# Lessons on the Use of Technology in Elections

## Election Case Law Analysis Series

ELECTION JUDGMENTS

CASE LAW SERIES | PART 3 | NOVEMBER 2022

# Lessons on the Use of Technology in Elections

## Election Case Law Analysis Series

*Ronan McDermott*

*Rebecca Cox*

*Typhaine Roblot*

**With Contributor**

*Catherine Murphy*


International Foundation
for Electoral Systems

ELECTION JUDGMENTS

# Election Case Law Analysis Series

With support from the United States Agency for International Development (USAID) and the Swedish International Development Cooperation Agency (Sida), in 2021, the International Foundation for Electoral Systems (IFES) launched ElectionJudgments.org, a curated global database that makes judicial decisions on election cases of all types more transparent and accessible. It is a resource for judges, election professionals, policymakers, and researchers who are working to resolve disputes and prevent violations to promote more credible elections around the world.

To facilitate the exchange of sound precedents across jurisdictions, IFES has used this database to conduct an initial analysis of critical judgments on a variety of topics, presented in an Election Case Law Analysis Series. This paper is the third in this series, focused on the resolution of electoral disputes that concern the use of election technology. Prior issues in the series are below:

Issue 1: Lessons on Gender Equality and Women's Political Participation
Issue 2: Lessons for Regulating Campaigning on Social Media

The ElectionJudgments.org database is updated on a periodic basis. To contribute judgments or resources, please use the appropriate form here or contact us via our website.

# About IFES

IFES advances democracy for a better future. We collaborate with civil society, public institutions and the private sector to build resilient democracies that deliver for everyone. As a global leader in the promotion and protection of democracy, our technical assistance and applied research develops trusted electoral bodies capable of conducting credible elections; effective and accountable governing institutions; civic and political processes in which all people can safely and equally participate; and innovative ways in which technology and data can positively serve elections and democracy. Since 1987, IFES has worked in more than 145 countries, from developing to mature democracies. IFES is a global, nonpartisan organization based in Arlington, Virginia, USA, and registered as a non-profit organization [501(c)(3)] under the United States tax code.

## IFES By The Numbers

**Reached 25M+** people with civic and voter education in 2021

**Supported 30** elections in 2021, training 300K+ election officials

**Worked across 58** countries in 2021

# Table of Contents

ELECTION JUDGMENTS

# Executive Summary

With support from the United States Agency for International Development (USAID) and the Swedish International Development Cooperation Agency (Sida), in 2021, the International Foundation for Electoral Systems (IFES) launched ElectionJudgments.org, a database for national election judgments from around the world. IFES has used this database to conduct an initial analysis of select judgments that involve the use of technology in elections by Election Management Bodies (EMBs). These cases show that with the constant evolution of technology and its use in elections, judges and judicial officials need to understand how technology is being used in voter and candidate registration, voter identification, the voting or counting process, and results tabulation and transmission, and re-assess both the conduct of proceedings and the availability of effective judicial orders and remedies. It is also essential that other election stakeholders — in particular parties, candidates and their agents — have a thorough understanding of election technology so they can support well-founded complaints.

Our case law analysis identified the following key lessons:

1. Given a growing lack of trust in election processes, it is vital that there is maximum transparency by the EMB around the introduction, testing, and use of election technology.
2. Similarly, in order to build trust in rulings, courts or tribunals should maximize transparency in election dispute resolution proceedings.
3. It is important for judges, judicial officials and all electoral stakeholders to have a basic literacy in the technologies being procured and used in the election process. While maintaining judicial independence and EMB independence is crucial, inter-institutional dialogue between the EMB and courts should be encouraged prior to elections to enable courts to effectively address disputes involving election technology and apply remedies that are appropriate to the operational situation and electoral timeline.
4. Election observers should understand the use of election technology and have observation methodologies that account for its use, especially as observer reports may be used as corroborating evidence in proceedings.
5. Courts should review and adapt court procedures as needed for election cases to consider digital evidence, chain of evidence, expert testimony, and e-discovery in order to expedite proceedings.
6. The EMB needs to ensure transparency for code and procurement processes
7. A physical vote record is important to enable auditability of electronic voting technology.
8. EMBs should ensure control over the design and implementation of technology systems procured from third party suppliers, including to be able to produce credible data quickly in case of a dispute. This requires clear ownership or licensing of intellectual property, and transparency in procurement processes, technology code, and system updates.

9. EMB and courts should also carefully consider protection of data integrity by ensuring adequate storage, record and archiving to manage data collected or shared, to guarantee protection of privacy rights and to ensure adequate cybersecurity protections to avoid theft or manipulation of data during court proceedings.

# Introduction

The use of technology in elections is continuously evolving. Technology touches almost every part of the election process, including voter and candidate registration, voter identification, voter education, voting, counting, results transmission and complaints management. In the last decade, multiple publications have explored the advantages and disadvantages of using different forms of technology in elections and attempted to define standards for its use.[1] As more countries establish digital voter registries and develop electronic results transmission systems, allegations about the actual or perceived misuse of technology can result in contested elections and complex litigation. A lack of transparency can provide an opening for those interested in sowing mistrust and confusion to do so, eroding public confidence in elections and democratic institutions.[2] This analysis of select jurisprudence involving election technology within the election infrastructure (that is, within the election process itself, not just in day-to-day work of the EMB) reveals the importance of sufficient auditability in the EMB's use of technology, and transparency in court proceedings. Transparency can help enhance understanding by all stakeholders of how a specific technology functions, which in turn assists with building or preserving public trust in both the election process and the adjudication of election complaints (including any scrutiny or audit process involving election technology).[3]

Different types of election technology can fail for a myriad of reasons, including procurement problems, institutional capacity constraints, lack of network coverage, or other factors outside the direct control of the EMB.[4] As noted above, technology can also be deployed effectively, but nonetheless become a vector for disinformation. Given that elections are increasingly litigated, judges need to be prepared to deliberate on a range of issues involving technology, including procurement, piloting, testing, deployment, auditability, and security. Transparency in each of these phases is a condition precedent for audibility. If allegations around election technology are brought to the courts, the judiciary may need to adapt rules of procedure to allow for the consideration of digital evidence and the involvement of ICT as experts during proceedings or as *friends of the court* (amicus curiae). The task of judges in these cases will also be made easier if they have the opportunity to familiarize themselves with the technology and its intended use by the EMB before the election begins.

> "African countries are migrating from manual processes to using election technology, so knowledge of the court on technology become more prominent. Courts have a greater role to play in sorting out these disputes."
>
> - *Justice Maria Kawimbe, High Court of Zambia*

[1] Impact of technology on democracy: https://rm.coe.int/study-on-the-impact-of-digital-transformation-on-democracy-and-good-go/1680a3b9f9; Venice Commission, Study on the Use of Digital Technology: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2020)037-e;

[2] Why public trust in elections is being undermined by global disinformation campaigns, Bluth Christopher, theconversation.com, April 28, 2022.

[3] The Council of Europe, Guidelines on use of ICT in electoral processes, February 2022 makes recommendations on transparency regarding the ICT including: communicating about the development and decision process, providing information on the feasibility of the overall implementation, on procurement of the solution, providing information on how conflicting or competing principles such as privacy and secrecy versus transparency are to be addressed, and publishing the source code.

[4] Late changes to legal and regulatory frameworks, lack of adequate time to procure, poor operational planning, environmental realities (lack of power or connectivity at remote polling locations) – these are not technology problems per se but feature heavily in the narratives surrounding failed election technologies.

This paper presents an analysis of select court judgments from IFES' database, ElectionJudgments.org, involving the use of election technology, and compares additional procedural issues raised by electoral judges globally, including evidentiary rules, effective investigation, protection of integrity of data, and the application of timely and effective remedies. Three key points emerge from the jurisprudence: ***First, the court judgments examined in this analysis raise procedural specific challenges for judges*** in light of the seven standards for election dispute resolution identified by IFES in our 2011 *Guidelines for Understanding, Adjudicating, and Resolving Disputes in Elections*. This includes the right to an effective remedy, the right to a fair trial, and the importance of a prompt, independent, effective and thorough investigation.[5] Our analysis shows that electoral judges may need to adapt their methods of fact-finding and analysis of election technology[6] in relation to access to and admissibility of evidence, and to clearly determine the roles and responsibilities of those conducting investigations and audits.

