Summary of an Experts Consultation on Human Rights, Digital Technologies, and Elections

Meeting occurred in Geneva, Switzerland, Palais Wilson on 21 February 2025

*This document is being issued without formal editing.

How to Cite This Report

U.N. Office of the High Commissioner for Human Rights, Privacy International, and The Carter Center. "Summary of an Experts Consultation on Human Rights, Digital Technologies, and Elections." *The Democracy Program, The Carter Center.* Atlanta, GA. (2025)

The Carter Center
453 John Lewis Freedom Parkway NE
Atlanta, GA 30307-1406

www.cartercenter.org
General Inquiries: (404) 420-5100 or (800) 550-3560
Donor Services: (404) 420-5109

Contents

1 Executive Summary

On 21 February 2025, an expert roundtable convened in Geneva to examine the international human rights implications of digital technologies in elections. The meeting brought together representatives from UN bodies, civil society, academia, and election oversight institutions under the Chatham House Rule to foster open, solution-oriented dialogue. Participants agreed that while digital technologies can improve electoral access and administration, they also pose serious threats to human rights, including privacy, freedom of expression, participation in public affairs, and equality, as well as democratic accountability if left unregulated. Discussions focused on three core areas: the role of national authorities, the conduct of political parties, and the responsibilities of private companies.

The first session examined how electoral management bodies (EMBs) regulate and deploy election technology. Participants emphasized the need for legal frameworks that guarantee data privacy, prevent discrimination, and ensure independent oversight. Concerns were raised about EMBs' reliance on opaque vendor contracts and inadequate audit procedures. The next session focused on political campaigning, highlighting how parties increasingly use personal data and Artificial Intelligence (AI) tools for microtargeting. While European Union (EU) regulations offer some protections, its coverage and enforcement is inconsistent. Participants called for expanded transparency, cross-agency collaboration, and internal accountability within political parties, especially around online voting practices. The closing session turned to the private sector's role, particularly technology vendors and social media platforms. Participants warned of "vendor lock-in," limited accountability, and data fusion risks between state-managed and commercial systems. Calls were made for human rights clauses in procurement, clearer data governance, and stronger platform responsiveness—especially in underrepresented regions.

Session participants stressed the need to embed human rights due diligence, transparency, and consultation throughout the electoral cycle. This report identifies recommendations and resources to support legal and policy reforms aligning electoral technologies with human rights standards.

2 Background

Elections and political campaigns are increasingly mediated by digital technologies in a complex landscape of public and private actors. Whether using social media platforms for political campaigning, AI technologies for content creation and manipulation, biometric registration and authentication of voters (i.e., using physical characteristics such as fingerprints or facial images to verify identity), or e-voting, technology is now infused into the political process. This applies to the use of digital technologies by traditional actors in electoral processes, such as electoral authorities and political parties, but also emerging new actors in this field, including data brokers, voting analytics companies, social media and digital communications platforms, advertising agencies, and other companies. These technologies rely on collecting, storing, and analyzing personal information to operate, thus raising significant human rights concerns and new challenges for ensuring the right to vote and free and fair elections.

The Office of the United Nations High Commissioner for Human Rights (OHCHR), Privacy International (PI), and The Carter Center (TCC) organized a half-day expert roundtable on the human rights implications of the use of digital technologies in the context of elections. The event took place on Friday, 21 February 2025, in a hybrid format with both physical and online participation. The roundtable convened 42 UN human rights experts, international election observers, civil society organizations, academics, and other key stakeholders to identify the main human rights implications of the use of digital technologies in the context of elections. To encourage open dialogue, the meeting was held under the Chatham House Rule, which allows participants to use the information received but prohibits identifying the speaker or their affiliation. The event convened with the following objectives:

1. Develop a shared understanding among participants of the implications of the use of digital technologies on human rights in the context of elections (including the rights to participation in public affairs, privacy, and freedom of expression, as well as institutional aspects such as review, oversight

and accountability).

2. Identify guidance/support available or needed for relevant national authorities (legislative, executive, regulatory bodies) to develop human rights compliant laws and policies regulating the use of digital technologies in elections to ensure the respect and protection of human rights.

