclosure and disclaimers on the use of AI technologies.

53. Election Management Bodies and/or relevant authorities, in consultation with data protection authorities, experts and civil society organisations, should develop guidelines for political parties and other political campaign organisations and businesses on human rights impact and risk assessments of the use of AI technologies in political campaigns.

Political parties, political campaign organizations and businesses

54. Political parties and other political campaign organisations should publish a complete, easily accessible and easily understandable list of any campaign groups or individuals (such as influencers) with whom they have contractual, financial or structured campaigning relationships, including where such actors coordinate or amplify campaign messaging on their behalf.

55. Political parties, other political campaign organisations and businesses providing services to them should not disclose voters' personal data collected during a political campaign to third parties to monetise or otherwise reprocess the data for other purposes. In particular, no personal data should be shared with online communication platforms for the purposes of digital advertising without consent of the individuals concerned.

56. Political parties and other political campaign organisations should ensure that the public can easily recognise political messages and communications, as well as the party or organisation behind them. They should make available on their websites and as part of the communication, information on how individuals can exercise their rights to protect their data and prevent being used for targeted political advertising.

57. Businesses, including online communication platforms, should make publicly available archives of political advertising and other paid for political content, including the ad imprints, the targeting criteria, the timing and location of ad delivery and the amounts paid.

58. Online communication platforms, including social media platforms and chatbot services, should conduct enhanced human rights due diligence proportional to the risk, and impact assessments of content governance policies ahead of elections; adopt meaningful transparency measures to communicate responses to content moderation requests and the application of their content governance policies; and ensure that they invest sufficiently in local languages, contextual expertise and fact-checking resources, including human resources. As part of their due diligence and ahead of elections, platforms should consult affected stakeholders and work with the relevant national authorities and civil society organizations to conduct stress tests ahead of elections.

59. Online communication platforms, including social media platforms and chatbot services, should review their recommender algorithms and monetization systems, ensuring that they promote access to accurate information on the electoral process. They should be transparent regarding the algorithms and safety efforts that they undertake surrounding elections.