***Second, this analysis reveals the importance of election officials ensuring a verifiable election process that can be corroborated by an audit to allow judges to quicky assess alleged irregularities or fraud.*** The need for verifiability of an electronic vote is a recommendation of the Venice Commission's Code of Good Practice on Electoral Matters and the Council of Europe's Recommendation on Standards for E-Voting.[7] Mircea Preotescu, Head of the Coordination Department of the Permanent Electoral Authority of Romania has observed that "[w]e must use technology, but it does not have to be the baseline. We also need to be able to conduct an audit. The paper trail is one of the most important aspects in elections, and that paper trail should be audited so that we can prove the accuracy of the results when technology fails us."[8] In IFES' Guide on Risk Limiting Audits, the authors reference the Indian Supreme Court ruling that all voting machines must be equipped with printers to provide "voter verifiable paper audit trails" (VVPAT) to "allow each voter to verify that his or her intended selections are correctly printed."[9]

***Third, this analysis suggests that it is essential for EMBs to familiarize judges and stakeholders with the type of technology that will be used in the election process and discuss access to evidence well in advance of elections.*** It is indeed crucial for judges to be *informed* in order to assess the verifiability, accuracy, and authenticity of a particular technology or the underlying information used in the technology (e.g., voter information on voter rolls, compared to votes cast) and its larger impact on the election process. Standards against which to situate the use of technology within existing election laws are underdeveloped and require further attention. Collaboration between EMBs and courts prior to the election can assist with this – bearing in mind the need to preserve the independence of both institutions. The joint trainings held between the judiciary in Kenya and the IEBC on the use of technology

[5] Chad Vickery ed., Guidelines for Understanding, Adjudicating, and Resolving Disputes in Elections (GUARDE), IFES, 2011, which sets out seven international standards applicable to electoral complaints and appeals processes. These legal standards stem from widely recognized fundamental rights, such as the right to participate in government; the right to a fair and public hearing; the right to an effective remedy and access to justice.
[6] United Nations, on behalf of the Office of the United Nations High Commissioner for Human Rights (OHCHR), and the Human Rights Center at the University of California, Berkeley, School of Law, Berkeley Protocol on Digital Open Source Investigations, 2020. Foreword.
[7] The Venice Commission Code of Good Practice on Electoral Matters 2002, paragraph 3.2 iv recommends "electronic voting should be used only if it is safe and reliable; in particular, voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage; the system must be transparent"; the Council of Europe's Recommendation on Standards for E-Voting CM/Rec (2017)5 says at paragraph 15 that electronic voting must be verifiable, and the Guidelines on Implementation at paragraph 15 explain that member states should consider the use of paper ballots for verification purposes.
[8] Intervention made during the third meeting of the Europe and Eurasia Regional Electoral Justice Network in May 2021.
[9] Mohanty, V., Akinyokun, N., Conway, A., Culnane, C., Stark, P. B. & Teague, V. (2019). Auditing Indian Elections. p. 2. Retrieved from: https://arxiv.org/pdf/1901.03108.pdf. See IFES Risk Limiting Audit: A Guide. (2021).

contributed to the quality and timely performance of the audit of IEBC servers and logs in the recent Kenyan 2022 presidential election process.[10]

## What is Election Technology and its Role in Elections?

Election technology is broadly defined as the information and communication technologies (ICT) used in the planning, management, and conduct of elections. The use of election technology[11] includes the digitization of information, including text, pictures, or sound; the digital data stored in a computer system; and the processing of the information, such as the biometric matching algorithms that are used to identify duplicate voter registrations. Increasingly, technology is used to supplement or otherwise augment various parts of the election process, such as voter registration and results transmission. Regardless of the type of technology used, the integrity of the system is of paramount importance. There are no specific international standards for the use of technology in elections, save for the regional standards recently developed by the Council of Europe and the Venice Commission.[12] However, general international standards on elections still govern the use of technologies, for example, guaranteeing the secrecy of the vote, ensuring privacy and data protection rights, accessibility for all, and requiring integrity and transparency of the election process. In addition, general international standards around cybersecurity are applicable to elections.

**Examples of technology used in the electoral process:**

- ***Biometric identification*** *– de-duplication of voter registries, voter authentication/identification at the polling station*
- ***Mobile device with access to internet*** *– voter registration, voter authentication / identification, electoral results transmission*
- ***Web servers*** *– dissemination of electoral information and transmission of results, online registration of political parties and candidates, submission of political finance compliance documentation*
- ***Electronic voting*** *– using electronic means to assist with casting ballots.*
- ***Optical scanning*** *– used for counting of marked paper ballots*
- ***Cryptography*** *– any electoral process requiring the protection of confidentiality (encryption, for example storage of voter biometrics in voter registration systems) or integrity (cryptographic hashing, for example, to establish or preserve chain of custody of digital evidence in EDR)*
- ***Geographic Information Systems (GIS)*** *– mapping constituency boundaries, interactive maps for registration and voting*

[10] Odinga & 16 others v Ruto & 10 others; Law Society of Kenya & 4 others (Amicus Curiae) (Presidential Election Petition E005, E001, E002, E003, E004, E007 & E008 of 2022 (Consolidated)) [2022] KESC 54 (KLR) (Election Petitions) (5 September 2022) (Judgment).
[11] The three-layer description is based on "Digital Technologies In Elections - Questions, lessons learned, perspectives," Ardita Driza Maurer, Council of Europe, March 2020. The first layer of digital technology in elections is the digitization of information, including text, pictures, or sound. A good example of this is the scanning of a candidate nomination form into a computer. Simply, this first layer is the process of taking something that is happening in the real world and putting it into a digital format. The second layer of electoral technology is the digital data stored in a computer system. For example, the payroll information for temporary election or poll workers that is stored on computers in an EMB office. The third layer is where the information is processed. For example, biometric matching algorithms that are used to identify duplicate registrations.
[12] See Compilation of Venice Commission Opinions and Reports concerning Digital Technologies in the Electoral Process (2018); Council of Europe, Guidelines on use of ICT in electoral processes, February 2022; Council of Europe CM/Rec(2017)5 of the Committee of Ministers to Member States on Standards for e-voting and Guidelines.

Legal frameworks governing election technology are diverse, ranging from legislation that provides for the optional use of technology by the EMB (Nigeria),[13] laws requiring a paper trail (some U.S. states), to mandatory requirements for the procurement and use of technology within strict deadlines (Kenya) or strict rules on piloting and testing (Albania). Some electoral laws refer to specific standards for the use of technology in elections, such as Albania's requirement that the identification, selection, and use of ICT be subject to the "principles of legality, transparency, inclusiveness, security, efficiency, and sustainability."[14] As noted by Justice Dr. Kachale, Chairman of the Malawi Election Commission, "A prescriptive legal framework on technology for EMB can generate more challenges before the court," and added "that whatever technology you use, it must speak to the legislative framework" to ensure the EMB has the legal basis to operate this technology in the election.[15]

## Impact of the Use of Technology on Election-Related Court Proceedings and Remedies

Courts have at times struggled to keep up with advances in technology and their implications on elections. In situations of disputed elections, this can present real world consequences. In 2018, during the launch event for the Europe and Eurasia Electoral Justice Network, Luie Tito F. Guia, former Commissioner of the Philippines Election Commission, referred to the importance of an "Analog Mindset in a Digital Process" when describing the slow adaptation of the EDR process to new technology used in Philippines elections (optical scan counting and electronic results transmission).[16] More than a decade ago, the use of technology in the 2010 Philippines elections provided important lessons for electoral judges and other electoral stakeholders:

> "A lack of IT training and tools for observing the new technologies made it difficult for party agents to collect the necessary evidence to support their candidates' claims…Parties also pointed to the importance of making sure the courts have the IT capacity to effectively rule on technology-related cases…[and] noted that the cost of filing complaints has increased, since parties have to hire more specialized legal and IT expertise…and educate themselves…about the new technologies."[17]

As new technology platforms are introduced in elections, new procedural issues may emerge around access to and admissibility of digital evidence. Digital evidence at its broadest level refers to data collected using digital mediums. This data can include (but is not limited to) videos, emails, photos, scans of results forms, open-source data, data

[13] Section 47 Nigeria Electoral Act (2022): The act makes provisions for electronic accreditation of voter using the Smart Card Readers or any technological device as may be determined by INEC.
[14] Albania, Electoral Code. 2020. Operational testing must take place in public sessions by randomly selecting from each electoral administration zone at least three percent of therein used systems, and with no less than 50 participants. Use of Electronic Voting in the Albanian Parliamentary Elections in 2021.
[15] Africa Electoral Jurisprudence Network Conference, 2ND Annual Meeting, Lilongwe Malawi, July 19-20, 2022.
[16] Presentation by Commissioner Luie Guia, Commission on Elections, Philippines in his presentation at the launch event of the Europe and Eurasia Electoral Justice Network workshop in Vilnius in 2018 - Working Group September 5, 2018.
[17] National Democratic Institute, Challenges and Recounts: Political Parties and the Complaints Process in the Philippines (2010).

from voter list, IP protected system social media posts or pages, and metadata.[18] Various technologies can be used to obtain digital evidence from devices such as voter identification kits, for example, to locate where and when the device was used. The increasing use of digital evidence offers new opportunities and challenges, including how to ensure its accuracy and authenticity. While the use of digital evidence such as smartphone photographs of results form can be helpful for electoral stakeholders who wish to document violations or irregularities, this can present new challenges for investigators in corroborating violations, and for courts that need to determine the authenticity of this evidence in a short timeframe. A different problem faces stakeholders who wish to bring complaints about technology platforms used by an EMB (such as an electronic results tabulation system) that relies on complex program code. Unless there has been extensive training of candidate agents and lawyers, and unless there is sufficient transparency in the use of the specific election technology, electoral contestants may lack the technical expertise to bring well-founded complaints or conversely for EMBs to respond to frivolous complaints that seek to sow doubt in the electoral process or result.

