Live free. Prosper.

South African Institute of Race Relations NPC (IRR)
Submission to the
Electoral Commission of South Africa (IEC)
regarding the possible introduction of
electronic voting in South Africa
30 September 2025

Table of Contents **Page**

1 Introduction

The Electoral Commission of South Africa (IEC) has invited interested persons and stakeholders to submit comments, by 30 September 2025, on the IEC's Policy Discussion Document, Exploring the Implementation of Electronic Voting in South Africa, of February 2025 ("the IEC Discussion Document").

This submission on the IEC Discussion Document is made by the South African Institute of Race Relations NPC ("the IRR"), a non-profit organisation formed in 1929 to oppose racial discrimination and promote racial goodwill. Its current objects are to promote democracy, human rights, development, and reconciliation between the peoples of South Africa.

2 The IEC's recommendation

The IEC Discussion Document asserts that "there would appear to be consensus that South Africa is ready for a form of electronic voting, supported by sufficient technological infrastructure. E-voting is seen as inevitable and necessary due to technological advancements and societal modernisation. It has the potential to enhance accessibility, voter participation and efficiency, particularly for persons with disabilities".[1]

[1] Electoral Commission of South Africa (IEC) and Human Sciences Research Council (HSRC), 'Policy Discussion Document: Exploring the implementation of electronic voting in South Africa', February 2025, ("IEC Discussion Document"), p. 86.

However, the document also acknowledges that, "while e-voting is seen as a promising solution to enhance voter turnout, accessibility and efficiency", it "faces significant barriers, includ[ing] technical glitches, inadequate training of IEC personnel, the digital divide, low public trust, security concerns, and a lack of political will". As a result, says the IEC Discussion Document, there is "a common perspective among stakeholders that the incremental implementation and testing of e-voting will be crucial". This gradual implementation could "start with by-elections and elections of student representative councils, for example", which would allow for the "testing and refinement of the e-voting system". This, the document claims, will "help identify and mitigate, even obviate, potential security risks, ensuring the system's robustness and reliability".[2]

In other words, the IEC has already decided that South Africa should adopt and incrementally implement an electronic voting system. It assumes that starting small will successfully "obviate potential security risks" but fails to provide any evidence as to how this will be achieved in practice. If anything, the Commission's "discussion" document on the issue further confirms its obvious bias in favour of electronic voting.

3 The IEC's obvious bias in favour of electronic voting

The IEC – whose political independence may well have been compromised by the ANC's cadre deployment policy and the evident links between the ANC and some senior figures within the Commission – has long wanted to introduce an electronic voting system.

In May 2019 deputy IEC chair Janet Love, a long-standing member of the ANC/SACP alliance, said that the Commission "had been exploring the use of electronic or digital voting systems in conjunction with their counterparts in other countries with a view to implementing that in SA. 'We are working with our colleagues around the world to investigate how we can use this system of voting in our country,' she said".[3]

In July 2020 IEC chair Glen Mashinini, a former adviser to President Jacob Zuma,[4] said the Commission was "considering an e-election", as this would "drive down costs" and "improve the counting and capturing of results".[5] (Both these claimed benefits are false, as further described below.)

In September 2020 the IEC, with the backing of the ANC government, tried to smuggle an electronic voting system into South Africa via the Electoral Laws Amendment Bill [B22-2020] ("the 2020 Bill") introduced into the National Assembly. This Bill sought to amend the Electoral Act of 1998 and the Local Government: Municipal Electoral Act of 2000 by inserting into both

[2] IEC Discussion Document, pp. 86, 87.
[3] The Citizen, 9 May 2019.
[4] Electoral Commission of South Africa, 'Who are we?, Mr Glen Mashinini': https://www.elections.org.za/pw/About-Us/Who-We-Are/Commissioners/Commissioner-1.
[5] Business Day, 14 July 2020.

statutes a new clause, stating: "Despite anything to the contrary contained in this Act or in any other law, the Commission may prescribe a different voting method".[6]

This vital change to the country's voting system was included in a number of largely technical amendments to several electoral statutes, while the IEC did little to alert the public to the most important change in the 2020 Bill. In addition, the public was given very little time to comment on the contents of the Bill. A call for comments was published in the *Sunday Times* on 11 October 2020, but the deadline for sending written submissions was set at "no later than 30 October 2020 at 16:00". Though this deadline was in time extended slightly to 4 November 2020, the period allowed was still far too short for proper public consultation on so momentous an issue as the introduction of an electronic voting system. That the 2020 Bill gave the IEC the power to introduce a "different voting method" on its own initiative – and without reference to Parliament – was also contrary to the doctrine of the separation of powers and the founding values of the Constitution.[7].

Despite the shortness of the period allowed, the IRR, Dear South Africa and other civil society organisations succeeded in alerting many South Africans to the proposed change, which most strongly opposed. More than 12,000 people signed an objection which was drawn up by Dear South Africa and sent in by it to the Home Affairs portfolio committee in the National Assembly. Several opposition parties also objected to the 2020 Bill and the underhand way in which the IEC was seeking to introduce an electronic voting system. In the face of this concerted resistance, the portfolio committee withdrew the contested clauses.[8]

The IEC has yet to come clean on its 2020 attempt to smuggle an electronic voting system into South Africa without adequate disclosure or public consultation. Instead, the current IEC Discussion Document claims that the purpose of the 2020 Bill was merely to allow the IEC to "experiment with e-voting methods in national and municipal elections". If this was truly the IEC's objective, it could easily have been made clear in the wording of the 2020 Bill – but this was not done. The IEC Discussion Document also falsely states that "the Portfolio Committee on Home Affairs conducted public outreach through the Dear South Africa website to determine public opinion on the Bill and received 12,305 responses", more than 90% of which rejected the Bill's proposed changes.[9] In fact, it was the IRR, Dear South Africa and various other civil society organisations that went to great effort to ascertain public views in the short time allowed for public consultation. And it was at Dear South Africa's initiative that more than 12,000 objections were sent in to the portfolio committee, so compelling the ANC and the Commission to draw back.

The IEC Discussion Document now urging the introduction of electronic voting again fudges many of the key issues that need to be taken into account. The document repeatedly assumes

[6] Clauses 14, 21, Electoral Laws Amendment Bill (the 2020 Bill).
[7] South African Institute of Race Relations NPC ("IRR"), 'Submission to the Portfolio Committee on Home Affairs (National Assembly) regarding the Electoral Laws Amendment Bill of 2020 [B22-2020], Johannesburg, 30 October 2020.
[8] IEC Discussion Document, p. 53.
[9] IEC Discussion Document, p. 53.

that the benefits of electronic voting have been proven, while downplaying the many risks in e-voting. Its single "solution" is always the same: that any problems can and will be overcome by introducing electronic voting on a pilot basis and incrementally expanding it. On the Commission's approach, there will be no real debate on the pros and cons of electronic voting. Instead, the decision to adopt e-voting is effectively being presented as a fait accompli – albeit with the caveat that the shift will need to be made on an incremental basis.

4 The pros and cons of electronic voting in South Africa

Any informed analysis of the pros and cons of electronic voting systems must begin with the basics. These include: the five stages in the voting process; the relative visibility and transparency of manual voting systems; the different types of electronic voting systems available; and why these electronic voting systems are more vulnerable to error and manipulation than manual ones. The reasons why various countries have tried and then abandoned electronic voting must also be explored, along with the experiences of countries which have opted for electronic voting and then maintained it (in India's case, for some 50 years).

The claimed benefits of electronic voting – as set out in the IEC Discussion Document, in particular – must also be examined. No less vital are the costs and constitutionality of electronic voting in South Africa, along with the key question of whether the IEC can be trusted to implement an electronic system with the necessary efficiency, probity and objectivity.

4.1 Stages in the voting process

According to Robert Duigan, who holds an MSc in Crisis and Security Management from Leiden University College and has written a paper entitled *An introduction to vulnerabilities in electronic voting*, there are various stages in the voting process. As he points out, the five stages identified below apply to both manual and electronic voting – and have various points of vulnerability in both systems.[10]

Registration: An accurate register of legitimate voters must be drawn up and maintained. The registration system must be reliable and secure, so that it excludes those not entitled to vote and prevents people from voting twice (for example, by using false identities).

Casting of votes: Voters must be able to cast their votes in secret and without intimidation or undue influence. The choices available to voters should be readily apparent, while votes cast should be clear and not easily altered. Votes cast should also be invisible to election officials and others.

Verification of votes: Voters must be assured that all votes cast will be accurately recordedand will also in time be counted, rather than altered or discarded.

[10] Duigan, R, *An introduction to vulnerabilities in electronic voting*, unpublished paper, October 2020, p4.

Storage and transporting of votes: The storage of votes must be protected from illicit access and tampering, while the transporting (or electronic transfer) of votes must be immune from interception. There must also be accurate means of detecting any violations in these spheres.

Tallying of votes: All votes must be accurately counted, while voting results from all voting stations must be accurately conveyed to the national counting centre and properly collated by it.