3 Summary of the Three Sessions

The three sessions of the expert roundtable addressed distinct but interconnected aspects of how digital technologies affect elections and the realization of human rights. While each session focused on a different actor — national authorities, political parties, and private companies — all underscored the urgency of embedding transparency, accountability, and human rights due diligence (i.e., systematic assessments by governments or companies to identify and mitigate potential human rights harms) into the digital transformation of electoral systems.

The first session, The Role of National Authorities in Governing Digital Elections, examined how national authorities manage digital technologies such as voter registration systems and e-voting. Participants emphasized that poorly designed or inconsistently enforced legal frameworks can enable discrimination, violate privacy, and erode public trust. Discussions highlighted the need for clear procurement rules, independent oversight, and gradual, well-audited rollouts of new technologies. Participants noted that governments that delegate electoral functions to private vendors do not relieve themselves of their human rights obligations.

Digital Campaigning and the Role of Political Parties focused on the practices of political parties and campaign organizations, especially their use of data analytics, AI-generated content, and microtargeted political advertising. Participants discussed how these tools risk undermining electoral integrity and public discourse when used without adequate safeguards. Regulatory advances in the EU were noted,

including the General Data Protection Regulation (GDPR) and upcoming Political Advertisement Act, but enforcement gaps persist. Participants stressed the need for legally binding codes of conduct, year-round regulation of campaigning, and cooperation between electoral and data protection authorities.

The final session, Private Companies and Electoral Technology Responsibilities and Risks, turned to the responsibilities of private companies, both vendors serving election authorities and firms working with political campaigns. The session revealed widespread challenges: vendor lock-in, opacity in technology contracts, limited responsiveness of platforms in lower-income countries, and the growing overlap between vendors handling election infrastructure and those managing campaign data. Participants emphasized the need for stronger public procurement standards, clearer data ownership rules, and more robust mechanisms to ensure corporate accountability, such as the IFES vendor commitments and the UN Guiding Principles on Business and Human Rights.

Across all three sessions, participants agreed that the rapid evolution of digital tools is outpacing existing legal and institutional safeguards. There was strong consensus on the need for updated laws, enforceable standards, and cross-sector collaboration among electoral bodies, regulators, civil society, and private companies. Taken together, the discussions highlighted a critical choice: whether digital technologies will entrench inequality and opacity, or be harnessed to uphold transparency, participation, and human rights in the democratic process.

The remainder of this report is structured as follows. It begins with a detailed summary of the expert sessions, each of which focused on a distinct actor in the digital electoral landscape: national authorities, political parties, and private companies. These summaries identify key challenges, areas of consensus, and concrete recommendations for aligning the use of digital technologies with international human rights standards. To support further analysis and implementation, the report concludes with an annotated bibliography, focusing on the documents highlighted during the expert meeting.

4 Expert Roundtable Session Overviews

4.1 The Role of National Authorities in Governing Digital Elections (Session 1)

This session examined how national authorities manage digital technologies such as voter registration systems and e-voting. Participants emphasized that poorly designed or inconsistently enforced legal frameworks can enable discrimination, violate privacy, and erode public trust. Discussions highlighted the need for clear procurement rules, independent oversight, and gradual, well-audited rollouts of new technologies. Participants broadly agreed that governments that delegate electoral functions to private vendors do not relieve themselves of their human rights obligations.

Interventions highlighted how voter registration processes and e-voting technologies can be manipulated, intentionally or otherwise, to disenfranchise certain groups. Examples drawn from recent United Nations Human Rights Committee concluding observations illustrated these concerns. In the United States, burdensome voter ID laws have restricted access to e-voting, particularly affecting marginalized communities. In Venezuela, under-registration of young voters has led to limited participation. In Pakistan, administrative registration rules requiring voters to declare their religion have been used to discriminate against members of the Ahmadi minority. These cases reflect not a lack of legislation, but its misuse to marginalize populations — raising concerns of compliance with ICCPR Articles 25 (participation), 26 (non-discrimination), 2(3) (effective remedy), and 17 (privacy).

A consistent theme was the inadequacy of data protection laws and oversight mechanisms, particularly in Latin America and the Caribbean. In some countries, EMBs operate outside the jurisdiction of general data -protection frameworks due to their independent constitutional status. This creates ambiguity over who manages voter data, how it is transferred among agencies, and what protocols apply. Even where data-protection laws exist — such as in parts of the EU and Latin America — they are not always effectively enforced in the electoral context.

