AEJN
AFRICA ELECTORAL JUSTICE NETWORK

Yiaga Africa
www.yiaga.org

Toolkit on

JUDICIAL OVERSIGHT OF AI IN AFRICAN ELECTIONS

Luminate
AFRICA JUDGES & JURISTS FORUM
10 YEARS SAJEL
SEACJF

JUDICIAL OVERSIGHT OF AI IN AFRICAN ELECTIONS

CONTENTS

Acronyms

AI	Artificial Intelligence
AU	African Union
EU	European Union
EMB	Election Management Body
OECD	Organization for Economic Co-operation and Development
ML	Machine Learning

Acknowledgements

Part 1 **Introduction** **6**

Objectives of the Toolkit

When to use the toolkit

How to use the toolkit

Methodology

Part 2 **Defining Artificial Intelligence** **8**

Differences between General electoral technology and AI

Key principles In AI deployment

Essential terms for judicial officers

Part 3 **Artificial Intelligence in Africa Elections** **11**

Growing Role of AI in Elections

Use cases of AI

Global and Regional trends in Democracy and Elections

Part 4 **Institutional Safeguards** **13**

Judicial Independence in an era of algorithms

Collaboration with EMBs and Other Mechanisms

Accountability, Transparency & Civil Society Oversight

Recommended Good Practices

Part 5 **Legal and Normative Frameworks** 18

Regional, Continental and International Norms

National Legal Framework and Policies

Semi-binding Instruments and Civil Society Soft Laws

Gap Analysis for Critical Evaluation of Legal & Normative Frameworks for AI in African Elections

Part 6 **Evidence Management in AI-related Election Disputes** 21

Categories of AI-related evidence in election disputes

Threshold for Admissibility and Probative Weight

Burden and Standard of Proof in AI electoral Disputes

Expert Witness Management

Strengthening Chain of Custody and Interim Remedies

Classifying AI-related Evidence

Part 7 **Judicial Remedies and Reliefs in AI-Electoral Disputes** 27

Types of Reliefs

Proportionality Analysis

How Courts should balance Public Interest, Urgency and Electoral Reforms

Examples of Electoral Disputes Involving Misuse of AI

Part 8 **Judicial Ethics and AI Use** 32

Key Ethical Risks

Normative Anchors

Practical Application

Model Judicial Questions

Part 9 **Simulated Scenarios for Judicial Engagement** 34

Disputes Arising from the Integrity of the Voter Register in the Context of AI Deployment

Disputes Arising from Malfunction and Manipulation in Electronic Transmission of Election Results

Disputes Arising from AI-Assisted Electoral Boundary Delimitation

Disputes Arising from AI-Driven Misinformation and Disinformation Affecting Voter Turnout During the Campaign Period

A Futuristic Legal Challenge for a Fully Electronic Electoral Process

Annexures 36

AI and Elections Remedies

Glossary of AI terminology

Acknowledgements

This Toolkit on Judicial Oversight of Artificial Intelligence in African Elections is the result of a consultative and collaborative process involving renowned experts, institutions, and partners who share the goal of enhancing democratic governance and electoral justice in Africa.

Yiaga Africa and the Africa Electoral Justice Network (AEJN) partnered to develop this pioneering resource toolkit to promote AI literacy amongst electoral judges in Africa and contribute to the development of the jurisprudence on AI in elections in Africa. This partnership is a demonstration of unwavering commitment to reinforcing electoral justice in an era of algorithms. Special thanks go to the Luminate Group for its generous financial support towards the project. The Centre for Human Rights, University of Pretoria is appreciated for its contributions to the toolkit development process.

We acknowledge the invaluable contributions of the esteemed members for the Working Group on Judicial Oversight of AI in African elections namely;

1. **Justice Dunstan Mlambo,** Deputy Chief Justice of South Africa
2. **Justice Boissie Mbha,** Chair, Africa Electoral Justice Network (AEJN)
3. **Justice Charles Mkandawire,** Justice of the Supreme Court of Malawi
4. **Justice Isaac Lenaola,** Justice of the Supreme Court of Kenya
5. **Justice Aliose Ndiaye,** Justice of the Supreme Court of Senegal
6. **Justice Fiola Mwale,** Acting Justice, Supreme Court of Malawi
7. **Arnold Tsunga,** Coordinator, Africa Electoral Justice Network (AEJN)
8. **Bonolo Makgale,** Programme Manager, Democracy & Civic Engagement, Centre for Human Rights, University of Pretoria
9. **Hon. Elizabeth Tanui,** Registrar, Automation Services, Judiciary of Kenya
10. **Sangwani Nyimbiri,** Coordinator – Southern and Eastern Africa Chief Justices' Forum (SEACJF) and Registrar of the High Court of Zambia
11. **Olusegun Ogundare,** Head, Research and Operations, Africa Division, Yiaga Africa
12. **Dr Justice Mavedzenge,** University of Capetown and Program Director at Africa Judges and Jurists Forum

We appreciate the contributions of members of the Africa Team at Yiaga Africa — Ibrahim Faruk, Africa Program Coordinator, and Aanuoluwapo Kokoyi, Program Officer — for their dedication and support throughout this process. Special thanks to Cynthia Mbamalu, Director of Programs, for her valuable technical input, and to Stephen Momoh for his creative work on the graphic design.

We recognize the torrents of contributions from judicial officers, election management bodies, lawyers, civil society organizations, scholars, and technology experts who took part in the consultative and validation workshops including peer review sessions in Africa. Their observations and thoughts defined the principles, frameworks, and case analyses in this toolkit.

Lastly, this toolkit is dedicated to the judges, election officials, and civil actors who toil day and night to protect electoral integrity and enforce the rule of law in the digital age of artificial intelligence. Their devotion to justice, accountability, and human dignity remains the inspiration for the quest for democratic perfection in the entire continent.

Samson Itodo
Executive Director, Yiaga Africa

1. Introduction

In recent years, the use of Artificial Intelligence (AI) in electoral processes has grown, offering opportunities to improve efficiency, data analytics, and voter outreach. However, these benefits come with risks, particularly for judicial actors who must adjudicate disputes where AI has influenced or determined electoral outcomes. This toolkit seeks to empower judicial actors in Africa to anticipate, understand, and respond to the integration of AI in African elections while safeguarding electoral integrity, transparency, accountability and other fundamental rights. It offers a practical guide for identifying, evaluation and resolving AI-related electoral disputes brought before electoral courts in Africa.

This toolkit is a living document, designed to evolve with the rapidly changing landscape of AI and democratic processes. Judicial actors are encouraged to contribute to its improvement and adaptation to local contexts.

Objectives of the Toolkit

1. Promote AI literacy among judicial officers to facilitate judicial response to AI application in African elections.
2. Provide practical tools for identifying, evaluating and resolving AI-related electoral disputes.
3. Address legal and ethical gaps in current electoral and judicial frameworks in relation to AI deployment.
4. Support the development of Africa's jurisprudence on Artificial Intelligence in elections

When to Use this Toolkit

1. When electoral institutions seek legal guidance on ethical adoption of AI in elections
2. When the electoral legal framework provides no guidance for AI in elections
3. When AI systems affect voter registration, voter verification, results collation and transmission and voter outreach.
4. When algorithmic bias, technical glitches, cyberattacks are alleged in electoral disputes
5. When the court is required to evaluate the probative value of AI generated evidence or expert opinion about AI systems

How to Use this Toolkit

The toolkit is crafted as a practical guide for judicial officers, and legal practitioners. It is a resource tool that can be used by judges, electoral dispute practitioners, and judicial educators for training. It can also serve an election adjudication support tool. The toolkit is structured into seven parts with each section providing practical insights and judicial response to AI in elections.

Users are encouraged to engage with sections according to their needs:

- **Section 1:** Institutional Safeguards outlines judicial independence, collaboration with EMBs, and institutional mechanisms essential for safeguarding electoral integrity in the AI era.
- **Section 2:** AI in Elections Landscape defines AI, reviews its adoption and use cases in Africa, and surveys global and regional trends affecting democratic processes.
- **Section 3:** Legal and Normative Frameworks presents regional, continental, and national legal instruments alongside guiding principles for AI oversight.
- **Section 4:** Evidence Management in AI-Related Election Disputes details types of AI-generated evidence, admissibility standards, challenges of AI opacity, and the role of expert witnesses.
- **Section 5:** Judicial Remedies and Reliefs explores available legal remedies, balancing of public interest, and the doctrine of proportionality in electoral disputes involving AI.
- **Section 6:** Case Scenarios provides illustrative examples to ground theoretical principles in practical adjudication contexts.
- **Section 7:** Checklists and Templates offers decision-support tools tailored for judicial and institutional users.

This toolkit can be utilised during case preparation, judicial reasoning, institutional training, and policy development, supporting a rights-based, contextually relevant approach to AI governance in African elections.