Some election courts have regulated the use of digital evidence in their rules of procedure (for example, the Philippines Senate Election Tribunal) and some courts have incorporated digital evidence as part of their rules of evidence or because their country's statute on evidence, while not specific to elections, applies to election proceedings. Digital evidence is increasingly relied upon in court. For instance, the International Criminal Court has shifted away from witness testimony in favor of digital documentary evidence.[19] However, determining the veracity of such evidence can be challenging. The United Nations Berkeley Protocol on Digital Open-Source Investigations states that, "One of the greatest challenges…is dealing with the discovery and verification of relevant material within an increasing volume of online information, especially photographs and videos captured on smartphones and other mobile devices, some of which may be compromised or misattributed."[20]

Courts and tribunals have also faced complexity in gathering and interpreting digital forensics and have reached different interpretations on what counts as valid forensics or how discovery has to be provided (in terms of format, reasonableness of request, etc.). In Kenya, the scrutiny of results forms ordered by the Supreme Court in the 2017 elections was managed by the Deputy Registrar who had not received specific training on the technology used to scan and transmit results forms. But in preparation for the 2022, the Judicial Committee on Elections (JCE) conducted a series of training for all judicial actors on election voting and counting procedure, the voting identification, and the results transmission system. In *Curling v. Raffensperger,* the court in the U.S. State of Georgia relied on a series of ICT expert testimonies relating to the disputed 2020 elections, but investigative measures undertaken by experts may carry their own challenges, such as impartiality of the expertise.[21] Finally, analysis of the jurisprudence also shows that courts have adopted very different types of remedies, with some courts taking into consideration the time needed for the EMB to implement required changes in election technology. Ultimately, digital evidence has been interpreted

[18] Council of Europe Guidelines on Electronic Evidence in Civil and Administrative Proceedings.
The Council of Europe guidelines on electronic evidence explain that this is a broad definition of "electronic evidence." It may take the form of text, video, photographs or audio recordings. Data may originate from different carriers or access methods, such as mobile phones, webpages, onboard computers or GPS recorders, including data stored in a storage space outside the party's own control. Electronic messages (e-mail) are a typical example of electronic evidence, as they originate from an electronic device (computer or computer-like device) and include relevant metadata.
[19] *PILPG Expert Roundtable: Civil Society Documentation, Use of Digital Evidence in International Courts (January 21, 2022)*.
[20] United Nations, on behalf of the Office of the United Nations High Commissioner for Human Rights (OHCHR), and the Human Rights Center at the University of California, Berkeley, School of Law, Berkeley Protocol on Digital Open Source Investigations, 2020. Foreword.
[21] U.S. State of Georgia, Curling v. Raffensperger.

and utilized by courts in a variety of often conflicting ways. Domestic, regional, or international standards for how to respond are nascent to non-existent with regard to EDR proceedings. Incorporating technology — especially brand-new technologies — into the electoral process has the potential to complicate subsequent dispute litigation and may invite contestation.

# Issues Related to Technology Used in Elections

## Issue 1: Verifiability of Votes in the Use of Electronic Voting Machines

This section examines case studies from Germany (2005) and India (2013) to highlight the importance of verifiability of votes in the use of electronic voting machines (EVMs). In both cases, the lack of transparency around results — spurred by a lack of public trust in voting machines — led to distrust in the elections and their outcomes.

Following the 2005 Federal Bundestag elections in **Germany**, complainants alleged that the electoral laws and specific EVMs used violated the principle of the "public" nature of elections, under which the essential steps of an election should be "subject to the possibility of public scrutiny." [22] The Federal Constitutional Court of Germany ruled on two complaints about the use of computer-controlled voting machines.[23] The central question was whether the use of EVMs was unconstitutional for not meeting the public scrutiny requirement and, if so, whether this presents sufficient ground to annul the elections. The complainants sought to invalidate the elections and to repeat them with voting papers and ballot boxes. They also alleged that the principle of equality had been violated by the differential treatment of voters who used voting slips and voters who used EVMs. In its 2009 judgment, the court ruled that one of the laws in question did permit voting machines without effective monitoring of voting or results and was therefore unconstitutional. The court found that the EVMs used were incompatible with the principle of public scrutiny; votes were recorded only on an electronic storage medium, so voters could not verify their votes, and could only see that the machines had registered a ballot. The court found that no procedure should render the voter unable to verify "whether his or her vote is unfalsifiably recorded and included in the ascertainment of the election result, and how the total votes cast [were] assigned and counted." However, in terms of remedies the court did not dissolve the Bundestag, saying that without evidence of manipulation or evidence that results would have been different without the EVMs, there was no sufficient reason to invalidate the elections. It is also worth noting that the court's judgement was issued four years after the 2005 elections, and that elected officials in the Bundestag had been sitting for almost a full term.

The 2013 case *Swamy v. Election Commission* in **India** raised the question of whether the EVMs that had been introduced in India met international standards for elections, notably due to the absence of a paper trail to record votes in the EVM.[24] The petitioner in the High Court of Delhi sought an order requiring the Electoral Commission of India (ECI) to implement modifications to the EVMs,[25] arguing that the EVMs were open to manipulation. In its response, the ECI argued that the system was impossible to hack. The High Court dismissed the petition, and the petitioner, a member of parliament, appealed to the Supreme Court. The petitioner claimed that EVMs should have

[22] Federal Constitutional Court of 3 March 2009 – 2 BvC 3/07, 2 BvC 4/07 – regarding the use of electronic voting machines (EVMs) in the 2005 Federal Bundestag elections.
[23] Federal Constitutional Court of 3 March 2009 – 2 BvC 3/07, 2 BvC 4/07 – regarding the use of electronic voting machines (EVMs) in the 2005 Federal Bundestag elections.
[24] Swamy v. Election Commission (2013, India).
[25] The petitioner sought the issuance of a writ of mandamus/direction(s) directing the Union of India, the Chief Election Commissioner and the Technical Experts Committee (Respondent Nos. 1-3) to effect the necessary modifications in the EVMs so as to allow the voters to verify their respective votes and to attach the printers to the EVMs with a facility to print the running record of the votes for the purpose of verification by the voters in the process of voting. He also sought a direction to frame guidelines and to effect necessary amendments in the Conduct of Election Rules, 1961.

a paper trail as a safeguard, as was common practice in other countries. The Supreme Court agreed and held that "the paper trail is an indispensable requirement of free and fair elections. The confidence of the voters in the EVMs can be achieved only with the introduction of the 'paper trail.' EVMs with VVPAT [voter-verified paper audit trail] system ensure the accuracy of the voting system."[26] The ECI and other stakeholders argued that the VVPAT system was the best option to provide an auditable paper trail but noted that it required time for full implementation. The court allowed the ECI to introduce paper trails through the VVPAT system gradually, given there were more than one million voting booths that would need modification.

Contrary to the jurisprudence in Germany, the court in India did not challenge the overall use of voting machines, but instead focused on the verifiability of the system — giving time for the EMB to progressively operationalize the required system country wide. This case is further discussed in IFES' 2021 paper, *Risk Limiting Audits: A Guide for Global Use*.[27]

## Issue 2: Ensuring a Secure, Transparent and Verifiable Electronic Results Transmission System

Transparent and verifiable results transmission systems are critical for ensuring free and fair elections. This section examines case studies in Malawi (2019) and Kenya (2017) where improper or incomplete mechanisms for electronic results transmission resulted in elections being declared null and void.

In 2019, in *Chilima vs. Mutharika and Election Commission*, the **Malawi** High Court addressed a petition challenging the results of the presidential election that raised constitutional issues. After months of investigation, and after the president had already been inaugurated, the court annulled the elections and ordered fresh elections to be held within 150 days of its judgment, which was upheld by the Supreme Court. The flawed use of the electronic results management system (eRMS) by the Commission was among the violations alleged by the petitioners.[28] The allegations included the deletion of data in the eRMS and rigging of tallies at the National Tally Centre by an unknown user. The court found no evidence to show that data was deleted in the eRMS since the Commission was able to retrieve records of all 5,002 polling stations, nor did it find proof of the alleged rigging at the National Tally Centre. However, the court held that the security of the eRMS was compromised due to the use of default account usernames with known passwords that were shared by several personnel of the Commission. The court stated (paragraph 1329), "[c]onsequently, we find that the default user accounts presented a risk to the integrity of the eRMS. This detracted from the quality and reliability of the eRMS and qualified as a cause for questioning the final national election result which was electronically collated and tallied by the system." Overall, the court found that certain actions and irregularities raised suspicions about the process, even if actual manipulation or fraud was not proved. This issue of

[26] Swamy v. Election Commission (2013, India), para 29.
[27] Shein, E. and Brown, A, Risk Limiting Audits: A Guide for Global Use, IFES, March 2021, https://www.ifes.org/sites/default/files/migrate/ifes_risk-limiting_audits_a_guide_for_global_use_march_2021.pdf, p.9.
[28] Other alleged irregularities included the use of altered tally sheets (tippex was used in some cases), omissions in logbooks and missing signatures on tally sheets.

annulling an election result without evidence of outcome-determinative fraud or irregularities has been examined in IFES' separate paper, *When are Elections Good Enough?*[29]

In *Raila Amolo Odinga & Another v. Independent Electoral and Boundaries Commission & 2 Others (2017)*, the Supreme Court of **Kenya** considered whether there were illegalities and irregularities in the conduct of the 2017 presidential election and, if so, the potential impact on the integrity of the election process and result. More specifically, the court considered whether the transmission of results forms, and the verification and declaration of results conducted by the Independent Electoral and Boundaries Commission (IEBC), was conducted in accordance with the Constitution and applicable laws. The court ruled that illegalities and irregularities in the process rendered the result of the election opaque and unverifiable, and therefore indeterminate. Irregularities noted by the court included the delay by the IEBC in announcing its inability to transmit results electronically in some areas (and in communicating alternative systems for the transmission of results) due to the weak telecommunications network; and delayed or missing polling station results forms.[30] As such, the court declared the elections to be invalid, null, and void, and the IEBC was ordered to conduct fresh elections within 60 days, in accordance with Article 140 of the Constitution. The court noted that no election is perfect, but "where parliament produces a technology roadmap with the sole aim of ensuring verifiable transmission" and the IEBC does not adhere to this, "how can the court close its eyes?"