Participants also expressed concern about the transparency and accountability of technology procurement. EMBs increasingly rely on private vendors for digital tools such as biometric registration systems and vote-counting software. Yet many contracts are governed by non-disclosure agreements that shield essential processes from public scrutiny. Case studies from Colombia and the Dominican Republic illustrated how technological failures and proprietary restrictions have undermined electoral trust and accountability.

There was broad agreement that the introduction of election technology must be gradual, needs-based, and subject to rigorous auditing and human rights due diligence. Proposals included mandatory human rights impact assessments, open-source or accessible code review, and enhanced consultation with civil society. These measures aim to prevent exclusion and strengthen public confidence.

In settings where private companies are entrusted with electoral functions, participants stressed that states remain accountable for human rights compliance under international law and standards. In line with the UN Guiding Principles on Business and Human Rights public procurement processes — especially those involving AI and voter data — must include safeguards to prevent abuses and ensure corporate accountability.

This session underscored that national authorities must not only modernize election systems but also ensure that such modernization strengthens, not weakens, fundamental rights. Key recommendations from the session include:

1. **Legal Reform:** Governments (i.e., regulators in collaboration with legislators) should enact or update legislation on digital election technologies to ensure human rights compliance, including rules on procurement, data ownership, and algorithmic transparency (i.e., ensuring that automated decision-making systems used in elections can be understood, tested, and challenged), and auditability.
2. **Independent Oversight:** Governments should establish or empower independent audit bodies to conduct technical reviews and human rights assessments of digital election systems, with requirements for public disclosure and independent verification.
3. **Data Governance:** Clarify data protection standards that apply to EMBs, and support internal policies on data privacy where legislative gaps exist.

4. **Transparency Protocols:** Limit the use of NDAs in election technology contracts, require publication of technical procedures (e.g., for biometric registration), and promote transparency in vendor relationships.
5. **Pilot Testing:** When new technologies are being introduced, governments should require the adoption of a phased rollouts, supported by feasibility studies, monitoring by independent observers (e.g., civil society groups or international experts), and documented lessons learned.
6. **Capacity Building:** Provide ongoing training for EMB staff in human rights, cybersecurity, and data management, including through partnerships with academic and civil society organizations.

Selected outside sources explained further in annotated bibliography:

- *Human Rights Committee Concluding Observations (U.S., Venezuela, Pakistan):* In highlighting discriminatory practices in voter registration and access to e-voting, participants echoed concerns raised in recent Human Rights Committee reviews of States. These include burdensome voter ID laws in the United States, under-registration of youth in Venezuela, and religion-based registration barriers in Pakistan.
- *Staderini v. Italy:* The importance of procedural safeguards and judicial oversight was underscored by the Committee's decision in Staderini v. Italy, which found that practical barriers to signature authentication effectively undermined the right to participate in public affairs. This case reinforces the obligation to ensure accessibility and legal safeguards in electoral processes.
- *UN Guiding Principles on Business and Human Rights:* Where states delegate electoral functions to private vendors, they retain a duty to ensure that such actors respect human rights. This duty is articulated in the UN Guiding Principles on Business and Human Rights, which call for regulatory measures to prevent business-related rights violations, including in public procurement.

4.2 Digital Campaigning and the Role of Political Parties (Session 2)

This session examined the use of digital technologies in political campaigns, focusing on how political parties and campaign organizations use personal data, microtargeting (tailoring messages to individuals based on their data profiles), and AI tools. Participants explored these practices' human rights implications, including privacy risks, transparency, electoral fairness, and democratic participation.

Speakers highlighted how data-driven campaigning, particularly when based on inferred political views, can undermine democratic values by encouraging voter surveillance and segmenting public discourse. The session opened with a review of European regulatory developments. Under the EU General

Data Protection Regulation (GDPR), political and religious beliefs are classified as sensitive data, and even non-sensitive data becomes protected when used to infer such beliefs. Complementary regulations — including the Digital Services Act (DSA), the forthcoming EU Regulation on the transparency and targeting of political advertising (effective October 2025), and the Artificial Intelligence Act — further restrict targeting based on sensitive data. These rules require political ads to be based on data collected directly from the individual with their informed consent.