Methodology

This toolkit was developed through a consultative process involving expert contributors in law, technology, electoral processes, and human rights. It's development combined in-depth desk research, expert interviews, and multi-stakeholder consultative workshops focused on AI, elections, and electoral justice. It adopts a modular approach, allowing it to be updated as the AI landscape evolves.

2. Defining Artificial Intelligence

This section provides judicial officers with an introduction to what AI is, and the terms likely to be encountered in evidence and expert testimony.

The concept of "artificial intelligence" has multiple definitions across disciplines. The OECD defines AI as a machine-based system that, for a given set of human-defined objectives, can make predictions, recommendations, or decisions influencing real or virtual environments.[1] The African Union's Continental Strategy for AI in Africa (2024) echoes this but places emphasis on transparency, accountability, and human rights safeguards in deployment.[2] For the judicial toolkit, it is essential to use plain-language definition: AI is a computer system that mimics certain human decision-making processes by finding patterns in data and using them to make predictions or choices.

To avoid abstraction, a short glossary of basic terms is provided (with an extended cersion in the Annex below), to aid with referencing AI scenarios, as gleaned from the OECD, AU and EU policy instruments for AI:[3]

- **Algorithm –** A step-by-step procedure or formula for solving a problem, forming the backbone of AI systems.
- **Machine Learning –** A method where algorithms learn from large datasets to improve performance without explicit reprogramming.
- **Bias –** Systematic distortion in data or models leading to unfair outcomes, particularly dangerous in elections where certain groups may be disadvantaged.
- **Explainability –** The extent to which the workings of an AI system can be understood by humans, critical for judicial scrutiny.
- **Audit Trail –** A record of inputs, processes, and outputs enabling verification of how decisions were reached; directly relevant in electoral disputes.

See expanded list in Annex for additional terms to consider when AI intersects with election technology.

Levels of Autonomy (practical taxonomy for judges)

- **Assisted AI –** system suggests but required immediate human control.
- **Augmented AI –** system enhances human decision-making; human remains final arbiter.
- **Autonomous AI –** system operates with minimal human oversight; highest accountability risk.

[1] OECD Data & AI Glossary: SDAIAPublications15.pdf.]

[2] AU Continental Policy on AI 2024: 44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf.]

[3] See above; EU AI Act: The AI Act Explorer | EU Artificial Intelligence Act.]

Differences	General Electoral Technologies	Artificial Intelligence
Decision-making and Outputs	Outputs and decision-making are based on pre-determined instructions	Outputs are based a learned patterns from data Rely on statistical patterns to predictions
Operational Functionality	Static	Dynamic due to consistent learning
Risks	System glitch or technical breakdown, intrusion and hacking	Hallucinations, bias, opacity, deepfakes
Oversight Mechanisms	Transparent, auditable process	Blackbox and difficult to explain

Key Principles

1. **Ownership and Dependence on Foreign Technology:** The ownership of AI systems must be clearly defined and it must remain accountable under electoral and data protection laws. African countries should reduce reliance on foreign technology by fostering domestic innovation and capacity for sustainable, context-relevant AI systems.
2. **Collaboration Between EMBs and Stakeholders:** Collaboration and partnership with civil society, tech firms, academia, media, and voters across all stages of AI deployment is an imperative. Structured mechanisms such as advisory panels can strengthen oversight, legitimacy, and public trust.
3. **Legal and Ethical Compliance:** AI use in elections must comply with national and international legal frameworks and uphold fairness, accountability, non-partisanship, and transparency. Laws should evolve to address risks like algorithmic manipulation and misinformation.
4. **Transparency Mechanisms:** Institutions deploying AI in elections must be open about AI tools' purposes, capabilities, limitations, and data sources. Simpler, auditable systems should be preferred. Public disclosure of impact assessments promotes trust and accountability.
5. **Data Protection, Integrity and Inclusivity:** AI systems must ensure secure, lawful data use, prevent bias, and reflect voter diversity. Protecting equity and integrity is essential for democratic legitimacy.
6. **Context-Specific Application:** AI must be adapted to each country's political, legal, and cultural realities. Pre-deployment audits, pilot tests, and third-party reviews are vital to ensure fairness, reliability, and contextual fit.
7. **Protection of Human Rights:** AI deployment must safeguard privacy, expression, association, and participation rights, avoiding surveillance, profiling, or censorship that could restrict civic freedoms.
8. **Human Oversight and Dispute Resolution Mechanisms:** Human judgment must remain central to AI decisions affecting elections. Transparent appeal and review mechanisms should exist for AI-assisted outcomes like registration or results management.
9. **Accountability, Explainability and Auditability:** AI systems must be independently verifiable and understandable. EMBs and vendors share responsibility for ethical use, with audits before and after elections to detect bias or harm.

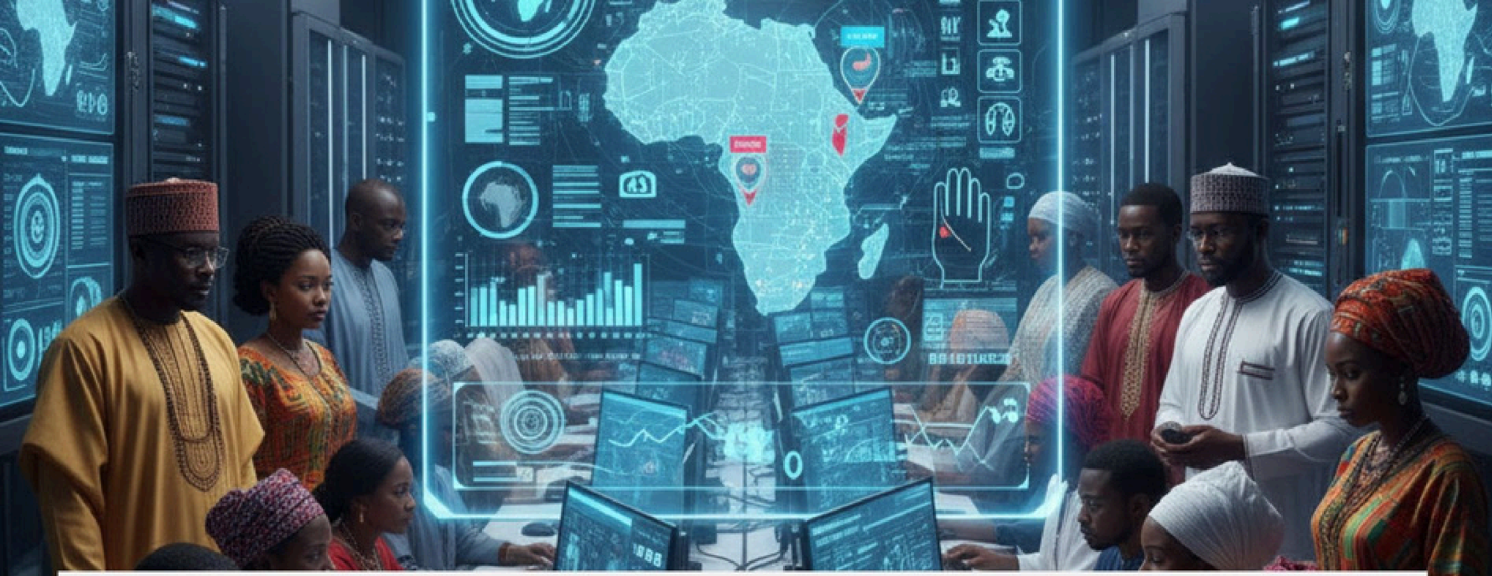
10. **Cost-Effectiveness:** AI should improve electoral processes efficiently and sustainably without draining limited financial resources. Tools must be affordable, scalable, and enhance—not replace—core functions.

Essential Terms for Judicial Officers

AI Key Term	Definition	Relevance to Elections
Algorithm	Step-by-step instructions a computer follows to make decisions	Determines outcomes like vote tallying or voter eligibility
Machine learning	AI technique that learns patterns from data and makes predictions	Used in election results management, biometric systems, content moderation and voter analytics
Large Language Models (LLMs)	AI system trained on vast amounts of text to understand and generate human-like language	Used in automated content moderation, chatbots for voter information, analysis of political communications, and potentially in generating campaign materials or disinformation
Generative AI	AI systems that create new content (text, images, audio, video) based on training data	Can produce deepfakes, synthetic political advertisements, fake news articles, or misleading audio/video content that may influence voter perceptions or spread disinformation
Natural Language Processing (NLP)	AI's ability to understand, interpret, and generate human language	Powers automated social media monitoring, sentiment analysis of political discourse, translation services for multilingual elections, and content moderation systems that may affect political speech
Data	Information collected, stored, and processed by AI systems, including personal, behavioral, and demographic information	Voter registration data, biometric information, voting patterns, and social media activity used for voter verification, targeted advertising, and electoral analysis.
Bias	Systematic errors leading to unfair outcomes	May exclude certain voter groups or favor particular candidates
Explainability	The ability to understand why an AI system made a decision	Essential for judicial review and public accountability
Audit Trail	Record of system inputs, processes, and outputs	Provides evidence for dispute resolution
Black box	AI system whose internal workings are not easily understood	Creates challenges for judicial scrutiny and accountability

Key Takeaways

- **Settled terms** (e.g. accountability, electoral technology) → judicial officers are encouraged to lean on established doctrine.
- **Developing terms** (e.g. explainability, transparency, bias) → courts can build comparative precedents.
- **Unsettled terms** (e.g. hallucination, adversarial attacks, burden of proof) → these are fertile grounds for judicial innovation and warrant doctrine development.