Unlike the Malawi Court, the apex court in Kenya did not give the IEBC specific guidelines for improving the results transmission process in 2017 but said the judgment "ought to lead the IEBC to go back to the drawing board." The court gave a clear signal to the IEBC to transparently implement new electoral logistics and procedures (testing, piloting and training on the results transmission system), resolve fundamental disagreements among key stakeholders, and demonstrably prevent anomalies identified by the court — all within a compressed timeline. While the IEBC made changes to its procedures, it was not technically or legally possible for the IEBC to fully comply with the scope of changes suggested by the court order within sixty days of the annulment — including, for example, because of restrictive deadlines around technology procurement and public consultation in the law. This reinforces the point that an annulment is a significant remedy, and a re-run election may not be able to resolve certain issues — particularly as it pertains to replacing or modifying election technology. As IFES has written about previously, a decision to annul an election is one that should not be taken lightly: "Repeat elections impose unexpected costs on state budgets and candidates; the normal operation of legislatures and governments may be disrupted while a revote is organized; candidates may refuse to participate in the fresh elections, leading to a political crisis; and repeat elections may themselves be subject to irregularities."[31] Hence, many countries follow an "outcome-determinative" approach to annulment.[32] That is, where the outcome has not been impacted, other remedial action, such as prosecution for fraud, may still be appropriate, but the results are allowed to stand. In 2022, the Supreme Court in Kenya dismissed the nine petitions filed against the presidential but in its full judgement released on Oct. 26, it issued two recommendations regarding the access to the servers.

[29] IFES, When are Elections Good Enough?, IFES 2018, https://www.ifes.org/document/when-are-elections-good-enough-validating-or-annulling-election-results
[30] Other irregularities included the lack of security features of some results forms, and the lack of a stamp, seal, or signature by a polling agent on various forms.
[31] IFES, When are Elections Good Enough?, IFES 2018, https://www.ifes.org/document/when-are-elections-good-enough-validating-or-annulling-election-results
[32] This includes all Council of Europe countries, as well as the U.S., Canada, and Australia.

## Issue 3: Discharging the Burden of Proof

The procedures governing the burden of proof and the standard of evidence that will be applied in election cases must be well-designed and established in advance of the start of an electoral process. In most jurisdictions, official election results typically enjoy a presumption of validity and challengers bear the burden of showing why they should be set aside.[62] But the extent of the challenger's burden of proof varies depending on the jurisdiction.

Considering that electronic evidence in elections can be difficult to access for a petitioner or for the courts, the Supreme Court in **Kenya** in *Raila Amolo Odinga & Another v. Independent Electoral and Boundaries Commission & 2 Others (2017)* shifted the burden of proof from the petitioner to the respondent (the IEBC) to prove that the election was conducted in accordance with the laws and rules in place, once it was satisfied that the petitioner had discharged the burden of proof to a sufficient degree. The court then ruled that the IEBC had not discharged this burden in its responses to the Court, including by refusing to provide access for the petitioners to its servers and transaction logs. Because the IEBC did not provide the full access requested in the order, and the Court considered that no reasonable explanations were provided by the IEBC to justify irregularities, the Court stated it "had no choice" but to accept the petitioners' claim that either the servers were infiltrated and the data compromised, or that the IEBC itself had intentionally or unintentionally compromised the data.[33] As presented in the IFES paper, *When are Elections Good Enough?*, courts have adopted different approaches to the burden of proof based on different balances between the presumption of validity and the need to get at the truth.[34]

> "A stronger presumption of validity may be most suitable in cases where the rules of evidentiary discovery give challengers the tools they need to gather the evidence required to make their cases. Where systems of evidentiary discovery are weak, or where courts are unable to compel defendants or third parties to comply with demands for information, a more flexible standard may be appropriate."[35]

In her dissenting opinion in *Raila Odinga & Another v. IEBC & 2 Others (2017)*, Honourable Justice Njoki Ndunga writes, "[172] Having determined that failure of technology could not supplant the will of the people, recorded in verifiable ballots and other election material and the results declared in (a) available (b) ascertainable (c) unchallenged (d) proper statutory instruments of declaration, it is my opinion that the Petitioners' case to exclude results from 11,000 polling stations which were out of 3G and 4G network would be an affront to the Constitution and the right to franchise." Arguably, the case hinged upon the Court's interpretation of the concept of the shifting burden of proof, whereby once the petitioner had established some illegalities and irregularities, it fell to the IEBC to prove that these were not of sufficient scale or scope as to overturn the result. This shift of the burden of proof by the court

[33] See section 299 of the ruling: "The IEBC in particular failed to allow access to two critical areas of their servers: its logs which would have proved or disproved the petitioners' claim of hacking into the system and altering the presidential election results and its servers with Forms 34A and 34B electronically transmitted from polling stations and CTCs."
[34] Vickery, Ennis, Ellena, When are Elections Good Enough? (2018), p.18.
[35] Ibid.

enabled it to redress potential imbalances in access to digital evidence relating to technology between the petitioner and the EMB. However, the dissenting opinion by Justice Njoki Ndunga in 2017 raises the question of whether the court has the capacity to examine the important amount of evidence, to record, store, archive the data and be able to protect the integrity of data processed during scrutiny process as discussed under Issue 7 (data protection and privacy) below. This is particularly relevant in Kenya, where the Supreme Court has only 14 days to hear a case and render a decision.[36] It is also important in light of the judgment of the European Court of Human Rights (ECtHR) in *Namat Alieyev v. Azerbaijan*, which charged domestic courts with the responsibility of "taking reasonable measures to investigate alleged irregularities when the evidence provided by an applicant is insufficient to decide the case but nonetheless strong enough to warrant additional inquiry." Unlike the 2017 elections, the Supreme Court did not shift the burden in its recent 2022 Odinga's presidential petition ruling. The IEBC published the audit report of voter registration, made all the result forms available on a public portal, and held public simulations of the technology prior to Election Day. Following allegations, including hacking of the servers, foreign interference, and manipulation of the results transmission systems (RTS), the Court ordered an audit of the technology with a supervised access to the server of the IEBC and found that the "Scrutiny Report prepared by the Registrar of this court did not reveal any security breaches of the IEBC's RTS" and that no credible evidence meeting the requisite standard of proof of access to the system "by unauthorized persons was adduced by the petitioners."[37] The enhanced transparency of IEBC and wide access to evidence in 2022 as well as the clear explanation from IEBC contributed to keeping the burden of proof on the petitioner. The Court found that "the petitioners have failed to discharge the legal burden of proof so as to shift it to IEBC." [38]

In *Chilima vs. Mutharika and Election Commission* in **Malawi**, the court also confirmed the more accepted international practice for election petitions that the burden is on the petitioners to prove the case, but found that the petitioners established a prima facie case and thus shifted the burden to the respondent, Mutharika and the MEC, to disprove the allegations. Unlike the Kenya case discussed above, the evidence was satisfactorily made accessible to the court and to the petitioners, allowing the courts to access and compare results forms. Given that the timeframe for appeals related to election petitions in Malawi is not set out in the law and took eight months of deliberation in 2019 (versus 14 days, which is set out in the Constitution in Kenya), this clearly illustrates the impact of deadlines on the ability to gather and assess evidence. The importance of a respondent effectively discharging a burden of proof was also emphasized by the court, which criticized the failure of the EMB to call commissioners as material witnesses. This judgment emphasizes that the use of technology in election results transmission and verification should not dilute commissioners' responsibilities as to the verification of the results.

## Issue 4: Admitting and Assessing Digital Evidence and Expert Evidence

Compared to physical evidence, alterations to electronic or digital evidence may not be immediately visible; detection of alterations or tampering may require additional expertise, and technology failures or security breaches may damage the data. As such, digital evidence may require different treatment by a court.