These five steps are essentially the same, whether manual or electronic voting systems are used. Manual systems are, however, more transparent and easier to safeguard – if only because the different stages are generally more visible to voters, participating political parties and election observers.

4.2 The transparency and visibility of manual voting systems

Traditional manual voting systems are not immune to irregularities. However, international experience confirms that the safeguards they provide are far stronger than those available under electronic systems. In particular, traditional voting systems are far more transparent because they provide a paper trail and can be observed at every stage.

Writes Mr Duigan in *An introduction to vulnerabilities in electronic voting*: "For the classic secret ballot to function, there need only be a secret booth, a sealed box, a legible ballot, and an impartial system of oversight for counting. For an electronic system, similar concepts apply (albeit in a virtual sense), but at each stage, the 'parts' of the system are far greater in quantity, and the failure of any one part can compromise the validity of a ballot, or even an entire election."[11]

Electronic voting is thus far more vulnerable to manipulation than manual systems. Adds Mr Duigan: "Traditional safeguards for ballot security have the advantage of being legible to the entire public, and violations of protocol are easy enough for anybody to comprehend. Violations are less ambiguous and easier to detect."[12] By contrast, "electronic systems can be harmed in a much more systematic way, and much more covertly, than traditional electoral systems". Interfering with electronic systems requires a high level of technical expertise, which means that relatively few people have the capacity to do it. It also means, however, that equally few people have the technical competence to guard against it or to assess whether manipulation has in fact taken place.

4.3 Different types of electronic voting systems

Both Mr Duigan and the IEC Discussion Document briefly describe the main different types of electronic voting systems. Most are designed to be used at voting stations, where voters must first be identified (often biometrically) and will then be allowed to enter polling booths equipped with one or other type of electronic voting machines. Only the last of the options outlined below ie, on-line voting, does not require voters to go to polling stations to cast their votes.

[11] Duigan, *An introduction to vulnerabilities in electronic voting*, p. 6.
[12] Ibid, pp. 9 – 10.

Stand-alone electronic voting machines (EVMs): As the IEC Discussion Document records, these EVMs were first developed in India in the 1980s, primarily to save the costs of printing ballot papers for more than 650 million voters in each election. These battery-powered machines are not connected to the Internet and are designed to cater for illiterate voters speaking many different languages. They include two devices: a "ballot unit" for the voter to cast his or her vote, and a "control unit" for the presiding officer. The control unit is retained by the presiding officer, who must individually authorise the casting of a single vote by each new voter who enters the polling booth (as further described below). Votes cast are recorded and in time are counted by the EVM.[13]

Automated paper-ballot voting machines (APVs): These machines register a decision made by a voter and then print a physical ballot to be counted later by hand or by a mechanical counter.[14]

Direct-recording electronic voting (DRE) machines: DRE machines allow voters to press a button, use a digital pen, or press a touchscreen to signify their choice of candidate. Votes are recorded on an electronic database on the voting machine and can be accessed later for counting purposes. Some DRE systems are also equipped with "voter-verified paper audit trail" (VVPAT) printers, as set out below.[15]

Voter-Verified Paper Audit Trail (VVPAT) option: A DRE system may be equipped with a VVPAT printer, which prints a "receipt" showing the voter the choice the DRE machine has recorded for him or her. If the voter is satisfied, he or she presses a button and the receipt is dropped into a ballot box, where it is available for counting should this be needed. Requiring voters to confirm the accuracy of printed receipts before they are placed in ballot boxes ensures the accuracy of the paper trail.[16]

Some systems release the printed receipts directly to voters, who then drop them into ballot boxes. Though this option has many advantages, the IEC Discussion Document denigrates it on the basis that voters could then take their receipts home, which would erode the auditability of the results. The IEC document also suggests that this option could promote vote buying, as rival parties might pay for votes shown to have been cast in certain ways.[17] To counter this, some machines allow voters to view the printed receipts, but not to touch them.

(Some VVPAT systems are "voter-verifiable" rather than "voter-verified". The latter systems require the voter to confirm the accuracy of printed receipts before they are deposited in ballot boxes. The latter systems have no such safeguard. Instead, as the IEC Discussion Document records, some provide for the paper trail to be printed only after the votes have been cast.)[18]

The precinct-count optical scan (PCOS) system: This involves paper ballots, which voters mark to reflect their choices and which are then scanned either at the polling station or at a central counting location. The scanner creates an electronic image of each ballot paper, which the

[13] IEC Discussion Document, pp. 36, 39.
[14] Duigan, op cit, p. 3.
[15] Ibid, p. 3; IEC Discussion Document, p. 36.
[16] IEC Discussion Document, p. 58.
[17] Ibid, p. 36; Duigan, op cit, p. 3.
[18] IEC Discussion Document, p. 58.

machine then uses to count the votes cast. These electronic images are stored for audit purposes, while the paper ballots allow for verification and promote transparency.[19]

Public-networked direct-recording electronic voting (PNV): Like DRE machines, PNV ones record votes purely electronically. With a PNV option, however, the votes are tallied centrally and electronically once they have been transferred via a secure public network.[20]

Online voting (OV): As the name suggests, online voting systems – commonly known as "i-voting" systems – allow voters to access the election system from network-enabled devices connected to the Internet. Voting takes place remotely and without the need for voters to travel to voting stations. Following biometric validation of their identifies, voters cast ballots which are transmitted to a central server and stored. Very few countries use this option, as further described in due course.

4.4 The greater vulnerabilities of electronic voting systems

Electronic voting systems are difficult to secure against penetration and/or manipulation by people with authorised access (including election officials and the employees of companies responsible for supplying or maintaining the machines) as well as unauthorised outsiders (representatives of rival political parties or foreign states, for example). Motives for penetration and/or manipulation may vary widely too. Some people may want to influence election outcomes by destroying ballots or falsifying the count. Others may seek to discover people's election choices, so as to intimidate and manipulate them. Some may want to discredit an election by successfully convincing at least a portion of the electorate that tampering has taken place and results cannot be trusted.[21]

Though manual systems can be compromised as well, there are fewer ways to do this and the relevant risks are easier to understand and guard against. Electronic systems, by contrast, have vulnerabilities that are difficult to grasp and harder still to counter. As Duigan writes: "It is easier to perform an attack without being detected – [in part because] understanding the system requires technical education. In addition, because of the length of the design, development and procurement process, electronic voting machines often have a lifetime of 20-30 years. It is almost impossible to prepare decades in advance for potential vulnerabilities, which multiply as technology advances."[22]

4.5 Some of the relevant risks in electronic voting

Relevant risks in electronic voting include the following:

Malware insertion: Here, the attacker accesses the relevant machines – whether e-voting machines, tabulation systems or election management systems – either physically or remotely and inserts a piece of malicious code which alters vote counts, deletes votes cast or makes systems inoperable. Such code is difficult to detect and could affect individual machines or an

[19] Ibid, 36.
[20] Duigan, op cit, p. 3.
[21] Ibid, p. 3
[22] Ibid, p. 4, citing Halderman, 2016: 150

entire network. It could also be introduced at almost any stage in the long lifetime of a machine: in the initial manufacturing process, during subsequent maintenance, or while machines are being transported, stored or deployed.

A small number of manufacturers with mainly proprietary software: A small number of companies dominate the market, both in Western democracies and in countries such as India and Brazil.) These companies generally use proprietary source code, which vendors are reluctant to share with the public. This makes it difficult for independent experts to check the code for hidden "back doors" that could enable the insertion of malware. This situation largely obliges the public to rely on vendor reassurances of adequate security. Yet, where controlled investigative "hacking" by outside experts has been permitted to help uncover vulnerabilities, significant weaknesses have been found. (This is illustrated by annual "Voting Village" events held in the United States since 2017. In 2019, for example, more than a hundred machines were included in the assessment, and hackers were able to find weaknesses in every one of them.)[23]

Problems in initial configuration and subsequent maintenance: Even where there is no malicious intent, the initial configuration of the machines is a complex process and is thus susceptible to human error. If mistakes are inadvertently made, this can affect the subsequent functioning of a machine. It can also create security weaknesses that attackers can exploit.

A machine in use for 20 to 30 years also needs considerable maintenance over this period. This offers opportunities for physical tampering with machines, during which malicious devices (such as rogue circuit boards) can be installed or software can be manipulated. Gaps in the necessary secure chain of custody may also arise and can be used for unauthorised access and tampering.

Possible encryption deficits: As Mr Duigan writes, "The key security element used in electronic voting is cryptography, which is used to secure the confidentiality and authenticity of votes. [This] is achieved by scrambling the data according to a certain pattern, the decoding of which is possible by means of a secure digital key – usually a very large unique number. End-to-end encryption can provide a high degree of security against interception." However, encryption of this kind can be vulnerable at its end points, as the leaking of WhatsApp messages has shown. In Mr Duigan's words: "An end-to-end encrypted platform is only as secure as the end devices."[24]

Blockchain technology – which is a highly complex cryptographic instrument – is now being mooted as an effective mechanism for protecting electronic voting systems from penetration and manipulation. Blockchain has no single point of failure and enables "secure, verified, and anonymous transactions between nodes in a decentralised network", as Mr Duigan writes. These are important strengths – but they do not suffice to make the system invulnerable. Adds Mr Duigan:[25]

---

[23] Blade Technologies, 'Can Electronic Voting be Hacked? Understanding the Security behind the Digital Ballot', 15 October 2024: https://www.bladetechinc.com/news/can-electronic-voting-be-hacked#:~:text=T

[24] Duigan, op cit, p. 8.