3. Artificial Intelligence in African Elections

The Growing Role of AI in Elections

Artificial intelligence (AI) is increasingly embedded across all phases of electoral cycles, from voter registration and boundary delimitation to political campaigning, election monitoring, and results management. AI tools have been used to speed up biometric voter verification, as well as to optimize electoral logistics, predict voter turnout, and micro-target political messaging through social media algorithms.

Yet the opacity of these systems, coupled with weak regulatory oversight, raises concerns over their effect on electoral fairness and public trust. The rise of "black box" algorithms and data-driven profiling in elections has led courts and electoral tribunals across jurisdictions to grapple with whether, and how, the use of AI can violate electoral law, undermining democratic outcomes.

AI can be implemented across the electoral cycle.

Pre-election:

- Voter registration and clean-up of voter rolls
- Constituency delimitation
- Candidate nomination and screening
- Disinformation monitoring

During election

- Voter authentication
- Prebunking and debunking disinformation
- Results transmission and collation
- Sentiment analysis

Post Election

- Results verification and auditing
- Dispute investigation and evidence evaluation

Use Cases of AI Adoption in African Elections:

According to a Yiaga Africa survey on the adoption of AI in election administration, the most prominent use cases of AI in election management are voter register management, voter verification, election results management, cyber threat detection and countering disinformation. These use cases were found in Kenya, Nigeria, South Africa, Kenya, and Eswatini, provide model cases of AI adoption in elections.

Global and Regional Trends of AI in Democracy and Elections:

- EU's proposed AI Act and its classification of high-risk AI in electoral contexts
- African Union's Digital Transformation Strategy and growing digital infrastructure
- Increasing involvement of multinational tech platforms in shaping public opinion

Civil society groups including Paradigm Initiative and Media Foundation, to name a few, have publicly advocated for courts to factor in digital literacy disparities in electoral disputes (this would necessarily encompass AI biases as well, as a sub-field), emphasizing that existing laws lag behind rapid digital interference and AI-enabled tactics. This helps judges apply a justice-sensitive and context-aware approach in technical cases.

4. Institutional Safeguards

Effective oversight of AI in African electoral systems demands institutional structures that uphold judicial independence, promote judiciary–EMB collaboration, and embed transparent accountability mechanisms.

1. Judicial Independence in an Era of Algorithms

The design of Artificial intelligence systems poses new challenges to judicial independence particularly in cases where judges depend on AI systems to resolve disputes. By all standards, it undermines judicial independence and technically strips the courts of its judicial powers. Safeguarding due process and public confidence requires that judges remain independent from these "black-box" technologies. Courts must demand full transparency and accountability from electoral bodies, AI vendors, and technology companies. Above all, judges must ensure that in adjudicating electoral dispute, they should defer to human primacy to avoid AI-powered judgement that may likely subvert justice delivery.

Protecting judiciary autonomy remains critical as electoral systems rely increasingly on AI technologies. The following case, though not based on AI in electoral disputes, considers how the courts have engaged broadly enforced technology transparency requirements:

Key African Precedents

- In Kenya, the Supreme Court's landmark annulment of the 2017 presidential election illustrated this principle. The Court emphasised the Independent Electoral and Boundaries Commission (IEBC)'s failure to validate electronically transmitted results, underscoring the judiciary's role in scrutinising electoral technology integrity. Presidential election results were transmitted electronically, but the opposition alleged manipulation and irregularities in the electronic results transmission system. The legal issue stemmed from whether the technological failures in the electoral process compromised the constitutional guarantee of free and fair elections, and the Supreme Court ultimately found it fit to annul the election, finding that the IEBC had failed to conduct the process in accordance with constitutional principles of transparency, verifiability, and accountability.

  The Court stressed that technological reliability is not a technical side-issue but a matter of constitutional integrity, meaning when digital systems obscure accountability, the credibility vote is undermined. Importantly, the court ruled that where electronic evidence is opaque or inaccessible, the benefit of the doubt must favour the petitioner. This principle is directly relevant for AI contexts, where algorithms may similarly be "black boxes." Though not involving AI, this case shows that technological opacity shifts evidentiary favour towards challengers. Judges could use this reasoning to justify shifting the burden of proof to EMBs or vendors when AI systems are not auditable ([Raila Odinga v IEBC, 2017] Kenya court blames electoral body for nullified vote | Uhuru Kenyatta News | Al Jazeera). See also the similar test and challenges to the Kenyan 2022 election result, Kenya's judiciary upheld the verifiability and security of the Kenya Integrated Election Management System (KIEMS) and found no credible evidence of hacking, upholding electoral technology under high pressure ([Chief Justice Koome's unanimous decision] Presidential Election Challenges & Legitimacy of the Court in Kenya — Columbia Journal of Transnational Law).

- In Nigeria, the case of Atiku Abubakar v. Independent National Electoral Commission (INEC) (2019 & 2023) provides an antithetical approach to consider when ascribing the burden of proof in technology-related disputes. Petitioners challenged election outcomes, arguing that INEC used servers to transmit results and that these systems were effectively compromised. The legal question concerned whether digital evidence irregularities were sufficient to annul results, to which the Supreme Court dismissed the petitions, holding that the evidence was speculative and insufficiently proven.

  The court underscored that the burden of proof lies with the petitioner to demonstrate irregularity. Where EMBs or vendors control access to technology, this standard becomes nearly impossible to meet. The decision highlights judicial caution in intervening without direct, verifiable proof of technological failure, which underscores the need for burden-shifting rules in AI disputes. If petitioners cannot access training data, audit logs, or algorithms, courts may need to presume against the EMB/ vendor [Atiku Abubakar v. Independent National Electoral Commission (INEC) (2019 & 2023) atiku_v_INEC_No1_2023_19_NWLR_pt1917.pdf. See also the South African Constitutional Court's My Vote Counts ruling affirmed the right to transparency in electoral funding, setting a precedent for the judiciary's authority over electoral accountability ([My Vote Counts NPC v Minister of Justice] My Vote Counts NPC v Minister of Justice and Correctional Services and Another (CCT249/17) [2n018] ZACC 17; 2018 (8) BCLR 893 (CC); 2018 (5) SA 380 (CC) (21 June 2018)).

International Good Practices

- In the Indian case of Subramanian Swamy v. Election Commission of India (2013) petitioners challenges the exclusive use of Electronic Voting Machines (EVMs) arguing lack of transparency and verifiability. The challenge concerned whether the absence of a paper audit trail comprised free and fair elections. The Supreme Court ordered the integration of Voter Verifiable Paper Audit Trails (VVPATs) alongside EVMs. It held that verifiability is a constitutional requirement under Article 324, ensuring elections are transparent and free from manipulation. The court described VVPATs as an "indispensable" feature of modern democracy, giving the voter confidence that their choice was accurately recorded. This case sets precedent to the fact that technical innovation is acceptable only if accompanied by independent verification mechanisms. For AI, this translates into mandatory auditability and explainability safeguards [Subramanian Swamy v. Election Commission of India (2013)] Subramanian Swamy v. Election Commission Of India . | Supreme Court Of India | Judgment | Law | CaseMine.
- In the European case of Kovach v. Ukraine (2008), the case involved alleged vote-county irregularities in a single constituency race, with the court having to decide whether minor irregularities undermined the right to free elections under Article 3 of Protocol No.1 of the European Convention on Human Rights. The court held that even minor electoral irregularities may violate democratic guarantees if they distort the will of the people. It stressed the notion that trust in electoral integrity is as important as the result itself and offers judges an interpretative baseline for determining similar implications in AI-related disputes. In the hypothetical case of an algorithmic error, even a "small" bias in an AI-voting-counting or voter-verification system can fatally undermine democratic legitimacy. Courts should therefore treat algorithmic distortions as constitutionally significant, regardless of scale.

- Finally, in Germany's Federal Constitutional Court, E-voting Case (BverfG, 2 BvC 3/07, 2009), the petitioners challenged EVCs used in federal elections, citing that the system failed to comply with the constitutional principle of public oversight of elections. To this end, the court found in its favour, ruling that all essential steps of the electoral process must be publicly verifiable without specialised knowledge. Mirroring the case of Raila Odinga v IEBC, the court found that closed or opaque technologies fail the test of "comprehensibility," even if technically reliable. The court found the machines unconstitutional because the average citizen could not understand or verify the vote count. This scenario introduces the principle of citizen-centered transparency, which may be extrapolated to AI in elections, and which considers that AI and technology in general must not only be reliable, but also intelligible to non-experts, and supports requirements for plain-language audit reports and public scrutiny mechanisms.