Despite these advances, participants warned that enforcement remains inconsistent, and international lawmaking struggles to keep pace with rapidly evolving technologies. Outside the EU, regulatory coverage is even more fragmented. One concern raised was the difficulty of applying existing electoral laws to the phenomenon of "permanent campaigning" — a phenomenon where digital outreach, micro-targeting, and online political content continue year-round, often beyond the scope of formal campaign periods and ordinary communication. Some participants referenced the post-2016 revelations around Cambridge Analytica as the origin of heightened scrutiny on voter profiling and permanent campaigning. In such cases, key protections — such as transparency about who pays for or targets advertisements — are often evaded. These practices underpin the recent legal and normative push for stricter data regulation for political campaigning.

The use of AI in campaigns was identified as increasing and under-regulated. Participants described emerging risks related to AI-generated disinformation, deepfakes (realistic but false audio or video content created using artificial intelligence), and automated dissemination of targeted content. While some propose regulating AI tool creators, others suggest focusing on political actors and mandating labeling of AI-generated content and promoting digital provenance — the ability to trace the origin and editing history of digital media to verify authenticity. Both approaches face technical and, perhaps, legal challenges.

Political parties' internal use of technology, particularly online voting to make key policy decisions,

was also flagged as an overlooked risk. In Spain, for instance, political parties use internet voting to determine leadership and legislative positions, yet these processes remain outside most legal or technical oversight. Participants acknowledged the tension between regulating party conduct and respecting freedom of association but agreed that transparency and accountability within parties must improve.

Participants called for increased collaboration between EMBs and data protection authorities to avoid gaps in the enforcement of data protection laws in the context of elections. These institutions often operate in isolation: EMBs understand electoral processes but lack expertise in data protection, while data regulators are equipped to handle privacy but seldom engage with political campaigning.

This session clarified that protecting electoral integrity in the digital age requires legal reform and cultural change within political parties and electoral institutions. As data and AI tools reshape campaign dynamics, robust safeguards must be in place to ensure transparency, fairness, and public trust. Key recommendations from the session include:

1. **Clarify Data Protection Obligations:** Ensure that political parties comply with data protection laws, especially concerning sensitive data and profiling.
2. **Adopt Codes of Conduct:** Political parties should develop binding internal policies governing AI, data analytics, and voter targeting. International bodies — such as the United Nations, the Council of Europe, or the European Commission — can assist in drafting model codes.
3. **Extend Campaign Regulations Year-Round:** Close the "permanent campaign" loophole by ensuring that data protection rules and transparency requirements are effectively enforced outside official campaign periods.
4. **Improve Transparency:** Mandate public repositories of political ads, disclose data sources used for targeting, and label AI-generated content.
5. **Enhance Cross-Agency Collaboration:** Establish formal channels for cooperation between EMBs and data protection authorities, including shared audits and complaint mechanisms.
6. **Promote Accountability in Internal Voting:** While respecting associational rights, encourage political parties to follow best practices for online voting, including independent audits and privacy safeguards.

Selected outside sources explained further in annotated bibliography:

- *Council of Europe Guidelines on Data Protection for Political Campaigns:* Emphasize transparency, consent, and safeguards against microtargeting and data scraping to ensure electoral fairness and lawful processing of personal data.
- *European Partnership for Democracy – AI and Electoral Processes:* Highlights AI-related risks like voter profiling and disinformation in EU elections, and the need for clearer regulatory frameworks and civil society engagement.
- *UN Working Group on Business and Human Rights in Public Procurement:* Underscores the need for human rights due diligence in public procurement, including digital services used in campaigns.
- *Eitan Hersh, Hacking the Electorate (2015):* Explains how microtargeting is based on imperfect data, revealing how limited voter data access can distort political engagement and raise equity concerns.

4.3 Private Companies and Electoral Technology – Responsibilities and Risks (Session 3)

This third session addressed the growing role of private companies in electoral processes and the human rights implications of their services. It explored two broad categories of corporate actors: (1) vendors supporting EMBs with technologies such as biometric registration and internet voting systems, and (2) firms aiding political parties and campaigns with digital marketing, analytics, and voter profiling. Across both sectors, participants emphasized the need for stronger procurement safeguards, clearer regulatory standards, transparency, and accountability mechanisms.

A major concern was vendor lock-in, where a government becomes dependent on a single private company for essential election infrastructure, limiting its ability to switch providers or access its data without that vendor's cooperation. Under such conditions, private companies — not public authorities — retain control over critical election infrastructure, including voter databases. In several countries, the inability to access or update these systems without vendor cooperation has jeopardized the feasibility of holding elections. Participants also noted that for-profit vendors may also lobby for procurement specifications that exclude competitors, effectively monopolizing electoral contracts.