[36] The Supreme Court in the Odinga case in both the 2017 and 2022 petitions recommended to extend this constitutional deadline in its full judgement.
[37] Odinga & 16 others v Ruto & 10 others; Law Society of Kenya & 4 others (Amicus Curiae) (Presidential Election Petition E005, E001, E002, E003, E004, E007 & E008 of 2022 (Consolidated)) [2022] KESC 54 (KLR) (Election Petitions) (5 September 2022) (Judgment).
[38] Ibidem.

"Electronic evidence presents unique characteristics which necessitate careful treatment."[39]

In both the case studies below, highly qualified ICT professionals found significant vulnerabilities and security breaches in the election technologies in use. In the United States' state of Georgia, the plaintiffs were able to gather a significant body of evidence over a prolonged period of time and were largely successful in their court challenge concerning an outdated electronic voting system. In the Honduran case, plaintiffs were unable to gather the necessary technical evidence in time to mount an effective challenge against the electronic results system, and the contested results remained in place. However, an ICT expert from the Organization of American States (OAS) was able to carry out a non-invasive audit and found that the Honduran results system had significant flaws. These two case studies demonstrate how much litigation deadlines and access to expertise can have on cases related to complex election technology. As such, these cases raise concerns over "equality of arms"[40] between complainants and respondents in terms of who may have access to the necessary means to recruit and deploy such experts. Courts must consider this type of extra cost associated with election technology litigation as a country's legislature or EMB introduces sophisticated election technology solutions.

In the **United States** Federal District Court case *Curling v. Raffensperger (2019)* in the state of Georgia, plaintiffs argued that Georgia's outdated electronic voting system diminished voters' First and Fourteenth Constitutional Amendment rights to cast votes that will be properly counted.[41] The electronic voting system implemented by the Secretary of State of Georgia was designed to have an audit trail, but the trail was never implemented over the 20 years the system was in use. Further, the court found that the direct recording electronic (DRE) voting software used was outdated, unreliable, and vulnerable to cyberattack. In 2018, a report by the National Academies of Sciences, Engineering, and Medicine and associated National Research Council had determined that the electronic voting system used by Georgia had serious security flaws, and since flaws were noted by earlier experts in 2006, there is no evidence that Georgia took steps to protect the electronic voting system after security threats were identified.[42] Additionally, the electronic voting systems were connected to a Global Election Management System that was linked to a public-facing internet-connected computer. Files were later transferred to secure USB drives and then transferred to personal computers belonging to contractors who did work in their own homes. The court found that the electronic voting system was not secure and was particularly susceptible to manipulation without detection.

In 2019, the plaintiffs requested a preliminary injunction to prohibit the use of the software for upcoming local elections that year and to order the use of paper ballots instead. The court considered the preliminary injunction in two separate prongs. First, the court determined that for future elections *after* the immediate off-year election, the balance between the state's hardships (resource and operational constraints) and the public interest (in an orderly and fair election

[39] Kenya, *William Odhiambo Oduol v Independent Electoral & Boundaries Commission and 2 others*, Election Petition (Kisumu) No. 2 of 2012.
[40] The principle of equality of arms requires that there be a fair balance between the opportunities afforded the parties involved in litigation.
[41] A list of Constitutional amendments can be accessed at: http://hrlibrary.umn.edu/education/all_amendments_usconst.htm
[42] U.S. Federal District Court, *Curling v. Raffensperger*: The Sept. 6, 2018 consensus report of the National Academies of Sciences, Engineering, and Medicine and associated National Research Council ("NAS"), titled "Securing the Vote: Protecting American Democracy," addressing the need to improve voting machine security, and recommending that voting machines that do not produce paper audit trails for each elector's vote "should be removed from service as soon as possible" and that "[e]very effort should be made to use human-readable paper ballots in the 2018 federal election."

process) required granting the requested prohibition. However, for the second prong, the court determined that for the immediately upcoming election, the requested injunctive relief could not be granted because the hardships outweighed the public interest – as the state would not be able to put a new voting mechanism or upgrades in place in time for the election. Ultimately, the Court allowed the defendant to use the machines one last time in 2019 but prohibited the state from using them after that. Further, the court directed the state to address errors in voting assignments and the voter register and mandated that each precinct has at least one physical copy of the voter registration list. The state was required to provide information to voters regarding provisional ballots, and work with a cybersecurity firm to improve and modify the voting system. The court approved the move to a new electronic voting system (ballot marking devices where the voter uses a touch screen then prints a paper ballot, which is read by an optical scanner) and directed the state to develop contingency plans that include audit provisions.

This case is notable for several reasons. First, the Court relied extensively on expert testimonies and a substantial body of academic and expert practitioner material regarding the technology in question, with the court finding "a mounting tide of evidence of the inadequacy and security risks" of the outdated paperless DRE system. Second, this case had implications for the contested 2020 presidential election. Had the Court not required the Secretary of State to switch to a new auditable system in 2020, it would have impacted the ability of the State of Georgia to administer credible primaries and general elections in 2020. Given the contested nature of the 2020 election and the very close margins in Georgia, the absence of strong audit rules and a paper trail (which were in place as a result of the court's decision) could have precipitated a major political crisis.

During the 2017 general elections held in **Honduras**, the Organization of American States Election Observation Mission (OAS EOM) reported in detail on failings in the electronic results processing system, which crashed during results tallying.[43] Although this situation was not addressed in detail by the courts, it presents an example of the type of technical and systems-based dispute that could result in EDR proceedings. The OAS' conclusion on the election technology was that the results processing system had significant flaws and serious breaches of IT security, and was not sufficiently strong to prevent fraud, although they could not identify a specific fraudulent incident. These concerns and other factors led to their overall conclusion that they had "observed a low-quality election process. The abundance of irregularities and deficiencies is such as to preclude full certainty regarding the outcome."[44] There were widespread allegations of fraud and mistrust in the results, and dozens of people were killed during protests over the results.

The OAS report explains the technical difficulties the EOM encountered when trying to understand what had gone wrong in the results process, and why an ICT expert was needed. Forensic evidence had not been preserved, and some evidence had been altered when software was installed onto new servers. The OAS was only able to carry out a limited, non-invasive audit, meaning they could not run tools or scripts or carry out any testing process. Their report noted, however, that 464 results forms were entered into the system by unknown persons using a non-standard method, and logs were out of sync with no explanation.[45] The OAS also reported that the company responsible for providing the scanning and transcription service had remote access to the servers, outside the EMB's control or oversight, which posed a very high security risk. Finally, the report noted that the results processing system had

[43] OAS EOM to General Elections in Honduras 2017, Report to the Permanent Council, p. 3-4 and Electoral Technology section, p.24-29 of English version.
[44] OAS EOM to General Elections in Honduras 2017, Report to the Permanent Council, p. 4.
[45] This finding suggests that some limited access was provided to the system for the limited audit.

inadequate storage space, and lacked proper planning, testing, and auditing. The OAS' limited audit was carried out in the days following the results process and required time, ICT expertise, and access to the computer system. However, it is important to note that a limited audit of the technology used in the result process is not the same as a court weighing arguments and evidence and considering the impact of such evidence on the outcome. Although opposition parties brought legal challenges to the results, they were not able to produce evidence (either on paper or digitally) that substantiated their claims regarding the results system, and so their challenges were dismissed by the Supreme Electoral Tribunal.[46]

This decision suggests that a litigating party would need extensive resources (including a well-organized network of party agents across the country) and a high level of ICT expertise in order to be able to bring a challenge successfully (or to provide sufficient proof to shift the burden to the respondent). It is also clear from the Georgia case that a court would need to rely on expert evidence to examine allegations of failings in an electronic results processing system, as the subject matter is highly specialized. One possible measure that a court could take is to appoint an independent ICT expert to act in an amicus[47] capacity to assist the court. This could help mitigate the lack of equitable access to ICT experts by less well-resourced litigants. However, key expertise may lie exclusively with the system vendor (if outsourced, as in this case) or the EMB's own ICT department (if developed in-house), either or both of whom may be parties to the legal proceedings. Even the OAS ICT expert in the Honduran case lacked sufficient time and access in order to carry out a full forensic analysis. If the elections technology under scrutiny is a "black box" to the public and relevant stakeholders, it has been poorly designed from the outset.