Estonia: A Model for AI-Ready Electoral Oversight

In an opinion on the Estonian Legislation Regulating Internet Voting, the Estonian jurisprudence on internet voting, buttressed by the Office for Democratic Institutions and Human Rights (ODIHRs) recommendations, does more than simply validate e-voting; it provides a framework for how new, high-risk digital processes in democracy can be governed and adjudicated. The recommendations touch on legitimacy through broad consultation, the safeguarding of electoral principles, continuous oversight, transparent technical standards, and independent monitoring.

Each of these themes resonates with the institutional architecture needed to adjudicate AI disputes. For instance, criteria for suspending or invalidating electronic votes find a parallel in defining when AI output should be halted or overturned, while post-election audits mirror the need for continuous monitoring of AI systems. Given their breadth and detail, the full recommendations (A-G) cannot be rehearsed here, but they deserve direct attention. They set out a comprehensive framework that could readily be extrapolated into the AI dispute resolution context, underscoring the importance of public legitimacy bolstered by technical and constitutional safeguards. See 593435.pdf for the full discussion.

At its core, Estonia's approach underscores three transferable lessons for developing an adjudicatory mechanism for AI disputes:

1. **Legitimacy through participation** – Substantial changes to electoral technology must follow broad-based consultations and civil society engagement. This mirrors the necessity for multi-stakeholder input in shaping AI dispute processes, to ensure not only expertise but also democratic legitimacy.
2. **Embedding international principles** – Estonia highlights that universality, equality, and freedom of participation must be expressly translated into the technical and legal design of voting. For AI adjudication, this suggests that principles such as fairness, transparency, accountability, and human rights must be hard-wired into both procedure and technology.
3. **Independent oversight and state-of-the-art safeguards** – The insistence on monitoring and oversight bodies in Estonia signals the importance of external checks. Any AI dispute resolution mechanism should similarly require independent supervisory authorities with clear mandates to review systems according to evolving international standards.

Taken together, Estonia's case law and the ODIHR guidance invite us to treat AI dispute adjudication as a civic infrastructure, not merely a technical forum, but a democratic process requiring durability, inclusivity and trust. Just as e-voting systems cannot operate without legitimacy and rigourous oversight, adjudicating AI disputes (especially those touching on political rights, elections or democratic participation) must be grounded in transparent standards (see note on burden and standard of proof in Section 5: evidence-management).

2. Collaboration with EMBs and Other Mechanisms

Cooperative frameworks between judiciaries and electoral management bodies (EMBs) are essential to secure access to technical data, whilst ensuring procedural fairness and upholding transparency when AI systems are deployed.

Meaningful collaboration ensures courts and EMBs share expertise and data to promote institutional trust:

- In Ghana, EMB-judiciary joint training programmes have improved digital and legal literacy among both election officials and judges. Electoral justice in Kenya and Nigeria | TheCable
- In Kenya, technical help desks and advisory panels were introduced to help judges interpret complex electoral technology, especially during the 2022 petition, drawing on multi-sectoral expertise.
- Civil society watchdogs such as Nigeria's Yiaga Africa, and Transition Monitoring Group (TMG) criticized the 2023 Supreme Court's constraints on electronic collations (IReV/ BVAS), highlighting the peril of guarded technology reducing transparency in elections. CSO faults S'Court verdict on electronic voting | The Guardian Nigeria News - Nigeria and World News.

Framework for EMB-Judiciary Collaboration

- In the pre-election period, electoral bodies and judiciary can development mechanisms for facilitating information sharing. For instance, before deployment, electoral bodies should avail the courts with all documentation related to the AI system. Reports of AI readiness assessment and other independent technical assessment should be accessible to the courts. The court can also demand for evidence of public inputs or inputs from other election stakeholders such as civil society, technology experts, political parties etc.
- During elections, electoral bodies should maintain both access and incident logs and ensure they are accessible to the courts. Election day monitoring reports should be provided to the judges while IT officers and technical experts of EMBs provide assistance to judicial officers.
- For post-election, all independent systems audit and assessment report should be accessible to the courts. Where necessary, expert testimony should be facilitated by the EMB.

3. Accountability, Transparency & Civil Society Oversight

Robust mechanisms are essential to govern electoral AI responsibly:

- Mandatory AI impact assessments and public certification should precede any deployment of electoral systems—aligned with principles articulated in the African Charter on Democracy, Elections and Governance (ACDEG) Judiciary and electoral disputes in Africa - The Nation Newspaper
- Data sovereignty: Kenya's Supreme Court accepted domestic ownership and operational control over KIEMS, even when implemented by a foreign vendor (Smartmatic), reaffirming EMB responsibility over outsourced systems There Was No Hacking – Supreme Court Declares | CIO Africa.
- Legal enforceability of auditability: Courts should demand access to system logs, audit reports, and vendor contracts to counteract "black-box" opacity. Post-2022 Kenyan elections, civil society and experts jointly called for full disclosure of audit logs to rebuild public confidence. Reinstating trust in elections in the era of artificial intelligence and emerging technologies | Data & Policy | Cambridge Core / The Nigerian Judiciary and Electoral Technology - THISDAYLIVE
- Multi-stakeholder oversight mechanisms, including civil society participation, foster checks and balance. Ghana, Nigeria, and Kenya have experimented with inclusive monitoring committees to validate AI deployment in election runs. Electoral justice in Kenya and Nigeria | TheCable.

Recommended Best Practices

Based on cross-jurisdictional evidence and regional lessons learned:

Practice	Why It Matters	Country Example
Formal judicial impact review protocols	Ensure technology is evaluated before use	
Dedicated tech-legal advisory units	Aid courts in interpreting AI and digital evidence	Kenyan judicial help desk
Legal mandates for AI transparency	Prevent vendor secrecy and opaque deployment	South African transparency law (My Vote Counts)
Independent public audit certification	Validates results, builds public trust	Post-Kenya 2022 election critique
Civil society participation in oversight	Offers external checks; engages citizens	Ghana EMB-CSO advisory panels

5. Legal and Normative Frameworks

Artificial intelligence is gaining traction faster than current democratic law regimes can keep up with. Regional norms such as the ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa and the UN Guiding Principles on Business and Human Rights, in addition to country data protection and cyber laws, constitute the legal basis for electoral integrity. They do, however, suffer from customized standards responsive to African electoral jurisprudence, long informed by values of democratic principles. Artificial intelligence poses new dynamics for these to reckon with.

Together, the continent's constitutional architecture provides a tripartite foundation: regional instruments set human rights benchmarks; national law regulates data, cybersecurity, and election behavior; and civil society informally-binding initiatives establish context-aware, dynamic guardrails.

But these standards remain inadequately tuned to the risks of the AI age. Courts and judges now must stretch and expand normative framework, insisting on algorithmic explainability as the condition for the proper and lawful application of AI in African electoral processes.

Regional, Continental and International Norms and Standards:

- African Charter on Democracy, Elections and Governance
- ACHPR Declaration of Principles on Freedom of Expression and Access to Information
- UN Guiding Principles on Business and Human Rights
- AU Convention on Cybersecurity and Data Protection (Malabo Convention, 2023)

The toolkit builds on regional instruments such as the African Charter on Democracy, Elections and Governance (ACDEG) which emphasises transparency as a pillar for credible institutions. However, these norms predate the emergence of AI and do not anticipate risks posed by data-driven, autonomous systems.

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) addresses cyber governance broadly, including data sovereignty and criminalisation of cyber-enabled threats, but does not directly regulate AI in elections. Likewise, the African Declaration on Internet Rights and Freedoms (2014) establishes high-level internet principles such as legal accountability and non-discrimination, but lacks binding enforcement specific to electoral AI governance. The African Governance Architecture (AGA) supports institutional harmony in implementing AU norms, but has yet to integrate AI-specific oversight pathways across judicial, electoral, and regulatory bodies.

The Durban Declaration was facillitated by the United Nations, specifically through the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance, held in Durban, South Africa, in 2001 and organised by the Office of the High Commissioner for Human Rights (OHCPR). It affirms that discrimination based on race, ethnicity, or related status is a violation of human rights and obliges states to prevent technologies from perpetuating such bias. An example where this protocol might prove efficacy is in the scenario where biometric mismatches disproportionately affect the elderly or rural voters, which would constitute indirect discrimination requiring immediate remedial or legislative action.

ACHPR Declaration on Freedom of Expression and Access to Information (2019): Article 9 of the African Charter mandates the right to information and expression; the Declaration expands this to include digital access and government data transparency. Its relevance to elections lies in requiring public access to electoral AI deployment data and system disclosures—vital prerequisites for judicial scrutiny and informed adjudication.

UN Guiding Principles on Business and Human Rights (2011): These establish corporate responsibility for human rights, including due diligence, transparency, and remediation obligations. Applied to vendors of AI electoral systems, they compel EMBs and private partners to ensure digital systems do not infringe rights and remain auditable.

AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention, 2023): Ratified by key African states, it mandates data protection authorities, impact assessments (Article 8), and cybersecurity policies. While not AI-specific, its emphasis on consent, accountability, and state-level enforcement offers a legal basis for regulating biometric and algorithmic electoral systems. Critical limitations include narrow ratification and lack of provisions for algorithmic explainability or audit trails in electoral contexts.

National Legal Framework and Policies

Countries are increasingly introducing data protection and cybercrime laws that may interact with AI in elections, but few explicitly regulate algorithmic systems. This creates gaps in oversight and remedy.

Kenya: The Data Protection Act, 2019, together with its 2021 Regulations, directly governs the use of biometric and digital election technologies such as KIEMS and the BVR system used in 2022. These laws require voter data to be processed lawfully, fairly, and transparently, and mandate Data Protection Impact Assessments (DPIAs) for high-risk electoral technologies. Missing, however, are AI-specific standards or accountability mechanisms for algorithmic decision-making. Policy Brief: Personal Data and Elections 2022 | KICTANet Think Tank.

Nigeria and South Africa: While neither country currently regulates AI in elections explicitly, Nigeria's Cybercrimes Act criminalises identity theft, impersonation, and disinformation — offenses that may be relevant when AI-generated deepfakes affect electoral integrity. South Africa's Protection of Personal Information Act (POPIA) enables judicial scrutiny of unlawful data handling and profiling during electoral processes. Both regimes lack AI-consistent transparency mandates or obligations for explainability.

These national laws illustrate foundational principles but expose a clear gap in regulating emergent AI practices in electoral contexts.

Semi-Binding Instruments & Civil Society Soft-Law Guidance

Civil society has proactively filled normative voids with practical frameworks:

- The Office of the Data Protection Commissioner released the Guidance Note on Processing Personal Data for Electoral Purposes recommended mandatory DPIAs, voter notices, and transparency protocols for biometric and electronic voter systems Safeguarding Personal Data During Kenya's 2022 General Election | KICTANet Think Tank.

- Organisations like Research ICT Africa, Paradigm Initiative, and Media Foundation for West Africa advocate for introducing AI-specific legal thresholds, including independent audits and consumer rights of contestability in electoral systems Paradigm Initiative Launches Impact Tools To Improve Digital Inclusion In Africa.
- Privacy International and others have insisted on vendor accountability clauses, open-source code mandates, and human-in-the-loop guarantees to prevent algorithmic delegation of electoral decisions Accountability | Privacy International.

These interventionist strategies act as practical supplements to formal regulations, providing judges and policymakers with normative tools to demand transparency and rights-based governance, even where laws lag behind.

The Global Index on Responsible AI (GIRAI) tracks responsible AI governance across countries. For example, according to the 2024 GIRAI report, Kenya scored 8.8/100, reflecting gaps in governance despite strong legal tools like its Data Protection Act (2019) and National ICT Policy (2019).

Complementary insights come from the AI Readiness Index (also called the Government AI Readiness Index), which ranks countries on infrastructure, policy, and technology uptake—for instance, Mauritius ranked highest in Africa, followed by South Africa and Kenya.

The AGILE Index (AI Governance International Evaluation Index) offers a structured baseline of governance maturity in a growing set of countries, with a focus on governance effectiveness, legal instruments, and risk exposure arXiv+1.

Civil society groups, such as AI4D Africa, have welcomed these indexes as critical tools for accountability, calling on EMBs and legislatures to leverage them in strengthening AI governance around auditability and public participation.

These indexes provide intersectional markers for countries to self-assess and for courts to benchmark institutional readiness against international governance standards.

Gap Analysis for Critical Evaluation of Legal & Normative Protection for AI in African Elections

- **Technological Neutrality of Normative Instruments:** Regional instruments (ACHPR Declaration, UNGPs, Malabo Convention) incorporate essential democratian norms but do not take a technology stance. They thus restrain their binding power in managing upcoming risks.
- **Deficits in Enforcement and Disclosure:** Even in countries with domestic law, like Kenya's Data Protection Act (2019) or South Africa's POPIA, enforcement is uneven. There is limited number of EMBs doing pre-election auditing of AI platforms or publishing algorithmic effects to the public or bench.
- **Absence of AI-Specific Jurisprudence:** Thus far, no African court has provided a precedent or made judicial pronouncements on contestability or algorithmic explainability in elections. This sets litigants and judges adrift without guidance to challenge or to uphold AI's involvement in the election cycle.

6. Evidence Management in AI-Related Election Disputes

This part analyzes the dynamic evidentiary environment before courts in artificial intelligence-related election contests, distilling new admissible evidence categories, fit levels of judicial intervention, and the overriding significances of expert testimony. With election technologies becoming more sophisticated, courts will need to develop an analogous competence in debunking algorithmic unreliability, in examining dark systems, and in controlling digital evidence decay risks. They do so in maintaining both the procedural and substantive justice of election contest resolution.

Categories of AI-related evidence in election disputes

Adjudicating AI-driven harms requires a reimagining of what constitutes "material evidence." In addition to direct impacts on voters or results, courts must consider:

1. **AI Systems Documentation:**
   - Source codes and algorithmic data & configuration
   - Machine learning data and model parameters
   - Reports of pre-testing of AI systems and validation reports
   - Vendor contracts, ISO certifications etc.
2. **Operational Evidence**
   - User access and modification records
   - System logs and audit trails
   - Performance metrics and data
   - Error and incident documentation
3. **Impact Evidence**
   - Expert witness testimony
   - Comparative analysis with manual processes and procedures
   - Voter patterns and demographic analysis

These forms of evidence are not self-evident; their probative value often depends on context, traceability, and interpretation by qualified experts.

Thresholds for Admissibility and Probative Weight

Courts must develop and apply new thresholds to determine whether AI-related evidence is reliable, relevant, and admissible. Three key standards emerge:

1. **Reliability Test: When the court is in its validity test mode, it would have to pose the following questions in arriving at its decision:**
   - Did the system undergo independent test and certification?
   - Are error rates and the AI system's limitations formally documented?
   - Are the decisions and results of the AI system testable?

2. **Relevance Test: The court could be required to establish the relevance of the evidence by answering the following questions**
   - To what extent does the evidence support the outcome of the vote and the rights of voters?
   - Is it probative of the allegations made?
   - Is the supposed irregularity likely to distort election outcomes?
3. **Verifiability Test: Ascertaining the verifiability requires determining the following questions**
   - Could parties or experts fruitfully scrutinize and question the evidence?
   - Are audit trails up-to-date and tamper-evident?
   - Is the expert testimony readily available to interpret technical proof?

These thresholds help courts filter speculative claims from legitimate disputes while preserving space for urgent judicial interventions.

Burden and Standard of Proof in AI Disputes Involving EMB/Vendors

AI-related election disputes raise unique evidentiary challenges. Courts may need to shift burdens (see Section 2: Institutional safeguards, to see how African courts have interpreted the adoption of new technology into dispute and legislative procedure, and from which the following has been gleaned:

AI-Modified Approach

- **Prima Facie Standard** – once the petitioner shows plausible irregularity (e.g. unexplained biometric rejection rates), the burden shifts.
- **Vendor/EMB Duty** – the obligation to disclose logs, source code, independent reports, presuming the plausible irregularity is on the Vendor/EMB.
- **Judicial Presumption** – if access is blocked, courts may presume adverse inference against EMB/vendor.

In this case, traditional remedies (rerun, recounts) must be expanded:

- **Third-party Liability** – tech vendors can be joined to proceedings where failure is traced to their systems.
- **Disclosure Orders** – compel vendors to provide code/audit material under protective orders.
- **Compensation** – damages to EMB or petitioners where vendor negligence caused electoral harm.
- **Apportionment** – responsibility split between EMB and contracted vendor.

Legal justification for burden shifting

1. **Information Asymmetry:** Information Asymmetry: Vendors and EMBs often have full system access and documentation of AI systems. Hence, the court will have to direct full disclosure of the information.
2. **The Black Box Challenge:** Most AI systems are implemented without transparent documentation and mechanisms for ex post review. Proprietary prohibitions frequently protect vendors from releasing their source codes or allowing training transparency, thus

thwarting adversarial testing and judicial oversight. This black box challenge directly imperils legal contestability. Courts should demand minimum disclosure requirements, such as algorithmic transparency and system auditing, as a condition for lawful deployment. Where information asymmetries remain, courts may activate the precautionary principle, leaving the burden of proof on state agencies or vendors to prove system integrity.

3. **Precedential Support:** International courts acknowledged the need for transparency in election technology.

Experts Witnesses Management

Given the technical complexity of AI systems, judicial officers cannot adjudicate such matters alone. Courts may require assistance from:

- **Autonomous experts in AI:** Set up as amici curiae for system performance review/audit.
- **Cross-examining of expert testimony:** To form scientific consensus/challenge technical methodology.
- **Interdisciplinary learning:** Judges should develop core digitally based literacy in order to appropriately balance contending professional arguments.