Participants pointed out that procurement processes often lack basic auditability (i.e., the ability of independent observers to verify a system's function and integrity), making it challenging to provide sufficient oversight and identify human rights implications. Requirements for transparency, post-election support, and open-audit capabilities are commonly absent. The result is opaque systems, limited oversight, and public mistrust. This is particularly concerning in internet voting systems, where trade-offs between privacy and verifiability are acute, and intellectual property claims often prevent independent review. The session also explored the risks of data fusion — that is, the combination of official voter rolls with commercial or third-party datasets to build detailed individual profiles — between EMB vendors and political campaign vendors. These networks are not entirely separate. In countries where political parties receive official voter registers, those datasets may be combined with commercial data to create detailed voter profiles, enabling sophisticated profiling and microtargeting.

Many in the group called for embedding human rights into procurement and technology governance. The UN Guiding Principles on Business and Human Rights (UNGPs) establish that companies bear independent responsibility to respect rights, even when domestic law is weak or silent. This includes conducting human rights due diligence and mitigating discriminatory outcomes in content moderation or system design.

Participants identified social media platforms for their lack of responsiveness to electoral authorities in the Global South. Despite hosting critical political discourse, these platforms often prioritize engagement with governments in the Global North. Civil society organizations and EMBs in other regions face obstacles in flagging disinformation or securing policy input. Compounding this, many companies have defunded their trust and safety teams, undermining election integrity efforts.

Participants noted the utility of the IFES Voluntary Election Integrity Guidelines for Technology Companies, which outline 11 principles for vendors, including meaningful consultation with stakeholders (e.g., civil society groups, political parties, technical experts, and affected communities) transparency,

and post-election accountability. Participants recommended these guidelines as a baseline for model contract clauses and public procurement protocols.

This session underscored that while digital tools can enhance electoral management, unregulated private sector involvement creates risks for democracy and human rights. Embedding accountability into procurement and fostering stronger oversight mechanisms are essential next steps. Key recommendations from the session include:

1. **Mandate Transparent Procurement:** Public contracts for electoral technology must include clauses on auditability, data governance, and human rights risk assessments.
2. **Support Vendor Accountability:** Require vendors to adhere to public commitments, such as IFES's 11-Point Guidelines, and conduct post-election performance reviews.
3. **Clarify Data Ownership:** Legal frameworks should specify that voter data remains under the EMB's control, with vendor usage and export restrictions.
4. **Foster National Partnerships with Platforms:** Social media platforms must establish permanent and effective communication channels with EMBs and civil society in smaller or underserved countries.
5. **Ensure Technology Auditability:** Governments should require parallel paper trails, cryptographic audits, or independent code review (i.e., technical examination of software by neutral experts to detect flaws or biases) to guarantee election transparency.
6. **Track Interconnected Vendor Networks:** Authorities should scrutinize data-sharing practices between election vendors and other private entities, including political consultants, to prevent misuse of voter data.

Selected outside sources explained further in annotated bibliography:

- *IFES – Voluntary Election Integrity Guidelines for Technology Companies:* These 11 principles outline vendor commitments to transparency, stakeholder consultation, and post-election accountability.
- *UN Working Group Report on Business and Human Rights (A/HRC/38/48):* Argues that compliance with national law is insufficient; stresses human rights due diligence in procurement and technology services.
- *Information Note on Public Procurement in Latin America and the Caribbean:* Identifies gaps in integrating human rights into procurement and provides guidance on supplier due diligence and institutional coherence.
- *Council of Europe Guidelines on Voter Registration and Authentication:* Recommend strict limitations and protections on biometric and voter registration data, including prohibitions on sharing with political parties.

5 Annotated Bibliography

5.1 UN Resources

- **Human Rights Committee, Concluding observations on the fifth periodic report of the United States of America (CCPR/C/USA/CO/5)**.
  `CCPR/C/USA/CO/5`

  Highlights systemic civil and political rights concerns, especially against racial minorities, Indigenous peoples, and women. It criticizes the U.S. for inadequate incorporation of the ICCPR into domestic law, failure to ensure reproductive justice, racial discrimination in policing and incarceration, and barriers to voting. The document urges structural reforms, treaty reservation withdrawals, and greater accountability mechanisms. It is a comprehensive call for aligning U.S. domestic law with international human rights standards.