## Issue 5: Politicization of 'Expert' Evidence

In hotly contested elections that are litigated in court, some expert evidence presented by parties may lack genuine expertise and/or may be partisan. A striking example of this appears in a **United States** case in the State of Michigan Court of Appeal regarding a challenge to the 2020 election results in Antrim County*, Bailey v. Antrim County and Benson (2021)*. The plaintiff challenged the use of electronic voting machines, alleging that they were programmed to be susceptible to fraud. The plaintiff alleged that there were questions "whether the audit logs were altered or edited by any person operating the system, (9) whether Dominion pre-loaded any algorithms and configurations on the machines that alter the results, and if so, what algorithms and configurations were pre-loaded, and (10) whether the 'purge option' that is built into Dominion utilized to cancel, switch, or manipulate votes…"[48] The plaintiff applied to the court to carry out a forensic analysis, which the court authorized. The plaintiff then submitted a report by a self-described cybersecurity expert (entitled the ASOG report), the central conclusion of which was that the electronic voting machines provided by Dominion Voting Systems were "intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results."[49] The expert did not claim to have any expertise in election technology. The ASOG report was widely cited by President Trump and his supporters as evidence of fraud in the 2020 elections, and the Congressional select committee investigating the events of Jan. 6, 2021 at the Capitol

[46] The European Union Election Observation Mission, Honduras 2017, describes the unsuccessful challenges to the results, p. 20-26.
[47] An amicus curiae is an individual or organization who is not a party to a legal case, but who is permitted to assist a court by offering information, expertise, or insight that has a bearing on the issues in the case.
[48] State of Michigan, Court of Appeal, Antrim County, *Bailey v. Antrim County and Benson* (2021), at 29.
[49] Antrim Michigan Forensics Report by Allied Security Operations Group, December 2020.

has heard witness testimony that the ASOG report was part of a national communications plan to discredit the 2020 elections.[50]

The defendants, Antrim County and the Michigan Secretary of State, responded with an expert technical investigation report prepared by a University of Michigan professor of electrical engineering and computer science, Alex Halderman, who is also one of top nations' experts on election security. He refuted the central allegations in the ASOG report and explored what had gone wrong (the "Halderman Report").[51] This report explained that there were significant errors in the unofficial results declared in Antrim County in the presidential and other contests, mis-stating vote totals by several thousand votes. However, the errors were corrected, and the presidential results were confirmed by a county-wide hand count of paper ballots and a state-wide risk limiting audit. The errors were a series of human errors caused by last-minute changes to the design of the electronic ballots, compounded by inadequate procedures, but were not due to a security breach, nor fraudulent actions. The Halderman Report describes how the ASOG report "contains an extraordinary number of false, inaccurate or unsubstantiated statements and conclusions," and explains why many of ASOG's assumptions and conclusions were erroneous. The plaintiff's case was dismissed by the Michigan Court of Appeals, who found that the plaintiff had failed to make any "clear and positive" factual allegations, and that the irregularities the plaintiff alleged could not have affected the outcome of the presidential election.[52] The ASOG report is the subject of a multi-million dollar defamation claim by Dominion Voting Systems, which has put out statements refuting the disinformation campaign against the company.[53]

The U.S. Federal Rules of Evidence define expert witness testimony as being from a person who "must have "scientific, technical, or other specialized knowledge" that "will help the trier of fact." (R. Evid. 702). In other jurisdictions, such as France, the Code of Administrative Procedure provides the possibility for the judge to nominate experts, and requires that the expert be impartial and provides for the drafting of a report.[54] Rules of procedure may also provide for a renewed trial in case a ruling has been based on false statements by experts.[55] Although expert evidence can be tested in court, through cross-examination or deposition of the expert and questioning of their expertise, such scrutiny only goes so far in discrediting partisan and inaccurate reports. In that respect, the Halderman report makes an important recommendation: that election technology incidents be rigorously investigated as a matter of course to enhance accurate understanding and public trust in elections.[56] But such investigations require time, and sometimes, the timeline for adjudication of election disputes by an electoral court or tribunal are too short to nominate experts. The recruitment of ICT experts, review of evidence available, conduct of an audit and preparation of reports can take months to finalize. In Kenya during the 2022 petition, the Supreme Court admitted three ICT experts as *amicus curia* to provide some expertise on election technology, but they were not allowed to make oral submission, notably due to the short adjudication deadline.

[50] Antrim County, Mich., Tied to Election Fraud Claim Strategy (govtech.com), January 6, 2022.
[51] The Antrim County 2020 Election Incident: An Independent Forensic Investigation, by J. Alex Halderman, an expanded version of the expert witness report of March 26, 2021.
[52] Bailey v Antrim County and Benson, Michigan Court of Appeal, April 21, 2022.
[53] Facts About Dominion And Antrim County, Michigan (mailchi.mp), Dominion Voting Systems, December 14, 2020.
[54] French Code of Administrative Procedure, 621-10; Law on General Administrative Procedure, Art.64 "Experts."
[55] See for example the General Administrative Procedure of North Macedonia, s. 114. "Ruling administrative act on false identification document or false statement by a witness or expert, or is consequence of a deed punishable according to the Criminal Code."
[56] On this issue, see also IFES' paper on Risk Limiting Audits: A Guide (2021) - https://www.ifes.org/publications/risk-limiting-audits-guide-global-use.

During the conference of the Africa Electoral Jurisprudence Network held in July 2022, judges also inquired about expert testimonies, and how judges deal with different — and potentially contradictory — technology experts. Initial research showed that there is an emerging approach in some common-law jurisdictions (Australia, England, U.S.) of the use of concurrent expert evidence, known as “hot-tubbing” the experts. The judge leads the process, whereby both experts are sworn in concurrently and questioned together. The judge may ask the experts to provide a joint teach-in on the issues in dispute at a general level; prepare a joint statement of the issues they agree on and the issues in dispute; answer the judge’s questions on the issues in dispute, including commenting on each other’s views and asking each other questions and allow limited cross-examination by counsel. While more research is needed this method is thought to increase the quality of the expert evidence and improve the court’s understanding of it. It acts as a constraint on experts behaving as partisan advocates and emphasizes their duty to assist the court. Peer scrutiny helps to avoid misleading answers and helps distil complex competing views. It may save court time and costs, although it requires greater preparation time by the judge. This approach also will require that the experts to be of a similar level of expertise and the judge needs to avoid a more assertive expert dominating the proceedings. Whether the court admits *amicus curia* with ICT expertise or rely on independent expert testimony and cross examine them, the judge should remain aware of the risk of potential political bias.

The marked increase in the volume of digital information in the election process presents significant challenges for petitioners, who may not be aware of the types of digital evidence that could support their claims and may not be given access to the data by the EMB or other institutional stakeholders due to security and integrity concerns. These challenges may justify a shift in the burden of proof as discussed in a previous section. It also presents a challenge for the judges, registrars, or clerks who will be responsible for receiving, recording, storing, analyzing, or archiving this information.

## Issue 6: Integrity of the Data and the Chain of Custody

As pointed out in IFES’ *Election Investigations Guidebook*, "investigative bodies and other relevant institutions — such as law enforcement agencies, election management bodies, prosecution services, and courts or tribunals — must establish communication mechanisms in advance of the election process to facilitate…effective cooperation during investigations."[57] This statement is particularly relevant for the investigation of election technology, where in the absence of cooperation between the EMB and the court at the time of collecting, storing, and retrieving the evidence, there is a risk of damaging the integrity of the data being investigated.

The marked increase in the volume of digital information in the election process presents significant challenges for petitioners, who may not be aware of the types of digital evidence that could support their claims and may not be given access to the data by the EMB or other institutional stakeholders due to security and integrity concerns. Petitioners and respondents, including EMBs and their lawyers, need to be aware of standards for verification and accuracy of evidence to ensure proper collection of digital evidence. It is crucial to ensure that the evidence is reliable and admissible.[58] In **Kenya**, in *William Odhiambo Oduol v. Independent Electoral & Boundaries Commission &*

[57] IFES. Election Investigation Guidebook (2020), p.96. https://www.ifes.org/publications/election-investigations-guidebook
[58] Kenya, Republic v. Mark Lloyd Steveson, High Court (Kiambu) Criminal Revision No. 1 of 2016) & Millitonic Mwendwa Kimanzi Kitute v. Independent Electoral and Boundaries Commission & 2 others, Election Petition (Kitui) No. 1 of 2017- [2017] eKLR. Kenyan courts referred to the authenticity and reliability of such evidence.

*2 Others,* Election Petition (Kisumu) No. 2 of 2012, the High Court of Kisumu called for a cautious approach to electronic evidence. The High Courts' reasoning centered on four parts, 1) Their belief that electronic documents are easily modified when collected as evidence, 2) an assumption that detecting alteration or tampering of digital evidence is much more difficult than detecting such things for paper processes, 3) The fallibility of information technology due to their general understanding of plausible security threats, and 4) The specialized knowledge required to capture, preserve, and present digital evidence. While the technical understandings embedded within the high court's articulated reasoning can be considered somewhat out of date, their caution is warranted. Good practice for digital forensics is not universally established globally across all judicial and political contexts. Combined with the short windows during which election disputes are litigated, the evidentiary chain of custody, integrity, and applicability can be challenged and can be a complicating factor in its own right.

The chain of custody of the evidence is critical in proceedings for both digital and physical evidence. IFES' *Election Investigations Guidebook* states that "election investigators must take care to closely adhere to the SOPs that pertain to the maintenance of a proper chain of evidence during the investigative process. A failure to do so could undermine the integrity of the evidence collected and, ultimately, the quality of the investigation itself."[59] For traditional evidence, it is a chronological paper trail of when, how, and by whom evidence was handled. But for digital evidence, it may be a challenge to maintain clear records of how data was generated, as well as the chain of custody in the transmission and storage of data to ensure there has not been any unauthorized access. It can also be difficult for a court or other law enforcement body to examine the evidence without compromising the data and without delaying the election process. In **Uganda**, the Uganda Electronic Transaction Act is applicable to election petitions and regulates the admissibility of digital evidence. In election petition, No. 1 of 2001 in *Dr. Kizza Besigye v. Yoweri Kaguta Museveni and the Electoral Commission*, the High Court rejected audio recordings and found they were inadmissible. The plaintiff did not submit sworn affidavits in support of the recordings and the court questioned the authenticity and the manner in which the voices were recorded on the CDs.