[25] Ibid, p. 9.

> A more comprehensive summary of the available proposed systems for blockchain-based voting is covered in Taş & Tanrıöver, 2020: 11-15. [T]his paper…point[s] out in [its] conclusion that the threats and vulnerabilities to blockchain voting are as yet unknown. For a blockchain system to be able to secure an e-voting system, it will need to integrate the registration, authentication, casting and tallying stages[26], and that high degree of scalability poses an unknown risk.
>
> It is also worth pointing out that blockchain technology is not invulnerable to attack. While the ledger is both transparent and anonymous, it is possible to crack. The most famous is a vulnerability…[allowing] a party with enough computing power to solve for 51% of the ledger [to] thereby gain control of the power to rewrite and edit the ledger for malicious purposes[27]. While solutions and workarounds to these vulnerabilities exist, more vulnerabilities are revealed over time.

Human error and uncertainty: The saga around the Diebold Accu-Vote TS, which was used by roughly 10% of the electorate in the United States in the 2006 mid-term elections, reveals a litany of human errors. Researchers found that the machines ran on a Windows operating system, which made it fairly easy for anyone with access to them to insert malicious software into them. In addition, as Mr Duigan writes, "the lock on the machine was easily picked with a paperclip", while a single universal key provided access to all the machines. Moreover, the company had posted on its website a photograph of that single key which was detailed enough to allow the making of physical copies of it. [28]

In addition, though the VVPAT system has improved public confidence in electronic voting, it also has various technical vulnerabilities which have come to light over time. Its value also depends on people being able to remember how they voted, which might seem a simple thing. In practice, however, writes Mr Duigan, "voters often have a poor recollection of how they voted, and can easily be convinced that they made an error"[29]. For this reason, a paper receipt is "insufficient to ensure integrity".[30]

Human error – particularly on the part of "unwitting insiders" – can be particularly damaging. Well-meaning staff working, for example, for election officials or vendor companies can inadvertently introduce vulnerabilities by failing to take adequate security precautions. (They might, for instance, use weak passwords or fall for phishing scams). They could also help to misconfigure systems by mistake, or by failing to follow established protocols.

Malicious insider threats: Most analyses assume that the biggest risk comes from external actors intent on gaining access to electronic voting machines and priming them to malfunction. However, the most dangerous threats – and the ones most difficult to detect or counter – come from insiders with authorised access and malign intent.

---

[26] Ibid, citing Taş & Tanrıöver, 2020: 4
[27] Ibid, citing Hasanova et al, 2018
[28] Ibid p. 7.
[29] Ibid, citing DeMillo, Kadel & Marks, 2018
[30] Ibid, p. 7.

Many "insiders" will inevitably have access to the machines, including election officials, IT experts charged with maintaining them and employees of the vendor companies which have supplied them. Their privileged access and in-depth knowledge makes them particularly dangerous, for it allows them to manipulate software, disable security features, steal the personal details of registered voters and alter voting results.[31]

4.6 The costs and speed of electronic voting

Proponents of electronic voting applaud its speed in tallying votes, as this allows overall results to be computed within minutes of polls closing. However, if no accompanying paper record has been generated, each election machine constitutes an inscrutable "black box" – and the accuracy of its cannot be fully verified. This undermines trust and may lead to costly and lengthy court challenges to the election results initially so swiftly computed.

VVPAT systems, with their printed receipts for votes cast, increase trust but add to cost and expense. The voting system becomes a hybrid one, in which an initially fast electronic count must be supplemented to some extent by a further manual count of paper receipts. This duplicates many costs, including personnel and logistics ones. Moreover, if the election outcome is close – or if parties have reason to distrust the official results – a full manual count of paper receipts may be needed. The high costs of electronic machines, as further outlined below, is then compounded by the costs of printing all the paper receipts and conducting a full manual count. Overall, this is likely to be more expensive – and more time-consuming – than if a manual system had been used at the start.

In addition, the initial costs of acquiring the necessary hardware and proprietary software for electronic voting machines are extremely high – and all the more so if VVPAT printers and software are used. Often these costs are so high, as Mr Duigan points out, that countries have little choice but to keep using the same machines for 20 to 30 years. However, no system can guard effectively against all the additional vulnerabilities likely to arise over this period.[32] Public trust in the machines thus diminishes with the passage of time, adding to demands for more comprehensive (and expensive) manual recounts.

The costs of maintaining the machines and safeguarding them against the new vulnerabilities sure to emerge over time are also very high. So too are essential storage, transport and security costs. Rigorous – and costly – procedures for documenting who has physical access to the machines and the data storage devices must also be maintained at all times. If this is not achieved, a single incident of unlogged access to them could lead to the undetectable manipulation of thousands of votes.

Voter education costs are also likely to be high, especially in countries with limited literacy and familiarity with digital technologies. A lack of public confidence in the accuracy of electronic voting may also lead to time-consuming and expensive court battles. Even where there is a comprehensive paper-based back-up, an electorate which distrusts the body administering the

[31] Ibid, pp. 4 – 6.
[32] ibid, p. 4.

poll is likely to reject the results, leading to additional legal battles and yet higher costs. This has been evident in both Namibia and Venezuela, as further outlined below.

4.7 The claimed appeal of electronic voting to young voters

It has sometimes been suggested that a shift to electronic voting could encourage apathetic and disengaged young voters to start registering and voting. This argument may have some validity where an i-voting system is in force and people are able to vote from their homes via the Internet. However, most electronic voting systems require voters to come to polling stations, which requires more time and effort. In addition, the reasons young people in many countries are staying away from the polls are political, not technological. Many young people have become disillusioned with democracy, which they see as incapable of resolving the complex problems confronting their societies. Shifting from manual to electronic voting systems is unlikely to overcome this disaffection.

5 Experience in countries which have abandoned electronic voting

According to the IEC Discussion Document, seven countries have tried and subsequently abandoned electronic voting. These are Namibia, the Democratic Republic of the Congo, Germany, Ireland, the Netherland, Norway and Peru. Why each of these countries rejected electronic voting is briefly described below.

5.1 Namibia

According to the IEC Discussion Document, the Electoral Commission of Namibia (ECN) decided to "switch to EVMs" after logistical difficulties and "a cumbersome verification process" had resulted in a six-day delay in the release of election results in 2009. The ECN said the use of EVMs would speed up the tally, "make for accurate human-error-free results", increase efficiency, and "improve voter convenience".[33]

In 2014 the Electoral Act was amended to allow this shift. The amendments empowered the ECN to "adopt voting by voting machines as may be prescribed". However, they also stated that the use of EVMs was "subject to the simultaneous utilisation of a verifiable paper trail for every vote cast by a voter, and [that] any vote cast would be verified by a count of the paper trail". In addition, if EVM results and paper trails did not accord, "the paper trail results would be accepted as the election outcome" for the polling station in issue.[34]

The minister for regional and local government was empowered to bring these provisions into effect by notice in the *Gazette*. In doing so, however, the minister omitted the sub-sections requiring a verifiable paper trail and giving it priority in deciding disputes. The effect was to introduce EVMs without the paper trail Parliament had expressly mandated. [35]

The use of EVMs without a paper trail was challenged on the eve of the 2014 election, but dismissed by the High Court (in the *Maletzky* case) on the basis that the paper trail provisions

[33] IEC Discussion Document, p. 47.
[34] *Itula* v *Minister of Urban and Rural Development and others*, Supreme Court of Namibia, Case No 1/2019, para. 34.
[35] Ibid, paras. 30, 40.

were not yet in force.[36] The ECN later indicated that it might introduce a paper trail before the 2019 presidential election, but waited until a month before the poll to announce that it would not in fact be doing so. [37]

This timing made it difficult to for the main opposition candidate in the 2019 presidential election, Panduleni Itula, to challenge the ECN's decision before the poll took place.[38] The election result subsequently announced accorded 56% of the vote to Hein Geingob of the South West African People's Party (Swapo) and 29% to Mr Itula.[39] Mr Itula's challenge thus proceeded and the Namibian supreme court handed down its judgment early in 2020.