1. Qualification Standards

- Technical experience in AI/ML systems
- Experience with electoral technology assessment
- Interdependence from parties and technology providers
- Sharpening of problem-solving and decision-making skills

2. Expert Report requirements

- Clear explanation of methodology
- Recognition of system limitation and uncertainties
- The use of non-technical language
- Particular recommendations for consideration in court

Judicial discretion should, therefore, be used in consideration of both the epistemological limits of expertise and the Eirenic values that form the basis for electorate democracy.

Strengthening Chain of Custody and Interim Remedies

Digital evidence is exceptionally vulnerable to corruption, alteration, or even loss. As such, courts should maintain an intense chain of custody for digital materials. Forensic methods, like timestamping and safe storage, serve to ensure evidentiary integrity. Further, for matters in which potential for misusing AI is envisaged in vulnerable pre- or post-election times, courts may issue interim relief for full consideration.

Checklist: AI-Related Electoral Evidence Triage

This is the tool for guiding the admissibility and probative value attached to AI-generated evidence in election disputes. It is non-binding, but serves as a guide in preliminary triage to determine:

- Whether it should be received in evidence;
- How much weight should be attached to the evidence;
- When additional expert interpretation is needed.

Use this checklist at the preliminary hearing stage, or during evidentiary challenge phases of litigation. This checklist is best used in combination with expert reports and a technology-neutral evidentiary framework. It supports, but does not replace, judicial discretion. In borderline cases, preference should be given to transparency, contestability, and remedial flexibility.

Criteria	Key Questions	Notes / Caution
1. Provenance	Is the origin of the data verifiable (e.g. timestamps, metadata, digital chain of custody)?	AI outputs lacking traceable origin may be inadmissible or carry diminished weight.
2. Relevance	Does the evidence directly relate to the electoral outcome, process integrity, or voter exclusion?	Establish nexus between AI function (e.g. biometric verification) and alleged harm.
3. Reliability	Is the AI system or tool used peer-reviewed, certified, or open to inspection?	Black-box systems with no technical validation are contestable. Consider requiring expert scrutiny.
4. Verifiability	Can the outputs or decisions be independently reproduced or audited?	If audit logs, API calls, or training data are unavailable, the evidence's weight should be downgraded.
5. Chain of Custody	Was the evidence preserved, transferred, and submitted without unauthorised modification?	Cryptographic logs or hash-matching may be necessary to prove integrity.
6. Technical Expertise	Has the evidence been interpreted or authenticated by a qualified AI or digital forensics expert?	Where complexity exceeds judicial familiarity, independent experts are strongly advised.
7. Procedural Fairness	Has the opposing party had an adequate opportunity to examine, challenge, or contextualise the evidence?	Due process may be compromised if only one party has technical access or capacity.

Primary or Secondary? Categorizing AI-Generated Evidence

In addition to admissibility and procedure, judges have to entertain a more profound query: what is the legal nature of outputs produced by artificial intelligence? Are such outputs primary evidence, direct reflections of the polling process, or secondary evidence, derivative illustrations that have to be corroborated?

This classification has practical implications for weight, review, and burden of proof. How a court categorizes AI-generated evidence determines whether it is independent or if it is to be corroborated by other records, witnesses, or verification. To inform this decision, courts may look to an orderly framework for when AI-generated may appropriately be regarded as primary evidence, and when it should only be admitted as secondary evidence subject to corroboration.

Framework for Classifying AI-Generated Electoral Evidence

Courts can classify AI-generated evidence as primary or secondary using three evaluative tests that is, the source test, the Human traceability test and the purpose and weight test.

1. **The Source Test** distinguishes direct from derived outputs. Evidence is primary if it directly records the electoral act, such as a biometric scan or raw server log, and secondary if it is a processed interpretation, like anomaly reports or predictive maps.
2. **The Human Traceability Test** takes verification into account. Evidence that is associated with a human act or near-simultaneous machine log, like fingerprint identifications or transmission logs, is first-order, and outputs that only relate to the performance of the AI system, such as sentiment analysis or model predictions, are second-order.
3. **Purpose and Weight Test** requires if evidence is independent or if it is for supporting other proof only. Biometric mismatch confirming duplicate registration could be primary, but flags of abnormal turnout from AI is still secondary, requiring human verification.

Test	Primary Evidence	Secondary Evidence	Judicial Approach
1. Source Test (Direct vs. Derived)	Direct outputs that capture the electoral process at source. Examples: biometric scan at registration; raw vote tally transmission logs.	Processed interpretations of primary data. Examples: anomaly detection reports; AI-generated risk maps; predictive voter trends.	Primary: may stand alone if authenticity is proven. Secondary: requires corroboration from primary records.
2. Human Traceability Test (Original Observer vs. Mediated Record)	Traceable to a verifiable human act or contemporaneous machine record. Examples: fingerprint match record; server log showing transmission.	Not independently verifiable without relying entirely on the AI system. Examples: sentiment analysis dashboard; algorithmic predictions.	Primary: treated like digital documentary evidence. Secondary: needs expert explanation or supporting material.
3. Purpose & Weight Test (Standalone vs. Corroborative)	Can stand on its own as direct proof of a fact in issue. Example: biometric mismatch proving duplicate registration.	Functions mainly as supporting/ corroborative evidence. Example: AI flagging “suspicious turnout” that still needs human verification.	Primary: admissible and weighty once verified. Secondary: admitted with caution, limited weight.

Judicial Implications of Categorizing AI-Generated evidence

As courts categorize outputs of artificial intelligence whether primary or secondary, they influence the evidentiary weight and admissibility of AI evidence in election disputes:

1. **Weight of Evidence**
   - Primary evidence (e.g., raw biometry, server logs) could have significant probative value when properly authenticated.
   - Secondary outputs (such as anomaly reports, sentiment analysis) demand circumspection and lesser weight unless it is validated.

2. **Burden of Proof**
   - Parties in possession of primary evidence need to demonstrate system authenticity, reliability, and integrity.
   - Secondary outputs require corroboration prior to transferring the burden.

3. **Corroboration and Expertise**
   - Secondary evidence of AI is not adequate on its own; primary records or professional interpretation must accompany it.

4. **Judicial Scrutiny**
   - Courts should insist on transparency and interpretability.
   - The less traceable the system, the stronger the presumption toward secondary classification.

7. Judicial Remedies and Reliefs in AI-Electoral Disputes

In the context of electoral justice for which there may be a broad number or type of disputes, judicial remedies and reliefs are essential for ensuring that electoral processes are fair, transparent, and just. This section of the toolkit focuses on three critical guidelines which play a vital role in shaping the effectiveness and fairness of judicial remedies in electoral matters. These guidelines are (1) balancing public interests, (2) timelines principles, and (3) the doctrine of proportionality. This section lists typical disputes that may arise involving the misuse of AI in elections. These disputes may arise at different stages such as the pre-election phase - for example, during the registration process; during the election i.e at the time of polling; and the post-election phase – for example during vote counting and transmission. In addressing these issues, three guiding questions have been used as follows:

i. What legal remedies should courts grant to litigants in electoral disputes involving AI and what are their justifications?

ii. Under what circumstances should courts grant injunctions in pre-election AI disputes?

iii. How should courts balance public interest, urgency and electoral reforms?

1.1 What legal remedies should court grant to litigants in electoral disputes involving AI and what are their justifications?

In litigation concerning electoral disputes that involve artificial intelligence (AI), courts should consider a range of legal remedies to address the unique challenges posed by technology in the electoral process. The following remedies may be used in isolation or in combination depending on the facts and circumstances of each case.

Judicial remedy in the age of artificial intelligence requires both doctrinal innovation and procedural discipline. Remedies should be commensurate with the injury inflicted i.e., restoring fairness without jeopardizing democratic stability. This entails annulments of elections or system-wide transformations being reserved for obvious, result-determinative failures, and less inquisitorial remedies potentially safeguarding more institutional continuity.

Courts also have to achieve haste and legitimacy, ensuring speedy adjudication that doesn't compromise rigor. Where AI mistakes or omissions jeopardize constitutional rights, delays and incomplete decision may erode public confidence. Here, the challenge is not necessarily to decide quickly, but justly, framing remedies that are both reparative and preventative, safeguarding electoral integrity today, but future-proofing it for tomorrow's automated wrongs.

Types of Reliefs

Remedy Type	Description	When It Applies
Declaratory Relief	A court may declare an algorithmic system unlawful, biased, or improperly used, without ordering immediate action.	Appropriate when the issue is systemic or emerging but not outcome-determinative.
Injunctive Relief	A temporary or permanent order to cease or alter the use of an AI system (e.g. halting use of biometric tools, suspending automated content takedowns).	Used when there is an ongoing or imminent rights violation.
Election Re-run / Annulment	In extreme cases, courts may order a partial or full re-run of an election where algorithmic interference materially altered results.	Reserved for demonstrably outcome-determinative failures. Requires high standard of proof.
Restitutive Relief	Voters excluded by faulty systems may be reinstated or offered supplementary voting mechanisms.	Often used where voter registers, biometric scans, or digital ID systems were at fault.
Structural Orders	Courts may order electoral bodies to improve algorithmic transparency, conduct audits, or engage in consultation.	Forward-looking remedy to prevent recurrence, especially in future electoral cycles.
Damages	Rare in public law electoral disputes, but may be available in associated claims (e.g. wrongful exclusion, reputational harm from misclassification).	Only in jurisdictions recognising state liability or hybrid public–private claims.