Courts need to establish clear rules to guide parties on how to prove or certify that a document has not been tampered with. In **Kenya**, the law requires a certificate of an electronic record and the courts have clarified that an affidavit that sets out all "the pre-requisites will suffice if it is deposed by a person in a responsible position in relation to the operation of the electronic device or management of the relevant activities."[60] **India** has a similar certification procedure for digital evidence. In India, in *Anvar P.K. v. P.K Basheer & Others (2014) 10 SCC 473; and T Karia, A Anand & Bahaar Dhawan*, the Supreme Court re-defined the admissibility of electronic evidence in an election petition. The petitioner had sought to rely on electronic evidence and the Supreme Court in its decision "emphasized the need to protect the credibility and evidentiary value of electronic evidence since it was more susceptible to tampering and alteration."[61]

In **Ecuador,** a recent case brought before the Prosecutor's Office (*Fiscalía General*) illustrates the real difficulty of carrying out a computer audit during an ongoing election process without compromising the data or delaying the process. This case raised the question how an electronic database could be examined by law enforcement during

[59] IFES Investigations Guidebook (2020), p.118-119.
[60] County Assembly of Kisumu & 2 Others v Kisumu County Assembly Service Board & 6 Others, Civil Appeal (Kisumu) No. 17 of 2015.
[61] India, Anvar P.K. v P.K Basheer & Others, (2014) 10 SCC 473; and T Karia, A Anand & Bahaar Dhawan

the election process without delaying the process and compromising the integrity of the data. During the 2021 general elections, one of the competing parties alleged fraud relating to anomalies observed in the digitized tally sheets and requested that the Comptroller investigate the issues and recount of more than 27,000 ballot boxes. In response, the prosecutor launched a preliminary investigation and obtained a court authorization to search and retain a copy of the records, but the hardware was not taken physically from the National Electoral Council's (CNE) computer server. The Comptroller made a request to the CNE to carry out an audit of the computer system, but the CNE objected to this action until after the elections had concluded — believing that these actions would amount to unlawful interference in the ongoing election process and would delay the pending second round and jeopardize the electoral calendar.[62,63] The CNE's concerns that these requests amounted to undue interference in the election process were echoed by the EU Election Expert Mission and the OAS EOM.[64] The Ecuadoran Congress subsequently brought impeachment proceedings against the Comptroller.[65] If the prosecutor had sought to enforce the court order, the CNE could risk being in contempt of court. If the CNE had complied with the prosecutor's request, they could have risked delay in the election process and may have compromised the data's integrity.

If limited audits or forensic audits are ordered by the courts, they should be conducted according to clear rules to ensure chain of evidence is respected and evidence is not tampered with during the audit process. To avoid such tensions and a potential political crisis, it is crucial for the EMB and courts to cooperate prior to elections to familiarize judges with the operational and technical challenges of investigating election irregularities during an ongoing election process.[66]

## Issue 7: Data Protection and Privacy

The need for security of election technology is not only vital to the integrity of the election process. It also affects the privacy and data protection rights of all individuals whose data is held by the EMB, including voters, candidates, observers, party representatives and polling officials. International standards emphasize the need for election technology to be secure.[67] While most election data belong to the public domain, there can be a tension between the need for public and stakeholder scrutiny of election data and ensuring the privacy of voters. In the **Philippines**, punitive measures were imposed on the Commission on Elections (COMELEC) for negligence in data protection in 2016. This followed hackers taking over COMELEC's website and releasing extensive voter information, including fingerprints. The National Privacy Commission recommended criminal charges against the COMELEC Chairperson Andrés Bautista for negligence.[68] While this case did not result in election court proceedings, it established a

[62] EU Expert Mission Report on the 2021 Ecuador Elections, p. 30.
[63] In the end, the requested actions did not take place, as Pachakutik agreed with the CNE to carry out a limited number of recounts, which did not change the overall first round result. When the alleged discrepancies were investigated, only a few were well-founded, and were due to problems in filling in the forms, rather than problems in the electronic system.
[64] The OAS Election Observation Mission Report on the General Elections in Ecuador 2021, pp. 13-15 (in English) and pp. 141-142 (in Spanish).
[65] Testimonies in the impeachment of the exComptroller have begun, El Comercio, July 18, 2021 (in Spanish).
[66] For further discussion on institutional coordination, and the development of investigations plans, see IFES' Election Investigations Guidebook (2020), https://www.ifes.org/publications/election-investigations-guidebook.
[67] The Venice Commission Code of Good Practice on Electoral Matters 2002 provides at paragraph 43, "Electronic voting methods must be secure and reliable. They are secure if the system can withstand deliberate attack; they are reliable if they can function on their own, irrespective of any shortcomings in the hardware or software." The Council of Europe's Guidelines on use of ICT in electoral processes, February 2022, sets out the responsibility for ensuring the integrity and authenticity of the information, including by continuous risk management of the ICT solutions. The Council of Europe's Recommendation on Standards for E-Voting CM/Rec (2017)5, section VIII provides that the EMB shall be responsible for compliance with all security requirements even in the case of failures and attacks.
[68] Privacy Commission recommends criminal prosecution of Bautista over "Comeleak" » National Privacy Commission, January 5, 2017.

precedent of holding EMBs and their leadership accountable for information security failure and data breaches. The National Privacy Commission ordered COMELEC to implement new security measures, including hiring a Data Protection Officer and instituting a Privacy Management Program and a Breach Management Program. A month later a computer containing voters' biometric records was stolen from a local election office. Being the second large scale data breach in less than a year,[69] COMELEC Chairperson Bautista was impeached in October 2017 and resigned that month. This is an example of both the institutional and personal liability that government bodies, and election officials may face regarding cybersecurity. In the 2022 election petitions in Kenya, the IEBC senior counsels called on the Data Protection Act in its response to justify that they could not publish the full audit report of the voter registry without putting data of Kenyan citizen at risks.[70] A similar expectation on data protection applies to the election court when evidence is handed over to the court in charge of conducting a scrutiny of election technology. There is a growing body of legislation on data protection, which provide obligations for government bodies to protect citizen data, for instance by protecting identity of voters or storing data on servers physically located inside the country.[71] Examples of such laws or regulations include Nigeria,[72] Uganda,[73] Zambia,[74] and the issue has received regional attention at SADC, ECOWAS, and EAC levels.[75] EMBs like in Kenya or Malawi, have already followed good practice on data protection, for instance by sharing a redacted version of the voter list with political parties or by using appropriate encryption tools, properly configured and managed. But courts should also abide by these standards to ensure protection of data when receiving, storing and making data accessible to petitioners or observers.

## Issue 8: The Availability of Effective Remedies

The process of measuring different types of remedies and their effectiveness for different categories of disputes is complex. A "proper analysis of effective remedies requires an examination of the core elements of effectiveness to ensure that a remedy: (1) ensures that the letter and spirit of the law is realized in practice (including to restore electoral rights or otherwise undo the harm caused by a violation); (2) is provided in a timely manner; (3) is proportional to the violation or irregularity in question; (4) is enforceable; (5) leads to deterrence or a change in behavior in question; and (6) reinforces the perception of fairness and credibility of the process."[76]

Judicial decisions involving election technology reveal different approaches by courts in their orders, with some courts giving more latitude and time to the EMBs to remedy defects in election technology or clarify interpretation and understanding of its implementation. Other courts are more prescriptive, on occasion making orders that are difficult for the EMB to comply with in a short timeframe. This may be due in part to the fact that election technology is relatively new in many countries, and it takes time for EMBs and courts to develop expertise in the subject matter.

[69] NPC starts probe into COMELEC's 2nd large scale data breach; issues compliance order » National Privacy Commission, February 20, 2017.
[70] For instance, in the 2022 presidential election petition, the IEBC senior counsels explained that the IEBC could not publish the full final audit report as "doing so would compromise the integrity and security of the election technology system and violate the provisions of the Data Protection Act, 2019, which imposes a duty to protect the data of Kenyan registered voters."
[71] Terms for this practice vary – data residency, data localization – see Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L. J. 677 (2015). Available at: https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2
[72] Ibid., p. 700, paragraph K, Nigeria.
[73] While not explicitly prohibiting offshore storage, the Ugandan Data Protection and Privacy Law addresses the topic, see https://pdpo.go.ug/media//2022/03/Data_Protection_and_Privacy_Act_No._9_of_2019.pdf
[74] https://www.parliament.gov.zm/node/8853.
[75] https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session%207_Verengai%20Mabika.pdf.
[76] Vickery, C. and Ellena, K. Measuring Effective Remedies for Fraud and Administrative Malpractice (2017).