The court found that the relevant minister had acted unconstitutionally in 2014 in failing to bring the paper trail clauses into effect, as Parliament had required.[40] The court also ruled that the paperless voting system used in the 2019 election had breached the guaranteed right to vote of Namibians. "The essence of the democratic process lies in elections conducted with transparency and accountability," it stressed.[41] The court also cited with approval a judgment of the Supreme Court of India, which had found that "a paper trail is an indispensable requirement of free and fair elections". In similar vein, it cited a ruling by the German Constitutional Court finding that EVMs are constitutionally compliant only where "the constitutionally required possibility of a reliable correctness check is ensured" and "votes are recorded elsewhere in addition to the electronic storage". [42]

However, despite having made these important findings of unconstitutionality, the Namibian Supreme Court declined to set aside the outcomes of the 2019 presidential election. Mr Itula had claimed that there were various irregularities in the functioning of the EVMs, but he had failed to provide adequate proof of this.[43] By contrast, the chairperson of the ECN had told the court that, while "no election anywhere was perfect", the presidential election had "reflected the will of the people and was transparent, free and credible".[44]

Overall, the Supreme Court went on, it had not been established that "the lack of a verifiable paper trail…had adversely impacted on the electorate's fundamental right to vote". In addition, the ECN had "proceeded without a paper trail on the clear assumption that it was by law entitled to do so". Added the court:[45]

> The Minister had in 2014 not put [the relevant sub-sections] into operation and when this was challenged, the High Court had in *Maletzky* upheld the Minister's determination and sanctioned the use of EVMs without a paper trail. The ECN had thus set out to act in

[36] Ibid, para. 59, 93.
[37] Ibid, paras. 59 – 62, 94 – 105.
[38] Ibid.
[39] Ndeyunyema, N, 'Vote, But You Cannot Verify: The Namibian Supreme Court's Presidential Election Decision, Oxford Human Rights Hub, 17 February 2020: https://ohrh.law.ox.ac.uk/vote-but-you-cannot-verify-the-namibian-supreme-courts-presidential-election-decision/#
[40] *Itula* v *Minister of Urban and Rural Development*, op cit, paras. 64, 70 – 76.
[41] Ibid, paras. 67 – 69, 82.
[42] Ibid, paras. 67, 69.
[43] Ibid, paras. 86 – 92.
[44] Ibid, para. 92.
[45] Ibid, para. 93.

> accordance with the law as then determined… Its chairperson states that the ECN was scrupulous in applying the law…as then determined by the High Court. [It was also] satisfied that the EVMs were capable of producing a free and fair, and credible election – and…that the EVMs effectively did so."

The ECN's rose-tinged assessment was thus accepted as true, while the difficulty of proving deficiencies in "black-box" EVMs was effectively brushed aside. Commented Dr Njodi Ndeunyema in the University of Oxford *Human Rights Hub* journal: "Paperless EVMs inherently undermine the election outcome challenger's ability to collect evidence of electoral manipulation for judicial assessment; the issue is not strictly one of *actual* manipulation but the high risk of *potential* and *opportunity* for manipulation". Moreover, "in declining to nullify the election, the Court had rendered hollow its own assertion of the 'indispensable' requirement of paper trails in electoral transparency, credibility and verifiability".[46]

In describing these developments in Namibia, the IEC Discussion Paper suggests that the ECN decided against adding a paper trail before the presidential election in 2019 because costs (at N$160 million) were too high. It also indicates that the problem lay with the Indian company that had supplied Namibia's EVMs and was too "busy" with Indian elections to help.[47] However, it has also been suggested that the ECN's specific EVM models were incompatible with a VVPAT system and the manufacturer was thus unable to provide a solution. Namibia reverted to a manual, paper-based system for subsequent elections in 2020 and 2024.

5.2 Democratic Republic of the Congo

As the IEC Discussion Document describes it, the decision to implement electronic voting in the Democratic Republic of the Congo (DRC) was made in 2018 by the Congolese Electoral Commission (CENI). This was necessary, said CENI, because hundreds of candidates planned to contest the presidential, national and provincial elections and this would result in "extremely long paper ballots…printed on dozens of pages". The costs of transporting printed ballot papers to 84,000 polling stations over often difficult terrain would also be very high. Hence, a shift to electronic voting would save up to $100 million, CENI stated.[48]

Though opposition parties objected that EVMs would be three times more costly, CENI's decision stood. However, it had to be abandoned after two of the three voting test kits supplied by South Korean company MIRU Data Systems malfunctioned, which meant that CENI's planned e-voting pilot study was unable to proceed. Resistance to the shift was also fueled by MIRU's touchscreen technology, which was unfamiliar to many voters. In addition, CENI lacked the time and budget for comprehensive voter education or even for the training of its own staff. According to the IEC Discussion Document, "the lack of a clear and transparent process for monitoring and auditing the electronic voting [further] raised alarms among stakeholders".[49]

---

[46] Ndeyunyema, N, 'Vote, But You Cannot Verify: The Namibian Supreme Court's Presidential Election Decision, Oxford Human Rights Hub, 17 February 2020: https://ohrh.law.ox.ac.uk/vote-but-you-cannot-verify-the-namibian-supreme-courts-presidential-election-decision/#.

[47] IEC Discussion Document, p. 47.

[48] Ibid, pp. 47 – 48.

[49] Ibid, p. 48.

5.3 Ireland

According to the IEC Discussion Document, Ireland spent some 60 million euros on an e-voting system without VVPAT between 2005 and 2009. Its election monitoring bodies (EMBs) had presumed a technologically advanced electorate would welcome the shift. Instead, voters "rejected the lack of transparency". In addition, reports the IEC, "the system was deemed unreliable and would have required additional costly modifications before it could be used". The machines were never used, but the country is still paying storage costs for them.[50]

5.4 Germany

"Electronic voting trials were conducted in Germany from 1998 to 2005", says the IEC Discussion Document. However, the proposed shift away from manual voting was abandoned in 2009, when the German Federal Constitutional Court ruled that electronic voting was unconstitutional without adequate safeguards capable of making "the entire electoral process, including vote casting and counting,...subject to scrutiny".[51]

The court found that "the public nature of elections", as set out in the Basic Law, "requires that all essential steps in the elections [must be] subject to public examinability". The court pointed out that, "in a representative democracy", the election of the people's representatives "constitute[s] the fundamental act of legitimisation". A viable democracy requires "compliance with election principles", together with public confidence that they are being fulfilled. "Only by the possibility of monitoring whether the elections comply with the constitutional election principles is it possible to ensure that the delegation of state power to the people's representati[ves]...does not suffer from a shortcoming". [52]

The court went on: "In a republic, elections are a matter for the entire people and a joint concern of all citizens. Consequently, the monitoring of the election procedure must also be a matter for and a task of the citizen. Each citizen must be able to comprehend and verify the central steps in the elections reliably and without any special prior technical knowledge... Particular significance attaches here to the monitoring of the election act and to the ascertainment of the election result. An election procedure in which the voter cannot reliably comprehend whether his or her vote is unfalsifiably recorded and included in the ascertainment of the election result, and how the total votes cast are assigned and counted, excludes central elements of the election procedure from public monitoring, and hence does not comply with the constitutional requirements."[53]

According to the court "it is primarily a matter for the legislature" to ensure that these principles are upheld". However, the Federal Constitutional Court must "review whether the legislature has remained within the boundaries of the latitude granted to it by the Basic Law". In the context of electronic voting, "the deployment of voting machines which record the voters' votes

[50] IEC Discussion Document, p. 49.
[51] Ibid.
[52] Federal Constitutional Court, Judgment of the Second Senate of 3 March 2009, Point 2(a), (aa), para. 109.
[53] Ibid, Point 2(bb), (cc), (b), paras. 110, 112, 113.

in electronic form and ascertain the result of the election electronically is…only compatible with the Basic Law subject to strict preconditions".[54]

Added the court: "It must be possible to check the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge". This is a necessity because electronic machines are susceptible "to manipulation" and have an "amenability to error". In addition, "the acceptance of the voters' votes and the calculation of the election result is based on a calculation act which cannot be examined from outside or by persons without special computer knowledge". This means that "errors in the voting machine software are…difficult to recognise".[55]

Yet "such errors can affect not only one individual election computer, but all the devices used". By contrast, "manipulations or election falsifications…are only possible [with manual voting systems] with considerable effort and with a very high risk of discovery, which has a preventive impact". With electronic voting, however, "a major impact may in principle be achieved with relatively little effort by encroachments on electronically controlled voting machines. Manipulations of individual voting machines can also influence not only individual voters' votes, but all votes cast with the aid of this device. The scope of the election errors which are caused by alterations and malfunctions of a single software program affecting multiple devices is even wider."[56]

Special precautions are thus essential. "The voter himself or herself must be able to verify…whether his or her vote as cast is recorded truthfully as a basis for counting or…for a subsequent re-count. It is not sufficient if he or she must rely on the functionality of the system without the possibility of personal inspection. It is hence inadequate if he or she is exclusively informed by an electronic display that his or her ballot has been registered. This does not facilitate sufficient monitoring by the voter. Equal viability must also apply to the election bodies and to interested citizens."[57]

The court went on: "The consequence of this is that the votes may not be stored exclusively on an electronic storage medium after the ballot. The voter may not be required to trust solely in the technical integrity of the system after the electronic ballot. If the election result is ascertained by computer-controlled processing of the votes stored in an electronic storage medium, it is not sufficient if only the result of the calculation process as implemented in the voting machine can be taken note of using a summary paper printout or an electronic display… It is not easily recognisable in such cases whether there have been programming errors in the software or targeted election falsifications through manipulation of the software or of the voting machines."[58]

[54] Ibid, points 2(d), 3, paras. 116 – 118.
[55] Ibid, point 3(a), para. 120.
[56] Ibid, point 3(a), para. 120, ibid.
[57] Ibid, point 3 (b), para 121.
[58] Ibid, point 3 (aa), para. 122.