- **Human Rights Committee, Concluding observations on the second periodic report of Pakistan (CCPR/C/PAK/CO/2)**.
  `CCPR/C/PAK/CO/2`

  Identifies persistent violations of civil and political rights, including enforced disappearances, torture, censorship, and gender-based violence. It criticizes the abuse of anti-terror laws, lack of judicial independence, and impunity for military and intelligence agencies. Discrimination against women, religious and ethnic minorities, LGBTI persons, and journalists is widespread. The Committee urges Pakistan to reform its laws, strengthen human rights institutions, and align its practices with international obligations. This review is a roadmap for accountability and legal reform in a politically constrained context..

- **Human Rights Committee, Concluding observations on the fifth periodic report of the Bolivarian Republic of Venezuela (CCPR/C/VEN/CO/5)**.
  `CCPR/C/VEN/CO/5`

  Finds widespread violations of civil and political rights, including arbitrary detention, torture, censorship, and repression of dissent. The judiciary lacks independence, and impunity for enforced disappearances and extrajudicial killings remains pervasive. Discrimination against women, LGBTI persons, Indigenous communities, and opposition groups is systemic. The report calls for urgent reforms to align domestic practices with international legal obligations. It underscores Venezuela's democratic backsliding and the global importance of human rights monitoring.

- **Human Rights Committee, Views on Staderini et al. v. Italy (CCPR/C/127/D/2656/2015)**.
  `CCPR/C/127/D/2656/2015`

  In Staderini & De Lucia v. Italy, the UN Human Rights Committee found that Italy's referendum rules imposed unreasonable restrictions on the right to participate in public affairs by making it overly burdensome to collect signatures. The system lacked mechanisms to ensure the availability of officials to authenticate signatures, leading to practical barriers that undermined constitutional guarantees. The ruling calls on Italy to reform its legal framework to ensure referendums are genuinely accessible. While the Committee rejected claims of political and economic discrimination, it reaffirmed that enabling direct democracy entails enforceable obligations. This decision strengthens protections for civic participation under international law

- **Communication of UN Working Group on Business and Human Rights to Meta, Google, Telegram and X (AL OTH 20/2024)**.
  `AL OTH 20/2024`

UN experts accuse Meta of discriminatory content moderation during the 2023–2024 Israel-Gaza conflict, disproportionately censoring pro-Palestinian content while allowing hate speech and incitement against Palestinians to flourish. The letter details algorithmic bias, arbitrary takedowns, and inadequate human oversight, especially regarding Arabic-language posts and journalists in Gaza. It calls on Meta to reform its practices to comply with international human rights standards and the UN Guiding Principles on Business and Human Rights. The communication highlights the platform's role in shaping public discourse during a conflict where the risk of genocide has been deemed plausible by the International Court of Justice. It is a landmark document in the push for digital accountability in conflict zones.ance.

- **Report of the Working Group on Business and Human Rights (A/HRC/38/48)**.
  `A/HRC/38/48`

  How can States better fulfill their duty under the UN Guiding Principles on Business and Human Rights (GPs), particularly Principle 4, by conditioning public trade and investment support on corporate respect for human rights? This 2018 UN report urges States to require businesses seeking trade support—such as export credits or participation in trade missions—to respect human rights. It criticizes the limited use of human rights due diligence in export credit agencies and highlights gaps in transparency and access to remedy. While some OECD countries are beginning to model best practices, most States still fail to align trade promotion with their obligations under the UN Guiding Principles. The report recommends expanding conditionality, disclosure, and grievance mechanisms in trade finance and economic diplomacy. It serves as a critical call for States to operationalize human rights in global commerce.

- **Integrating Human Rights in Public Procurement – Focus on Latin America and the Caribbean**.
  `INFORMATION-NOTE-on-PP_LAC_EN.pdf`

  Discusses the integration of human rights into public procurement in Latin America and the Caribbean. It reveals that while environmental and labor considerations are sometimes included, a holistic human rights approach is often missing. The report recommends enhancing policy coherence, requiring supplier human rights due diligence (HRDD), and building institutional capacity. Addressing these areas can help states fulfill their human rights obligations and promote sustainable development.