Sometimes, legal challenges do not relate to defects in the election technology but instead relate to the lack of or differing interpretation and understanding of the existing corpus of law and procedure relating to the technology. In a recent interview with IFES, Judge Tunheim, Chief Justice of the U.S. Federal District Court, Minnesota noted:

> "People sometimes don't trust electronics…to the extent that we can have a backup for a judge or judges to look carefully to make sure that the machine works properly, then we are better off for all."[77]

It is also important to note that challenges or appeals arise at different phases of the election process, giving some courts more flexibility in the remedies they order. Timelines for adjudication may also play a role in remedies ordered. While in Malawi and Kenya, the courts decided to annul and order a repoll during the post-election results adjudication phase, the German court did not. The courts in Malawi and Kenya were making their decisions soon after the elections in line with tight deadlines (although in Malawi the President and MPs had already taken office), whereas the German court issued its judgment four years after the elections.

In India and in the United States, the courts acknowledged the need for time to implement any changes to the use of technology in elections. When assessing adequate remedies, the judges considered the time required to change, update or introduce a new technology, in comparison to Kenya and Malawi where the judges gave only limited time for the EMBs to reform their processes prior to the repoll. Moreover, in Kenya, the scrutiny ordered and conducted by the court within a limited timeframe and without predetermined rules raised questions as to the method and quality of the exercise, and as to the legal force of the scrutiny report prepared. The importance of there being adequate time to establish any new election technology, including for there to be public discussion of it, is highlighted in the recent OSCE/ODIHR report on the 2021 Albania elections. Although not related to a court challenge, the OSCE/ODIHR mission commented on the recent pilot of electronic voting in Albania as follows: "The very short timeframe for implementation did not allow for substantive public discourse and independent scrutiny of the new technologies…an important component for ensuring public trust."[78] The challenge brought to the first-round results in the 2021 elections in Ecuador also showed the importance of the timing of remedies. The EMB made it clear that it would not be possible for the prosecutor or the Comptroller to conduct their requested audits of the electronic results system mid-way through the election process without compromising the integrity of the data and delaying the election process, and so the EMB refused the requests. As noted above, the apex court in Kenya also called for a constitutional amendment to extend its short 14-day deadline to rule on a presidential election petition, which includes time to conduct a potential scrutiny and recount.

In Malawi, the court in its judgment gave the EMB an extensive list of recommendations and instructions for reform. The issuance of highly prescriptive instructions from the court to an EMB could, however, raise questions as to the independence of constitutionally appointed EMBs and undermine the ability of election officials to determine how to effectively conduct elections. Another concern is the capacity of the EMB to make changes ordered by a court, and

[77] IFES Interview on EDR proceedings (May 12, 2022) with Chief Justice, Judge Tunheim of the U.S. Federal District Court, Minnesota.
[78] The OSCE/ODIHR Final Report on the Albania General Elections 2021 describes how the procurement process for the voting equipment ended a month before, and the configuration of the software a week before Election Day, leaving a short preparatory period for voter education and discussion.

the impact on public trust if these changes cannot be made effectively. The EMB may require time to procure information systems and arrange for access to the source code (in cases where the software is proprietary). This raises the issue of technology service providers, which are usually not a party to proceedings, but their co-operation is required for the EMB to make required changes or provide the required information to the court.[79] This highlights the need for an EMB to retain control of their election process and of the different aspects of the technology so that they can be accountable to the public. The Kenyan Supreme Court also recommended that IEBC ensures restriction of access to its servers to IEBC staff unless where and when it is absolutely necessary to avoid suspicions by stakeholders.[80] The Council of Europe recommended in 2022 that source code should be made public.[81] Again, these cases demonstrate the need for early dialogue and engagement between the EMB and the courts to enhance understanding of these issues.

[79] For example, in Kenyan Presidential Petition 1 of 2017, access to the logs of the results management system required the co-operation of the vendor who was not party to the proceedings and was not resident in Kenya.
[80] 2022 Odinga, at D.b) "To avoid suspicion from stakeholders, unless where and when it is absolutely necessary, access to the servers supporting the transmission and storage of Forms 34A, 34B and 34C should be restricted to IEBC staff during the election period."
[81] Council of Europe, New guidelines on use of technology across all electoral processes, February 2022, paragraph 7(9).

# Conclusion – What Do These Select Cases Tell Us About Election Technology?

Despite a diversity of jurisdictions, powers of the court, and types of election technology used, judges have faced similar challenges when considering the verifiability, accuracy, or transparency of technology and its impact on election processes and outcomes. While technology is constantly evolving, we can draw the following lessons for EMBs, courts, litigants, and other stakeholders:

1. *Transparency in the use of technology and the related EDR process by both EMB and the courts is essential to ensure confidence in the election process as whole.*

Given that public trust can be severely undermined by poor understanding of election technology, it is vital that there is maximum transparency around both election technology and the dispute resolution process. This requires the EMB to communicate as much information as possible to all stakeholders about the technology in use at all stages of an election. This includes transparency in the design of election technology and in its implementation.[82] Public trust in elections also depends on court processes being as open and transparent as possible. In election petitions, courts should ensure openness of their hearings and of any court-ordered audit or scrutiny.[83]

> "Transparency is critical to legitimacy of the election process. In light of suspicion around the use of technology, it is extremely important that we engage early in training with EMBs, otherwise citizens will become suspicious close to the elections."
>
> - *Justice Lillian Tibatemwa, Uganda Supreme Court*[84]

2. *It is essential to build a good understanding among electoral judges, judicial officers, and all stakeholders of election technology in use* and *improve EMB-judicial collaboration well in advance of elections.*

Effective training and awareness-raising of all electoral stakeholders is paramount to ensuring a good understanding of technology used in elections. EMBs should share information with courts and tribunals about the technicalities of systems being used in the elections. When judges have a good understanding of the technology, they are more able to deal effectively with disputes involving that technology. In addition, election technology is usually used in conjunction with paper-based records, and judicial officials must be adequately prepared to physically receive, store, retrieve, and return significant volumes of election material that may be used as evidence, while ensuring such materials (and the chain of custody) are protected. Judges must also ensure that remedies they order are suited to the operational realities faced by EMBs and to the timing of the election process. In terms of effective training of

[82] For example, by ensuring sufficient access to observers, publishing reports of audit exercises, and by conducting a public simulation of an electronic results management system prior to Election Day.
[83] During the Africa Electoral Jurisprudence Network meeting in July 2022, judges present all agreed on the importance of training and called for cooperation with EMBs on this issue.
[84] Africa Electoral Jurisprudence Network Meeting, Lilongwe Malawi, July 19-20, 2022.

judges and collaboration with EMBs, not all jurisdictions have specialized courts or tribunals for elections, so training may be required on a large scale throughout different levels of the judiciary prior to the election. Thus, judiciaries could design a curriculum on election technology and a cascade training program prior to elections to reach a large audience of judges and judicial officers, as was done in Ethiopia and Kenya prior to elections in 2021 and 2022. Education and training are also important for parties or candidates who may wish to collect and present evidence in election petitions, and for election observers to enable them to make sound recommendations.

3. *Judicial procedures need to be adapted to account for digital evidence relating to the use of election technology and to plan for additional resources to order effective investigation measures and remedies if necessary, such as an expert audit process.*

Courts should consider adopting rules of procedure that account for the admissibility of digital evidence, verifiability of digital evidence, effective chain of evidence, rules and forms relating to the conduct scrutiny of technology, and engagement of ICT experts in proceedings or admission of ICT experts as amicus curiae. The rules need to be sufficiently flexible to adapt to new digital tools and should be based on a sound understanding of the electoral process and election technology. Potential complainants also need to be informed about these rules to enhance the quality of their evidence collection.

4. *The courts need to guarantee data integrity by protecting privacy rights of citizens and establishing adequate cybersecurity protections.*

Upon receipt of data during election proceedings, courts should guarantee that relevant data protection protocols are observed to avoid manipulation, theft, or tampering of data. While most election data is in the public domain, there are some notable exceptions (for example, related to biometric information) that can be crucial to protect rights of citizens. The growing body of laws and rules on protection of data should be incorporated to the practice of the court and EMBs should clearly convey these rules in their response or defense before the court.

5. *The EMB needs to ensure there is a physical vote record to enable auditability of election technology used in the voting process and also needs to retain control of election technology used.*

Increasingly, EMBs must ensure that their electoral technologies are “scrutiny-ready” or “digital forensics-ready.” EMBs should also retain control over the technology and information systems during the design and implementation phase to ensure they can quickly provide access to evidence or make changes as required by the court. As stressed by IFES Principal Advisor Peter Erben at the international conference of the Association of World Election Bodies (AWEB) in 2017, EMBs should ensure more open, careful deliberation of technology choices, for example, by insisting that such an important decision be subject to a comprehensive well-resourced feasibility study: “The misperception and suspicion surrounding election technology have at times proven as damaging as actual weaknesses of technology.”[85]

[85] Peter Erben, IFES Senior Global Electoral Advisor “Raising Trust in Electoral Technology; Innovation Aided by Traditional Approaches.” Presentation delivered during the Association of World Election Bodies International Conference: “Counting the Ballots and Accounting for the Votes: The Use of Technology for Enhancing the Transparency of the Electoral Processes” (September 2, 2017).