This did not mean that electronic voting was excluded altogether, but it did require adequate safeguards. Said the court: "The legislature is not prevented from using electronic voting machines in the elections if the constitutionally required possibility of a reliable correctness check is ensured. In particular, voting machines are conceivable in which the votes are recorded elsewhere in addition to electronic storage. This is for instance possible with electronic voting machines which print out a visible paper report of the vote cast for the respective voter, in addition to electronic recording of the vote, which can be checked [by the voter] and is then collected to facilitate subsequent checking." Safeguards of this kind would ensure that "the voters are in charge of their ballot and that the result of the election can be reliably checked by the election authorities or by interested citizens without any special prior technical knowledge".[59]

According to the IEC Discussion Paper, the lesson for South Africa from the court's judgment is that "public scrutiny and transparency is important when implementing electronic voting".[60] The more pertinent lesson, however, is that voters must be able to ensure that their votes have been accurately captured and accurately counted – and that the capacity for this public monitoring is vital to democracy.

5.5 The Netherlands

As the IEC Discussion Document reports, the Netherlands in 2008 "withdrew [its] e-voting machines after over 20 years of use and returned to paper ballots". This, it suggests, is because "two versions of the software failed to address risk and trust issues". In addition, "an official commission found that the Ministry of the Interior and Kingdom Relations, which was responsible for organising elections, was lacking in-house expertise, causing too much dependence on vendors and certification agencies".[61]

Having failed to acknowledge the validity of such concerns, the IEC Discussion Document states that many voters in the Netherlands "still trust e-voting" and want to return to it "on the basis of positive experiences from the past". Moreover, the document fails to draw the key lesson for South Africa: which is that major risks were uncovered, leading to the abandonment of electronic voting. Instead, it stresses that "the IEC should work closely with experts in the field of electronic voting and ensure they build internal capacity in this area".[62]

This comment suggests that a key IEC aim is to expand its own expertise and thereby consolidate its control over a voting system that is opaque to others and can thus be manipulated without significant risk of detection.

5.6 Norway

According to the IEC Discussion Document, Norway sought to introduce an Internet voting ("i-voting) system rather than an electronic one using EVMs at polling stations. In 2008, it decided to pilot i-voting in the local government election to be held in 2011, some three years hence.

---

[59] Ibid, point 3 (bb), paras. 123, 124.
[60] IEC Discussion Document, op cit, p. 49.
[61] Ibid, p. 50.
[62] Ibid.

Though the pilot was confined to ten municipalities out of 429 – and Norway had only 3.8 million registered voters in this period – the time and effort involved in preparing the i-voting system was substantial.[63]

Adds the IEC: "Despite a high level of trust in the electoral system, Norway discontinued internet voting due to concerns about voter coercion and the potential for votes to become public, which could undermine the democratic process. Additionally, the low uptake of online voting (only about 1.5% of voters) indicated a preference for traditional voting methods, leading to the decision to abandon the initiative."[64]

Again, the lesson the IEC draws is not that Internet voting brings risks and may be comprehensively rejected by voters, but rather that adequate time – say, three to four years – is needed for preparation, especially "in a young democracy like South Africa, where citizens may similarly prefer to vote in person".[65]

5.7 Peru

In 2010, following delayed election results in various municipal and regional polls, the Peruvian Congress called on the country's election institutions to explore the possibility of shifting to electronic voting. The National Office of Electoral Processes (ONPE) was asked to conduct a pilot of electronic voting technology – and was assisted by the International Republican Institute (IRI) in the United States in doing so.[66]

Following the pilot, the ONPE and IRI concluded that there were many technical and logistical obstacles to implementing a national electronic voting system that would have to be overcome. Though this might be achieved, a further challenge was that the costs would be extremely high. Since then, as the IEC Discussion Document records, "the Peruvian Congress has not demonstrated serious interest in allocating any significant level of funding for electronic voting".[67]

6 Experience in countries which use electronic voting

The IEC Discussion Document provides examples of seven countries that use electronic voting. (It also describes Internet voting in Estonia and the various voting systems used in different states in the United States of America (US). However, the experiences of these two countries is omitted from this submission as the IEC's main focus is on EVMs intended for use in polling stations.)

In describing the experience of these seven countries, the IEC Discussion Document fails to mention how very few states across the world have opted for electronic voting. Yet, as the International Institute for Democracy and Electoral Assistance (International IDEA) has pointed out, the overall number of countries using e-voting is limited to 34 or 19% of the total. By

[63] IEC Discussion Document, ibid, p. 50.
[64] Ibid.
[65] Ibid.
[66] Ibid, p. 51.
[67] Ibid.

contrast, 81% of countries have chosen not to use it. Voters in most countries – including the most advanced democracies – thus still cast their ballots on paper.[68]

6.1 India

India had a population of close on 1.4 billion people in 2022 and needed to cater for almost 970 million voters in its most recent elections, held in 2024.[69] Mainly because of the country's population size – but also because some polling stations had been violently seized and flooded with fake ballots[70] – electronic voting pilots began in 1982. By 2002 simple, paperless and stand-alone EVMs, powered by batteries and unconnected to the Internet, were in use across the country.[71] These EVMs were developed by two state-owned enterprises, Bharat Electronics Limited and Electronics Corporation of India Limited, which could be seen as adding to state control and eroding the independence of the system.[72] All elections are administered by the Electoral Commission of India (ECI).[73]

The IEC Discussion Paper claims that India's EVMs are broadly trusted, but opposition parties have long warned about their vulnerability to manipulation. In 2013 the Supreme Court of India, in *Dr Subramanian Swamy* v *Election Commission of India*, ruled that a VVPAT system must be introduced as well, as an accompanying paper trail was "an indispensable requirement of free and fair elections". However, this could be done on a phased basis, given the magnitude of the task.[74]

By 2017 all electronic voting systems included a "ballot unit", with buttons showing the names and symbols of the candidates, a "control unit" administered by the polling officer, and a VVPAT printer.[75] Once the voter presses the button on the ballot unit to make his or her choice, the control unit sends a message to the VVPAT printer, which then prints a receipt. This is displayed to the voter for seven seconds from behind a translucent screen. After seven

---

[68] Gemini AI: International Institute for Democracy and Electoral Assistance (International IDEA), 'Use of E-Voting Around the World', 6 February 2023: https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world.

[69] IEC Discussion Document, p. 39; Jacinto, L, Trust deficit at the heart of India's electronic voting debate, *France24*, 3 May 2024: https://www.france24.com/en/asia-pacific/20240503-trust-deficit-at-the-heart-of-india-s-electronic-voting-debate.

[70] Somanathan, M. (2019). India's electoral democracy: How EVMs curb electoral fraud. *Brookings,* 5 April. Available from: https://www.brookings.edu/articles/indias-electoral-democracy-how-evms-curb-electoral-fraud/; Sisir, D., Mudit, K. and Shamika, R. (2017). The Impact of Electronic Voting Machines on Electoral Frauds, Democracy, and Development. Indian School of Business WP Forthcoming, 16 March. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041197.

[71] IEC Discussion Document, p. 39.

[72] EVMs, VVPATS designed, manufactured indigenously by 2 PSUs: Government, 17 March 2023, Business Standard. Available from: https://www.business-standard.com/evms-vvpats-designed-manufactured-indigenously-by-2-psus-government-123031701024_1.

[73] Bawa J, Singh S and Singh D, 'EVM Allegations: Deflecting Accountability In Indian Politics – Analysis' Eurasia Review, 13 December 2024: https://www.eurasiareview.com/13122024-evm-allegations-deflecting-accountability-in-indian-politics-analysis/.

[74] *Dr Subramanian Swamy* v *Election Commission of India*, Civil Appeal No 9093, 8 October 2013, paras. 29, 30: https://indiankanoon.org/doc/113840870/.

[75] Supreme Court of India, Summary of leading opinion by Justice Sanjiv and concurring opinion by Dipankar Datta, 3 May 2024: https://www.scobserver.in/reports/vvpat-vote-verification-judgement-summary/.

seconds, the receipt is automatically cut and drops into a sealed ballot box, from which it can, if necessary, be extracted and counted.[76]

This system is seen as meeting a voter's need for reassurance that his vote has been accurately recorded and will be accurately counted. However, voters may find it difficult to read the receipts behind the screen in the short time allowed. In addition, penalties are applied to any voter who claims a discrepancy but is unable to prove it, which deters people from raising objections.[77] Moreover, even if all votes are properly recorded, this does not guarantee that they will be accurately counted.