Proportionality Analysis

The court should consider the following factors when determining the proportionality of the AI harm or failure in the electoral dispute;

1. **Scale of Impact:**
   - Number of affected voters
   - Geographical spread of the harm or problems
   - The pattern of the systemic failure and its demographic distribution
2. **Materiality to Outcome**
   - Comparison between the margin of victory versus the scale of irregularities
   - Potential for changed results

3. **Availability of Alternatives**
   - Availability of remedial measures short of nullification
   - Cost and time implications
   - Public interest in finality versus accuracy
4. **Systemic or isolated incidents**
   - Whether the problems reflect broader system failures
   - Likelihood of reoccurrence
   - Need for precedential clarity

How should courts balance public interest, urgency and electoral reforms?

Courts have a duty to carefully balance public interest, urgency, and the need for electoral reforms when ordering remedies. The following are guidelines in the form of critical principles that the courts should use:

a. **The Stage of the Proceedings:** Whether it is a pre-election dispute, a dispute during elections or post elections has a bearing on the type of remedy to be given. The court should consider whether a temporary or permanent remedy is needed and be very specific in the order as to when the order is to take effect and for how long.

b. **Assessment of Public Interest:** Courts should evaluate the broader implications of their decisions on public confidence and trust in the electoral process always bearing in mind that they are the last bastion of democracy. Whatever remedies the court orders, they should serve to uphold democratic values and protect the rights of voters.

c. **Prioritizing Urgency:** Given the time-sensitive nature of elections, courts should prioritize cases involving AI that could impact the electoral process. Expedited hearings and swift resolutions may be necessary to prevent harm. Timelines with a minimum period of 14 days maybe appropriate (like Kenya) since "justice delayed is justice denied" however "justice hastily given is no justice at all" so use of the word "reasonable" may be more appropriate.

d. **Integrating Electoral Reforms:** Courts must use their rulings to promote necessary electoral reforms. By issuing guidelines or mandating changes in AI practices, courts have a duty to ensure that EMBs adopt more transparent, ethical, and accountable AI usage.

e. **Cross-sector Collaboration:** Fostering trusted cross-sector partnerships with stakeholders such as EMBs (for procedural understanding), data protection authorities (for oversight on data users), ICT regulators (for system standards) civil society organizations and academia (for public accountability and so that the courts are not ahead of the population) regional election bodies (for comparative learning), bar associations, political parties and technology experts (for knowledge sharing that prevents frivolous, vexatious and unnecessary litigation). Ultimately cross-sector collaboration can help the public understand the implications of judgments, rulings and remedies and foster collaborative solutions.

f. **Flexibility and Adaptability:** Courts must approach the electoral dispute with flexibility and adaptability depending on the facts and the circumstances of each case, adapting remedies to the evolving nature of AI technology and electoral practices. This adaptability is crucial for addressing unforeseen challenges that may arise in future elections.

Examples of typical electoral disputes involving misuse of AI

Type of Dispute	Examples
1.3.1 Misinformation and Disinformation - resulting in disenfranchisement	· Misinformation that polling stations will open at 10 am and people come when polling has closed. · Algorithms that facilitate voter manipulation or misinformation · An AI-driven social media campaign spreads false information about a candidate's policies or personal life, potentially swaying public opinion and affecting voter decisions. Disputes may arise over the accountability of the platforms or entities responsible for disseminating such information. · System or technology bias against certain parts of the population · Lack of algorithmic transparency
1.3.2 Delimitation/ Delineation – resulting in disenfranchisement	· Being stopped from registering because they are in the wrong area · Gerrymandering
1.3.3 Failure of systems and voter recognition of technology	· Lack of algorithmic transparency · Poor programming of AI with result that it fails to recognize rural faces as opposed to urban ones · Failure of verification of voting credentials leading to failure to vote
1.3.4 Voter Manipulation	AI algorithms analyze voter data to target specific demographics with tailored messages that may unduly influence their voting behavior. This could lead to challenges regarding the ethical implications and legality of such targeted campaigning.
1.3.5 Algorithmic Bias	An AI system used for voter outreach or engagement inadvertently exhibits bias by favoring certain groups over others, leading to unequal treatment of voters. This could prompt disputes about fairness and compliance with anti-discrimination laws.
1.3.6 Data Privacy Violations	An EMB uses AI to collect and analyze personal data from voters without proper consent or transparency. Disputes may arise over breaches of data protection laws and the unauthorized use of sensitive information.

1.3.7 Miscellaneous • **Erroneous Election Monitoring and Results Reporting** – Failure or Manipulation in electronic transmission of results and declaration – Erroneous Counting of votes – Malfunction in AI vote counting system	• AI tools are employed to monitor electoral processes and predict outcomes based on early voting data. Disputes may arise if the predictions are perceived as influencing voter turnout or if AI analysis is challenged for accuracy and reliability. • Transmission of results by either by fax, mobile phone or email may be compromised. • When it turns out that the counting doesn't reflect the votes on the ground. The votes cast, t raises an issue for determination – the AI could have manipulated intentionally or by malfunction
1.3.8 Fraudulent Activities	An AI system is manipulated to generate fake ballots or alter voting records, leading to disputes about the legitimacy of the election results. Challenges may focus on the security of the AI systems used in the voting process.
1.3.9 Disputes Over AI-Driven Voting Systems	If an AI-based voting system malfunctions or is accused of being hacked, disputes may arise regarding the integrity of the votes cast and the overall election process. This could lead to calls for audits or recounts.
1.3.10 Regulatory Compliance Issues	An electoral commission implements an AI system for voter registration but fails to comply with existing legal frameworks regarding data handling and processing. This could result in disputes over the validity of registered voters and the legality of the electoral process.
1.3.1 1ransparency and Accountability	A political party or candidate may challenge the transparency of AI algorithms used in electoral processes, arguing that proprietary systems lack oversight and could manipulate outcomes. Disputes may focus on the need for transparency in algorithmic decision-making.

8. Judicial Ethics and AI Use

Guidelines for Courts in Electoral and Governance Cases

AI is increasingly used in both judicial administration and in the electoral systems brought before the courts. While promising efficiency, these tools also present distinct ethical challenges. Judges must safeguard independence, impartiality, and public confidence in justice when AI enters the courtroom – either directly or indirectly.

Key Ethical Risks

- **Overreliance:** AI outputs may subtly shape judicial reasoning, embedding systemic bias.
- **Confidentiality:** Use of external AI tools may compromise sensitive case materials.
- **Transparency:** Where AI materially informs a judgement, disclosure may be required to preserve fairness and parties' rights.

Normative Anchors

Judicial reliance on artificial intelligence in electoral disputes must be situated within existing ethical frameworks. While AI offers efficiency and data-driven insights, its use risks undermining judicial independence, impartiality, and public trust if not anchored in clear normative standards.

The Bangalore Principles of Judicial Conduct (2002) establish independence, impartiality, equality, and diligence as non-negotiable values of the judiciary.[4] In an AI context, over-reliance on opaque tools could erode independence, algorithmic bias could violate equality, and diligence requires judges to understand AI's limitations. These principles provide the universal baseline: AI can never substitute judicial reasoning, only support it.

The Council of Europe's CEPEJ Ethical Charter on AI Justice (2018) goes further, directly addressing algorithmic risks.[5] It requires that AI tools used in judicial systems respect fundamental rights, remaining transparent under judicial control. This makes explicit the fact that judges must never defer uncritically to automated outputs, and that explainability is a prerequisite for AI adoption in courts.

Complementing these institutional standards, the Council of Bars and Law Societies of Europe (CCBE) Statement on AI in the Justice Sector (2023) warns of the "black box" problem and insists that judicial discretion cannot be replace by automation.[6] The CCBE links technical opacity with erosion of due process and public trust, which is a vital concern in electoral disputes where legitimacy is on the line. Together, these instruments form a layered normative framework: universal principles (Bangalore), European AI-specific ethics (CEPEJ), and professional legal guidance (CCBE). Applied to electoral disputes, they converge on a simple but robust standard: ***AI may assist judges but never displace them.***

[4] [THE BANGALORE PRINCIPLES,2002.]

[5] [CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment - European Commission for the Efficiency of Justice (CEPEJ).]

[6] [EN_ITL_20230525_CCBE-Statement-on-the-use-of-AI-in-the-justice-system-and-law-enforcement.pdf.]