5.2 Europe (EU & CoE-related) Materials

- **European Partnership for Democracy, The EU's AI Act and Its Impact on Electoral Processes**.
  `AI-and-elections.pdf`

  Policy paper evaluates how the EU's Artificial Intelligence Act and related regulations affect electoral integrity, particularly in the 2024 European Parliament elections. It identifies risks posed by AI systems—such as voter manipulation, profiling, and disinformation—and critiques enforcement delays, transparency gaps, and definitional ambiguities. The authors call for urgent clarification of high-risk and prohibited AI use cases and recommend more substantial civil society involvement, clearer regulatory guidelines, and interim moratoria on AI in campaigning. The report bridges human rights law and digital governance, offering timely insights on protecting democracy amid technological disruption. It is a foundational contribution to election-focused AI policy debates in Europe.

- **Council of Europe, Guidelines on Voter Data for Registration and Authentication**. `tpd-2023-2rev6`

  These Council of Europe guidelines provide a framework for how personal and biometric data should be processed for voter registration and authentication under Convention 108+. They stress lawfulness, transparency, and the minimization of data use, particularly concerning sensitive categories such as political opinions and biometric identifiers. Biometric voter ID should only be used when necessary and subject to safeguards, transparency, and impact assessments. The guidelines prohibit sharing voter data with political parties and call for public accountability from private tech vendors. They offer critical guidance for protecting privacy and democratic rights in an age of digital and biometric electoral systems.

- **Council of Europe, Guidelines on Data Protection for Political Campaigns**. `guidelines-on-data-proetction`

  The Council of Europe's 2021 guidelines set out rules for protecting personal data during political campaigns, emphasizing transparency, consent, and safeguards for sensitive political opinion data. They warn against voter profiling, microtargeting, and data scraping, which can undermine electoral fairness and voter autonomy. Campaigns must ensure lawful data practices, train staff, and be accountable for third-party processors. Supervisory authorities are urged to collaborate with election bodies and tailor national codes of conduct. The guidelines offer a critical blueprint for balancing privacy and democratic participation in data-driven elections.

5.3 Americas-related Materials

- **OAS, Observing the Use of Electoral Technologies: A Manual (2010)**. `Technology_English-FINAL-4-27-10.pdf`

  Offers a structured framework for observing the use of electoral technology, covering processes from voter registration to electronic voting and results transmission. It outlines legal, technical, and procedural benchmarks for evaluating the transparency, security, and reliability of ICTs in elections. It equips observers with standardized tools and emphasizes pre-election audits, system testing, and public transparency. Though dated, it is a helpful tool for understanding electoral tech governance. Its central insight is that digital elections require robust legal and institutional safeguards to preserve democratic legitimacy.

- **Presidential Commission on Election Administration (2014)**. `Amer-Voting-Exper-final-draft`

  Outlines practical, nonpartisan strategies to improve U.S. election administration. It calls for expanded online voter registration, early voting, improved polling place management, and modernization of voting technology. Emphasizing voter service and accessibility, it proposes a 30-minute wait time standard and tools to optimize resource allocation. While advisory and lacking enforcement power, the report remains a cornerstone for election reform efforts. Its enduring value lies in elevating administrative professionalism and voter-centered design in democratic governance.

- **National Academy of Sciences, Securing the Vote (2018)**. `securing-the-vote`
  `verifiedvoting.org copy`

  Outlines urgent reforms to protect U.S. elections from cyber threats, disinformation, and technical failures. It recommends mandatory paper ballots, rigorous post-election audits, and an end to

Internet voting until secure methods exist. The report emphasizes decentralized yet coordinated administration, with improved funding, research, and certification standards. While advisory, it has become a foundational reference for modern election security practices. Its core message: electoral integrity requires resilient, transparent, and verifiable systems grounded in science and public trust.

- **Fundación Karisma & Friedrich Ebert Stiftung – Colombia Report (2023)**.
  `20651.pdf`

  Maps Colombia's extensive use of technology in its 2023 elections, highlighting 17 tech-driven stages from voter registration to national vote counting. It identifies recurring issues: contractor overdependence (especially on Disproel and Indra), lack of auditability, delayed implementation, and system failures—often in violation of legal timelines. The authors flag serious transparency and security concerns, including unregulated biometric use and opaque software that undermines public trust. Despite its non-academic format, the report is a vital intervention into the real-world risks of digital election administration. Its central warning is clear: technology without oversight can erode electoral legitimacy.