In addition, few VVPAT receipts are taken into account. ECI guidelines initially stated that "only one randomly selected polling station in each constituency would undergo verification of VVPAT slips". In 2019, in *N. Chandrababu Naidu v Union of India*, the Supreme Court directed that physical verification should be increased from one ECM to five ECMs in each constituency .[78] However, concerns remain that this is too small a sample to provide adequate verification of overall election results.

In 2023 a civil society organisation, the Association for Democratic Reforms, applied for an order compelling 100% VVPAT verification, but the Supreme Court rejected this. It said that there was insufficient evidence of shortcomings to warrant full VVPAT verification and a manual count, as this would be costly and time-consuming.[79] According to the Court, "there were no instances, except one, where data from the VVPAT was found to be mismatched with the votes cast through EVMs. The one instance took place in the 2019 Lok Sabha Elections in Andhra Pradesh where a presiding officer forgot to delete mock poll data, resulting in a discrepancy".[80] The Court did, however, rule that dissatisfied candidates who come second or third in a constituency may, within seven days, require "a panel of engineers from the manufacturing companies to inspect whether the burnt memory in the semi-controller of the EVMs has been tampered with in five percent of the EVMs within a constituency". However, those requesting this would have to pay for this inspection – though the costs would be refunded if any irregularity was found.[81] The refund rule gives the state's technicians still more reason *not* to

---

[76] Chokkar, J S, 'It's EVS – electronic voting system – not EVM', *The Week* magazine, 7 April 2024: https://www.theweek.in/theweek/current/2024/03/30/electronic-voting-machines-drawbacks-and-solutions.html; Supreme Court of India, Summary of leading opinion by Justice Sanjiv and concurring opinion by Dipankar Datta, 3 May 2024: https://www.scobserver.in/reports/vvpat-vote-verification-judgement-summary/.

[77] Chokkar, J S, 'It's EVS – electronic voting system – not EVM', *The Week* magazine, 7 April 2024: https://www.theweek.in/theweek/current/2024/03/30/electronic-voting-machines-drawbacks-and-solutions.html.

[78] Supreme Court of India, *N Chandrababu Naidu v Union of India*, Case no WP (C) 273/2019, 8 April 2019: https://indiankanoon.org/doc/24904462/; see also Supreme Court of India, Summary of leading opinion by Justice Sanjiv and concurring opinion by Dipankar Datta, 3 May 2024: https://www.scobserver.in/reports/vvpat-vote-verification-judgement-summary/.

[79] Jacinto, L, Trust deficit at the heart of India's electronic voting debate, *France24*, 3 May 2024: https://www.france24.com/en/asia-pacific/20240503-trust-deficit-at-the-heart-of-india-s-electronic-voting-debate; Supreme Court of India, Summary of leading opinion by Justice Sanjiv and concurring opinion by Dipankar Datta, 3 May 2024: https://www.scobserver.in/reports/vvpat-vote-verification-judgement-summary/.

[80] Supreme Court of India, Summary of leading opinion by Justice Sanjiv and concurring opinion by Dipankar Datta, 3 May 2024: https://www.scobserver.in/reports/vvpat-vote-verification-judgement-summary/.

[81] Supreme Court of India, Summary of leading opinion by Justice Sanjiv and concurring opinion by Dipankar Datta, 3 May 2024: https://www.scobserver.in/reports/vvpat-vote-verification-judgement-summary/

find relevant problems. In addition, a "request for information" to the ECI has revealed that EVMs "do not have software permanently burnt into one-time programmable (OTP) chips, as previously claimed. Instead, they use chips that can be reprogrammed, raising concerns about the potential for unauthorised modifications".[82]

According to the IEC Discussion Document, India's electronic voting system (the word "machine", in the singular, seems inappropriate for a system with three linked components)[83] has demonstrated "the potential of technology to enhance democratic processes. By embracing e-voting, India has set a benchmark for other large democracies considering electoral innovation".[84] The IEC acknowledges that India's enormous population, which is many times bigger than South Africa's, provides the main reason why an electronic system is needed to cater for almost a billion voters. It also avers that the system is accurate and reliable – and is thus broadly trusted. Yet, as *France24.com* reported in May 2024, "opinion polls have recorded undisputed declines in levels of trust among Indian voters". In 2024, moreover, "the biggest Indian pre-election poll, the CSDS-Lokniti pre-poll study, found that public trust in Election Commission and EVMs had dropped from roughly half in 2019 to about a quarter five years later."[85]

Various commentators state that the Indian system is well protected and that "the M3 EVM is a standalone device akin to a simple calculator and incapable of being hacked". The M3 model introduced in 2019, they add, "incorporates automated functions that revert the machine to factory settings if tampering is detected". In addition, "Indian EVMs undergo stringent checks to uphold their integrity, [including] mock polling exercises conducted under the scrutiny of candidates' representatives. The machines are then sealed using specialized security paper from the Nashik security printing press – the same material used for Indian currency notes. Additionally, EVMs are stored in highly secure locations under strict surveillance, with provisions for continuous monitoring by candidates or their designated representatives, ensuring transparency and trustworthiness throughout the electoral process."[86]

However, various critics continue to claim that the system has major vulnerabilities which need to be addressed. The biggest problem is that very few VVPAT receipts are ever checked. In addition, voters are given only seven seconds to read the VVPAT receipts displayed behind the translucent screen, while the risk of penalties encourages them to remain silent rather than

---

[82] Bedi, A, EVM & VVPAT in Elections: Legal Battles & Technical Challenges Explained! LawChakra, blog, 12 Feb 2025: https://lawchakra.in/blog/evm-vvpat-elections-challenges/.

[83] Chokkar, J S, 'It's EVS – electronic voting system – not EVM', *The Week* magazine, 7 April 2024: https://www.theweek.in/theweek/current/2024/03/30/electronic-voting-machines-drawbacks-and-solutions.html op cit.

[84] IEC Discussion Document, p. 39.

[85] Jacinto, L, Trust deficit at the heart of India's electronic voting debate, *France24*, 3 May 2024: https://www.france24.com/en/asia-pacific/20240503-trust-deficit-at-the-heart-of-india-s-electronic-voting-debate; see also Shastri, S, The Hindu, 'CSDS-Lokniti 2024 pre-poll survey | Level and intensity of voter trust in select institutions and processes', 12 April 2024: https://www.thehindu.com/elections/csds-lokniti-2024-pre-poll-survey-level-and-intensity-of-voter-trust-in-select-institutions-and-processes/article68054233.ec.

[86] Bawa J, Singh S and Singh D, 'EVM Allegations: Deflecting Accountability In Indian Politics – Analysis', Eurasia Review, 13 December 2024: https://www.eurasiareview.com/13122024-evm-allegations-deflecting-accountability-in-indian-politics-analysis/.

object.[87] It would thus be preferable, some critics say, for the VVPAT receipts to be made available to voters who would be able to scrutinise them properly before placing them in sealed ballot boxes. Counting all these receipts could be speeded up by printing a bar-code on each one, as this would allow a machine to do the tallying.[88] The paper on which the VVPAT receipts is printed should also be of "good and durable quality capable of retaining the printed information for seven years" (as opposed to the current paper from which the printed matter reportedly disappears after a rather short time).[89]

In addition, critics say, all EVMs are vulnerable to manipulation in various ways. "Attackers can change the votes stored in electronic voting machines between the election and the public counting session using a pocket-sized device, altering the election outcome. Even electronic identification to access the voting machine can be vulnerable to cyber-attacks... Furthermore, the lack of transparency in electronic voting systems can make them susceptible to dishonest vote counting, while computers can be programmed to count votes honestly or dishonestly."[90] Critics have also proposed that further safeguards be introduced. They recommend, for example, that "robust encryption protocols be used to secure data transmission between EVMs and central servers" and so guard against interception and tampering; that "multiple authentication steps" be introduced to prevent unauthorised access to EVMs; that an "independent audit" of proprietary software should be introduced, with regular security checks and "expert vulnerability assessments"; and that additional measures should be used to secure EVMs while they are in storage or being transported.[91] (Even where no attempt at fraud is in issue, transporting millions of machines across India's vast and diverse land mass is an enormous logistical challenge that sometimes involves the use of helicopters – but can also require elephants, camels or bullock carts in areas still lacking modern infrastructure.)[92]

The IEC Discussion Document brushes aside these problems, however. It describes the Indian experience as "a transformative journey, showcasing the potential of technology to enhance democratic processes" and thereby "setting a benchmark for other large democracies considering electoral innovation". It praises the hands-on involvement of the ECI in helping to create the two SOEs responsible for designing and manufacturing the machines and in "coordinating the implementation of e-voting". It claims that "the processes were transparent and understood by the electorate", when experts warn that considerably more needs to be done to scrutinise the software and reduce the risks of covert manipulation. It praises the Supreme Court for being "meticulous in applying the law",[93] but it fails to acknowledge that

---

[87] Chokkar, op cit.
[88] Ibid.
[89] Ibid.
[90] Devpura, H and Johari, Y, 'Critical analysis of electronic voting system; Security concerns and policy implications in India', *International Journal of Advanced Legal Research*, Volume 4, Issue 3, February 2024, ISSN 2582 – 7340: https://ijalr.in/wp-content/uploads/2024/04/Heeral-and-yash-Research-paper.pdf.
[91] Devpura, H and Johari, Y, 'Critical analysis of electronic voting system; Security concerns and policy implications in India', International Journal of Advanced Legal Research, Volume 4, Issue 3, February 2024, ISSN 2582 – 7340: https://ijalr.in/wp-content/uploads/2024/04/Heeral-and-yash-Research-paper.pdf.
[92] Pasricha, A. (2014). India's Election Involves Daunting Logistical Challenges. VOA, 25 March. Available from: https://www.voanews.com/a/indias-election-involve-daunting-logistical-challenges/1878514.html
[93] IEC Discussion Document, op cit, p. 39.