Practical Application

Judges should approach AI with caution, guided by three principles:

1. **Maintain Human Oversight:** AI may inform but never substitute judicial reasoning.
2. **Safeguard Confidentiality:** Avoid processing case-sensitive data through unsecured or commercial tools.
3. **Demand Transparency:** Require disclosure of AI use by parties and consider whether judicial reliance on AI should itself be disclosed.

Model Judicial Questions

Courts adjudicating AI-related disputes should consider probing the following:

- ***What independent certification preceded this system's deployment?***
- ***What audit mechanisms exist to test accuracy and bias?***
- ***Who retains custody of training data and decision logs?***
- ***What safeguards exist for voter privacy?***
- ***What remedy applies if discriminatory outputs are proven?***

9. Simulated Scenarios for Judicial Engagement

- **Disputes surrounding the use of AI in elections could arise at three different levels: pre-election, election day (on days of elections) and post-election.**
- **All levels entail critical choice that could be mediated or swayed by Artificial Intelligence, and therefore pose legal questions for the courts to determine.**
- **Thus, the scenarios envision the wide range of conflicts that could emerge, yet keep their feet firmly planted in the constitutional and normative systems of African law systems.**
- **Various scenarios can be generated from these three levels. Each scenario highlights key legal issues, findings, and possible judicial remedies. These examples assist EMBs and legal practitioners in anticipating complex disputes and tailoring principled responses.**

Scenario One

Disputes Arising from the Integrity of the Voter Register in the Context of AI Deployment

Issues: Duplicate, deceased, or excluded voters; biometric data privacy; systemic bias.

- Identify infringements on the right to vote and political participation.
- Assess biometric data handling and data protection compliance.
- Verify anomalies flagged by audits or expert testimony.
- Evaluate impact on voter roll accuracy and possible disenfranchisement.

Reliefs: Consider mandamus for audit, registration extension, and monitoring mechanisms.

Scenario Two

Disputes Arising from Malfunction and Manipulation in Electronic Transmission of Election Results

Issues: System failures, manual overrides, data discrepancies, potential tampering.

- Determine if technical failures compromise election transparency and integrity.
- Cross-check electronic vs manual result records for discrepancies.
- Assess fairness where failure unevenly affects constituencies.
- Evaluate need for recounts, annulments, or fresh elections.

Reliefs/Orders: Consider criminal referral if fraud or tampering is evident.

Scenario Three

Disputes Arising from AI-Assisted Electoral Boundary Delimitation

Issues: Unequal constituency sizes, outdated data, partisan bias, disenfranchisement.

- Examine equality of the vote principle and demographic accuracy.
- Assess claims of partisan manipulation in AI algorithms.
- Verify timely and transparent public notification of boundary changes.
- Consider suspension or correction of delimitation process with judicial oversight.

Reliefs/Orders: Order equitable redistribution of development resources if applicable.

Scenario Four

Disputes Arising from AI-Driven Misinformation and Disinformation Affecting Voter Turnout During the Campaign Period

Issues: Deepfakes, false security alerts, polling misinformation, voter suppression.

- Investigate how misinformation interferes with voter participation and rights.
- Balance freedom of expression with electoral fairness.
- Assess targeted disenfranchisement and discriminatory impacts.
- Consider nullification or rerun where misinformation decisively impacted results.

Reliefs/Orders: Order improvements in EMB digital communication and refer deliberate disinformation for prosecution.

Scenario Five

A Futuristic Legal Challenge for a Fully Electronic Electoral Process

Issues: Progressive realization of voting rights, equality in access, electoral transparency.

- Evaluate State's duty to adopt effective technological means to protect voting rights.
- Assess risks of mixed systems privileging certain demographics.
- Review safeguards for accessibility, data protection, and auditability in electronic systems.
- Consider phased transition plans with legislative and EMB accountability.

Reliefs/Orders: Ensure continued use of hybrid systems is conditional and monitored.

Annexures

ANNEX I

AI & Elections Remedies Matrix

Scenario	Judicial Findings	Remedies	Implications
1. Legal Challenge to Use of AI in Voter Registration	**- Constitution permits tech-enabled elections -** EMB has duty to implement accessible tech	**- Declare duty to progressively implement e-voting** - Mandate enabling legislation- Require EMB roadmap- Conditional approval for hybrid systems with oversight	**- Creates legal basis for AI use -** Pressures EMBs to modernise- Sets precedent for tech-enablement with accountability
2. Algorithmic Candidate Disqualification	**- AI system lacked transparency** - Violated due process rights- Disproportionate impact on marginalised candidates	**- Nullify disqualification** - Require human oversight in decision-making- Mandate AI transparency and explainability standards	**- Elevates procedural fairness** - Curtails unchecked automation- Requires hybrid human-machine processes
3. Electoral Disinformation Amplified by AI	**- Disinformation harmed voter autonomy -** Platform moderation algorithms lacked safeguards- Election not free and fair	**- Require independent content audits -** Impose algorithmic impact assessments- Temporary suspension or correction mechanisms	**- Sets accountability standards for platforms -** Expands EMB oversight beyond physical voting- May prompt legislative updates on digital campaigning
4. Biometric Verification Failure on Voting Day	**- Discriminatory or faulty biometric systems -** Disenfranchised eligible voters- Violated right to vote	**- Order re-runs in affected areas -** Require biometric system audits- Mandate fallback authentication options	**- Encourages robust system testing -** Mandates inclusivity in tech deployment - Elevates remedy for tech-induced disenfranchisement
5. AI Audit Trail Tampering or Loss	**- Integrity of AI system compromised** - No verifiable record of results- Legal standard of proof not met	**- Annul results in affected precincts -** Require immutable logs, audit trails- Mandate real-time integrity checks in future systems	**- Highlights need for digital evidence standards -** Anchors remedy in verifiability - Spurs investment in AI-forensics tools

ANNEX II

Glossary of AI Terminology (extended):

Term	Definition (Plain Language)	Technical Note / Mechanism	Relevance to Electoral Disputes
AI (Artificial Intelligence)	Computer systems performing tasks normally requiring human intelligence	Includes machine learning, NLP, computer vision, neural networks	AI can automate voter registration checks, result transmission, or campaign monitoring, raising questions of transparency and reliability
Algorithm	Step-by-step instructions a computer follows to make decisions	May be deterministic or probabilistic	Determines outcomes like vote tallying or voter eligibility; errors can disenfranchise voters
Machine Learning (ML)	Subset of AI where systems learn patterns from data	Supervised, unsupervised, reinforcement learning	Bias in training data can affect automated decisions in voter registers, candidate visibility, or boundary delimitation
Deep Learning	ML method using multi-layered neural networks	Often used in facial recognition or image processing	Raises opacity issues ("black box") in voter identification and biometric verification
Explainability	Ability to understand why an AI system made a decision	Includes model interpretability, feature importance, audit logs	Crucial for courts to assess AI fairness, reliability, and compliance with electoral law
Bias	Systematic error leading to unfair outcomes	Can be dataset-driven, model-driven, or human-driven	May result in exclusion of certain voter groups or skewed electoral boundary outcomes
Transparency	Clear visibility into AI processes, datasets, and decisions	Open-source models, audit trails, documentation	Courts require transparency to verify electoral integrity and accountability
Audit Trail / Log	Record of system operations and decisions	Includes input data, processing steps, and outputs	Provides evidence in disputes regarding AI outputs and potential manipulation
Voter Verification / Biometric Authentication	Use of physical or biological traits to confirm identity	Fingerprints, facial recognition, iris scans	Misidentification or duplication can compromise right to vote and election integrity

Algorithmic Accountability	Holding systems and operators responsible for outputs	Documentation, certification, independent audits	Ensures vendors and EMBs can be held liable for errors affecting elections
Data Privacy / Protection	Safeguarding personal data from misuse	Compliance with GDPR-like or national privacy laws	Critical when AI processes voter data; breaches may violate constitutional rights
Disinformation / Deepfakes	False or manipulated content designed to mislead	Synthetic media, AI-generated audio/ video	Suppresses voter turnout, misguides electoral choice, raises questions of freedom of expression vs. manipulation
Black Box System	AI whose internal workings are not easily interpretable	Complex neural networks or proprietary algorithms	Judicial challenge: difficult to assess reliability, bias, or compliance with legal standards
AI Certification / Validation	Independent assessment confirming system reliability	External audit, stress testing, bias evaluation	Supports courts in weighing admissibility and reliability of AI evidence

References

https://www.saflii.org/za/cases/ZACC/2018/17.html

https://www.thecable.ng/electoral-justice-kenya-nigeria/?utm_source=chatgpt.com

https://guardian.ng/news/cso-faults-scourt-verdict-on-electronic-voting/?utm_source=chatgpt.com

NOTES

NOTES

Get in touch **with us:**

YIAGA
Website:
www.aiandelectionsinafrica.yiaga.org
/yiaga

AJJF
Website:
africajurists.org/aiandelectionsinafrica
LinkedIn /africajurists

SEACJF
Website:
seacjforum.org/aiandelectionsinafrica
/seacjf