- **Transparencia Electoral (2025): Index of Data Protection during elections in Latin America**.
  `Indice-de-Proteccion-de-Datos-Personales-en-Elecciones-de-America-Latina-3.pdf`

  An extensive and interactive index on data protection during elections in Latin America.The index evaluates laws and regulations around data protection during the election cycle in 16 countries in the region: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Panama, Paraguay, Peru, the Dominican Republic and Uruguay.

- **Brennan Center, Framework for Election Vendor Oversight**.
  `framework-election-vendor-oversight`

  Proposes a federal oversight framework for private election vendors, emphasizing cybersecurity, transparency, and personnel integrity. It calls for expanding the Election Assistance Commission's role to certify all election-related vendors—not just voting machines—and enforce standards for supply chain security and breach reporting. With U.S. elections increasingly dependent on opaque, under-regulated private actors, the report highlights systemic vulnerabilities and prescribes reforms inspired by oversight in the defense and nuclear sectors. Though many recommendations require new legislation, the report outlines actions the EAC can take under existing authority. Its core insight is that democracy's digital guardians must be held to public accountability standards.

- **IFES – Voluntary Election Integrity Guidelines for Tech Companies**.
  `election-integrity-guidelines`

  The Voluntary Election Integrity Guidelines for Technology Companies outline 11 commitments aimed at enhancing collaboration between tech firms, election authorities, and civil society to safeguard electoral processes. Developed through multi-stakeholder consultations, these guidelines address challenges such as disinformation and cyber threats by promoting clear policies, resource prioritization, and open communication channels. Their implementation seeks to bolster public trust and uphold the integrity of democratic elections worldwide.

5.4 Books and Research

- **Eitan Hersh, *Hacking the Electorate* (2015)**.
  `Hacking the Electorate`

Hacking the Electorate shows that campaigns perceive voters through a lens shaped by state-level public records, not sophisticated behavioral data. Using proprietary datasets and campaign staff surveys, Hersh demonstrates that differences in voter data access (e.g., party affiliation, race) systematically affect who gets contacted and how. The book is noted for its "Perceived Voter Model," which reveals that campaigns act on imperfect proxies, creating uneven political engagement. It also debunks the myth of omniscient microtargeting and reframes data laws as central to democratic representation. It is valuable for how information regimes shape political strategy.

6 Organizers

The Office of the High Commissioner for Human Rights (OHCHR) is the leading United Nations entity in the field of human rights, with the mandate to promote and protect all human rights for all people. It works with governments, NHRIs, CSOs, journalists and other electoral stakeholders to ensure all activities during the electoral cycle take human rights protection and promotion into account. OHCHR engages in human rights monitoring and reporting, protection, technical assistance and capacity-building, and advocacy at every stage of the electoral process. In 2018, OHCHR and The Carter Center published *Human Rights and Election Standards: A Plan of Action* and in 2021, OHCHR published *Human Rights and Elections - A Handbook on International Human Rights Standards on Elections*.

Privacy International (PI) supports electoral observers and civil society to address some of the challenges posed by the use of technologies and data in elections. Based on our research in 2023 we published *Technology, data and elections: an updated checklist on the elections cycle*. This checklist aims to reflect on the most recent developments in the space, including PI's analysis and providing electoral observers and interested members of civil society with the relevant tools to examine and unpack some of the most complex and challenging aspects of the electoral process as they pertain to data and technology.

The Carter Center (TCC) conducts systematic and comprehensive desk analyses of the laws and institutions that govern expression, defamation and disinformation. To support the activities envisaged under this project, the Center will make this data available to the event participants so that they can use real-world evidence to inform their arguments on what international human rights standards on technology, data, and elections should (and should not) contain. The Carter Center also maintains a searchable database of over 300 sources of public international law related to human rights and elections. In 2023, the Center published the second edition of its handbook companion to the database, *Election Obligations and Standards: A Carter Center Assessment Manual*.

Organizing Participants: Tomaso Falchetta,[1] Azin Tadjdini,[2] Bikramjeet Batra,[2] Layla Abi-Falah,[2] David Carroll,[3] Obehi Okojie,[3] Anthony J. DeMattee[3]

[1]Privacy International
[2]United Nations High Commissioner for Human Rights
[3]The Carter Center