VVPAT verification ordered by the court needs to be far more extensively applied to guard against potential fraud and increase voter trust and confidence in the system.

6.2 Brazil

Brazil also has a large voting population (100 million in 2000), many of whom are illiterate. According to the IEC Discussion Document, Brazil's complex voting system required voters to "choose from thousands of legislative candidates, making results tabulation a logistical challenge". Brazil's election monitoring body, the Tribunal Superior Electoral (TSE) or the Superior Electoral Court, thus "conceptualised and led the development" of a Direct-Recording Electronic (DRE) voting system, known as the *urna eletrônica* or the *urna*, for short.[94]

The TSE introduced the *urna* by incremental steps. The devices were first used in 1996 by 30% of participating voters, amounting to some 33 million people. Thereafter, in 1998, the *urna* was extended to 60% of voters (68 million people) and then to 100% of voters (110 million) in 2000. The user interface on the *urna* has a numeric keypad (similar to that on a smartphone) through which voters enter the numbers associated with their preferred candidates. "The *urna* then displays the candidate photograph corresponding to that number, helping the voter affirm their selection."[95]

According to the IEC Discussion Document, the new system has greatly increased efficiency. It has "accelerated the vote count exponentially", whereas the earlier paper system required "multitudes of vote counters" and could result in weeks of "uncertainty and tension". The 1989 presidential election vote count, for example, took nine days. "By comparison, the 2022 run-off election count required less than 12 hours, underlining the time efficiency benefits of e-voting."[96]

The IEC document omits to mention that presidential candidate Luiz Inácio da Silva (known as "Lula") won the 2022 election on this second run-off count with a bare 50.9% of the vote, up from the 48.4% recorded in the first round.[97] Nor does the IEC acknowledge that the Brazilian system is in fact a paperless "black-box" one lacking any scope for VVPAT verification even where election results are very close – as they were in 2022.

The discussion document also glosses over the ramifications of comprehensive TSE control over the system. It notes that "the TSE develops the software, manufactures the machines through state-owned companies, and oversees the entire process", but makes no comment on this. Though critics claim that TSE control undermines a necessary independence from the government, the IEC seems to accept the TSE's view that central control is important in maintaining integrity and preventing fraud.[98]

---

[94] Ibid, p. 40.
[95] Ibid.
[96] Ibid.
[97] Wikipedia, 'Lula da Silva': Wikipedia: https://en.wikipedia.org/wiki/Luiz_In%C3%A1cio_Lula_da_Silva.
[98] Gemini AI, International IDEA, "Varieties of Electoral Integrity Risk: Protecting Elections in Brazil", Case study, September 2023, Tarouco, G. Available: https://www.idea.int/sites/default/files/2023-09/varieties-of-electoral-integrity-risk-protecting-elections-in-brazil-en.pdf.

Critics also complain that the TSE's proprietary source code is not publicly available for independent review and may thus have undetected "back doors" or other vulnerabilities. The TSE has tried to counter this criticism by holding public security tests, during which a commission of computer scientists and hackers is invited to try to break the system. Some vulnerabilities have been found and patched in this way, but critics have questioned whether the tests conducted are comprehensive or rigorous enough.[99]

The TSE nevertheless claims that its counter-measures against fraud are effective. Before voting begins, a report called the "zeroth" is printed from each machine. This report – which is signed by all party representatives present – is supposed to show that the machine has no pre-recorded votes already embedded within it. In addition, all the software used in the machines is digitally signed at a public ceremony (though this is clearly no substitute for an independent audit of it). When voting ends, moreover, each machine prints out a "bulletin" or summary of the votes cast at that particular polling station. This bulletin is signed by polling officials and party representatives and serves as a physical record for a public audit.[100] Again, however, voters have no means of verifying that their votes have been correctly recorded or counted.

The IEC brushes aside these issues in claiming that the "slow and steady" roll-out of the system has succeeded in "gaining public trust". Having ignored a number of relevant concerns, it concludes that Brazil's experience provides "important lessons".[101]

6.3 The Philippines

The Philippines, with some 65.7 million registered voters, uses a Precinct Count Optical Scan (PCOS) system. This allows voters to mark paper ballots manually, in the long-established way, while the ballots are then scanned and counted by machines. Following regional pilots in 2008, the system was implemented country-wide in 2010.[102]

The system is administered by the Commission on Elections (COMELEC). In the 2013 election, when the system was still new, various problems became evident (as the IEC Discussion Document acknowledges). Election officials had not been adequately trained, particularly on voter management and authentication, which led to inefficient processing and long lines. Other issues arose too, "such as the failure of machines to read security marks and the lack of training for staff on using security features". However, in the 2022 elections, COMELEC used approximately 107,000 Smartmatic Vote Counting Machines (VCMs) to facilitate the count at some 18,000 polling stations, which seems to have gone better.[103]

---

[99] Gemini AI, International IDEA, "Varieties of Electoral Integrity Risk: Protecting Elections in Brazil", Case study, September 2023, Tarouco, G. Available: https://www.idea.int/sites/default/files/2023-09/varieties-of-electoral-integrity-risk-protecting-elections-in-brazil-en.pdf; "Richter, A., "TSE Releases Electronic Voting Machine Security Test Results," 29 November 2021, Available from: https://agenciabrasil.ebc.com.br/en/justica/noticia/2021-11/tse-releases-electronic-voting-machine-security-test-results; Superior Electoral Court, n.d., Public safety tests (PSTs), https://international.tse.jus.br/en/electronic-ballot-box/public-safety-tests-psts.

[100] Gemini AI, https://international.tse.jus.br/en/electronic-ballot-box/auditability..

[101] IEC Discussion Document, op cit, p. 40.

[102] Ibid.

[103] Ibid.

On this slender foundation, the IEC Discussion Document concludes that "the successful handling of elections by COMELEC in the Philippines, even with challenges such as illiteracy and a complex geography, demonstrates that effective trust-building strategies and transparent processes can lead to successful electoral outcomes".[104]

6.4 Venezuela

The IEC Discussion Document fudges the fundamental problems in Venezuela's electronic voting system. This was introduced in 1998, with EVMs supplied by a Spanish firm (named Indra) being used in the December presidential election that brought Hugo Chávez to power. Observers from the International Republican Institute (IRI) in the United States reported that the machined had functioned well in the vast majority of sites they visited.[105]

Six years later, when Chávez faced a recall referendum (as opposition parties had mustered sufficient signatures on a petition demanding this), the Spanish EVMs were nevertheless replaced by ones supplied by Smartmatic. Smartmatic was a company founded in Florida in 1999 by Antonio Mujica and two other Venezuelan engineers and it had no experience with EVMs. It was nevertheless awarded the $91 million contract to supply the new machines, together with a small software company called Bizta, which was part owned by Mujica and the Venezuelan government (which held a 28% stake). When Chávez won the recall election, some critics alleged that there were significant disparities between this outcome and what exit polls had showed. However, the Carter Institute did an audit and thereafter endorsed the election result, as did the US State Department.[106]

Smartmatic continued to provide Venezuela's election technology until 2017, when the company claimed that a million votes had effectively been "lost" during the 30 July election for a Constituent Assembly. According to Mujica, then Smartmatic CEO, the difference between the actual number of participating voters – and the number announced by the authorities – was "at least one million". He blamed the manipulation which had seemingly occurred on a lack of proper auditing by opposition parties.[107]

After 2017, Venezuela's election monitoring body – the National Electoral Council (CNE, in its Spanish acronym) – began using other EVMs but failed to disclose their supplier(s). In the 2024 presidential election, these EVMs were buttressed by a VVPAT system. Voters cast their ballots via touch screens on the EVMs, after which the machines printed out paper receipts, termed "*acta*" in Spanish. Having verified their ballots, voters deposited the *acta* in sealed ballot boxes. When the polls closed, the machines printed out partial summaries of the votes cast, while

---

[104] Ibid.

[105] The Carter Center, *Postelection Statement on Venezuela Elections*, 7 December 1998. https://www.cartercenter.org/news/documents/doc874.html#:~:text=Our%20delegates%20overall%20reported%20that,visited%2C%20the%20machines%20functioned%20well

[106] Zetter, K, 'New allegations against Smartmatic executive in company's voting machine contract with LA country, The Guardian, 26 August 2025: https://www.theguardian.com/us-news/2025/aug/20/smartmatic-voting-machines-bribery.

[107] Ibid; IEC Discussion Document, p. 43; Smartmatic, *Postelection Statement on Venezuela Elections, Dec. 7, 1998*, para 4, 6 December 1998: https://www.cartercenter.org/news/documents/doc874.html#:~:text=Our%20delegates%20overall%20reported%20that,visited%2C%20the%20machines%20functioned%20well.

copies of these "*acta*" tally sheets were given to representatives of opposition parties. Opposition parties claimed to have obtained more than 80% of these printed tally sheets, which provided a crucial manual back-up to the electronic results.[108]

The opposition's manual count showed a landslide victory for Edmundo González, the opposition candidate. However, the official results published by the CNE claimed that Chávez's successor as president, Nicolás Maduro, had won 51% of the vote. The CNE failed to provide a breakdown of the electronic vote tally from each polling station, which would have allowed for verification. Maduro was nevertheless declared the victor because the government controlled both the CNE and the Supreme Tribunal of Justice (TSJ), which soon endorsed Maduro's victory. This decision closed off internal legal channels for contesting this. Many countries and various international organisations questioned or rejected the official results, but they were swiftly accepted by China and Russia. This provided Maduro with international support and made it more difficult to challenge his claimed victory.[109]

The 2024 presidential election in Venezuela shows that even a comprehensive and credible paper trail may not be enough to invalidate an implausible outcome generated by EVMs. What also secured Maduro's victory was his government's control over the CNE and the TSJ – the key domestic institutions responsible for verifying and declaring the election results. This state control made it possible to discount the manual tally, rely on the electronic one instead, and declare Maduro the victor.

Commentators have suggested that the manual back-up system could have been strengthened by electoral rules requiring that the manual tally sheets (the "*acta*") be publicly posted at every polling station as soon as voting was complete. These tally sheets could also have been signed by all party representatives and then swiftly uploaded to a central database easily accessible to the public. Electoral rules could also have required a comprehensive audit of the election results at a significant percentage of randomly chosen polling stations. This would have allowed a direct comparison between the manual tally sheets and the EVM results for each of these stations. Electoral rules could also have required that full access and audit capacities be provided to independent election monitoring bodies with no ties to the Venezuelan government.[110]

The IEC Discussion Document brushes aside most of these issues. Instead of cautioning that Venezuela's EVMs might have helped Maduro claim an undeserved victory in the presidential election in 2024, it criticises the fact that the paper receipts were made available to voters at

[108] Associated Press, Venezuela's opposition secured over 80% of crucial vote tally sheets. Here's how they did it, CNN world, 2 August 2024:
https://edition.cnn.com/2024/08/02/americas/venezuelas-tally-sheets-intl-latam.

[109] Yang Lin, China stands by Maduro in Venezuela to safeguard its investments, Voanews, 3 August 2024:
https://www.voanews.com/a/china-stands-by-maduro-in-venezuela-to-safeguard-its-investments/7729148.html

[110] Carter Center, Venezuela - Final Report, 2025: Election Technologies, p.41:
https://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/venezuela/venezuela-final-report-2025.pdf

all. This, it implausibly claims, could have allowed "some voters [to] take the slips as a souvenir or [to] take them to a briber". [111]

In addition, though it notes Smartmatic's claim that "the voter turnout [in 2017] was manipulated by at least million votes", the IEC document brushes over the likely impact of this apparent intervention on the election results. Instead, it implicitly blames Smartmatic for having voiced a criticism that, it says, subsequently prompted a major fall in voter turnout (to a meagre 30%) in the 2020 parliamentary election. This assessment brushes aside the many other reasons that voters might have had for staying away from the polls.

As regards the 2024 presidential election, the IEC seems to see the main problem not as a seemingly fraudulent outcome, but rather as a deficit of trust on the part of voters. It goes on to say that "photos of the voting rolls" – not the tally sheets – were "uploaded…in a digitally scanned format that was easily accessible and verifiable by each and every citizen through a QR Code. Each code led to a sequence of numbers that identified the state and the voting centre, and the exact number of votes for each party and candidate".[112] (How photos of voting rolls could have yielded this information on votes cast is not explained.)

The IEC's confused description of events fails to acknowledge that the outcome of the electronic vote (victory for Maduro) was entirely different from the overwhelming support for González that the tally sheets had revealed. The IEC also overlooks the CNE's failure to provide the detailed EVM data from individual polling stations that would have allowed direct comparisons between electronic and manual results. Instead, the document states that the QR Code saga (as confusingly described by it) "illustrates that for e-voting to be truly accepted, it can be enhanced by other technologies, such as those used in parallel in the Venezuelan elections".[113] That Maduro was seemingly able to steal the election, despite the supposed safeguard of the VVPAT system, is simply ignored.

6.5 Bhutan

Bhutan is a small and mountainous country located on the Himalayan Mountain Range. In 2018, some 11 years after it had ceased to have an absolute monarchy, the country had fewer than 440,000 registered voters. Its election monitoring body, the Election Commission of Bhutan (ECB), nevertheless opted for electronic voting in the country's first ever parliamentary election, which was held in 2008. Electronic voting was also used in 2013 and 2018.

The ECB chose to use EVMs supplied by India because they were stand-alone machines with off-grid battery capability and were easy for its many illiterate voters to use.[114] Though the IEC Discussion Document does not clarify this point, the Indian EVMs it bought in 2008 would not have been equipped with VVPAT printers, which were introduced in India only later. It seems unlikely that these EVMs have since been equipped with VVPAT capability. They are thus "black-box" machines, the accuracy of which cannot meaningfully be assessed by voters.

---

[111] IEC Discussion Document, op cit, p. 43.
[112] Ibid.
[113] Ibid.
[114] Ibid, p. 42.

The IEC document acknowledges that Bhutan has experienced "challenges related to costs, training and security", which must "constantly be addressed". However, it fails to explain these further. Instead, it praises the ECB for "having worked to build trust through public education and transparent processes", thereby (supposedly) "ensuring that voters feel confident in the integrity of the electoral system".[115]

6.6 Nepal

The IEC Discussion Document provides little information about Nepal, another mountainous country located in the Himalayas. It has a much bigger population than Bhutan, with 18.1 million registered voters in 2022. Nepal also decided to acquire paperless Indian EVMs, which it piloted in a small way in 2004 and on far larger basis in 2009. According to the IEC document, the 2009 pilot was "not a huge success", because the EVMs "could not handle the large number of candidates who participated in the polls".[116]

This experience, says the IEC, "exemplifies the cost-saving value of conducting a pilot" as this would have helped Nepal realise in time that its EVMs would have to be "capable of handling [its] specific electoral dynamics,…including a large number of candidates". This point seems an obvious one.

On this slender foundation, the IEC Discussion Document goes on to draw a noteworthy – and worrying – conclusion. "In the case of South Africa", it says, "the IEC must therefore carefully consider sharing resources, such as EVMs, with countries in SADC or even BRICS+."[117] What the IEC seems to be proposing is that South Africa's EVMs should travel far and wide in-between the country's own elections – not only to neighbouring states in the SADC region – but also to Egypt, Ethiopia, Iran, Russia and China. How adequate security would be maintained in these circumstances is not explained.

6.7 Fiji

Though Fiji has not yet implemented an electronic voting system, its election monitoring body, the Fiji Elections Office (FEO), is preparing to take this step. According to the IEC Discussion Document, the FEO has opted for MIRU machines manufactured by a company called MIRU Systems in South Korea. These machines, it says, have been used "in national elections in South Korea, Kyrgyz Republic, Ecuador, Russia, the Democratic Republic of Congo [and] Guinea".[118]

Fiji has also been testing these EVMs in trade union, industrial and student elections. According to the IEC Discussion Document, its underlying aim is to build up public trust in the machines through "the outcomes of these pilot programmes and the transparency of the implementation

[115] Ibid, pp. 42 – 43.
[116] Ibid, p. 43.
[117] Ibid.
[118] Ibid, p. 44.

process". The IEC agrees that "non-political trials" of this kind, carried out "before national implementation, can help identify potential issues of concern and build public trust".[119]

7 IEC arguments for introducing electronic voting

In seeking to explain the supposed advantages of electronic voting, the IEC Discussion Document is endlessly repetitive. Since it cannot provide adequate evidence of any of the benefits it claims, it tries to compensate for this by repeating the same (generally unsubstantiated) points under every head.

This approach is particularly evident in the document's description of the *Objectives of Electronic Voting* (in section 7.3). The four key objectives listed are to "increase accessibility", "enhance efficiency", "improve voter turnout" and "ensure security and integrity". That the IEC describes these as "objectives" to be sought, rather than verifiable "gains" to be secured via a switch to e-voting, is itself revealing.

Before examining these objectives further, it is worth recalling that what the IEC is exploring for South Africa is "e-voting" at polling stations, rather than "i-voting" via the Internet. I-voting takes place remotely, with people casting their ballots from their homes or business premises and without having to go to polling stations first. However, i-voting for all voters within a country is still extremely rare and is used only by two countries: Estonia and the United Arab Emirates.[120] I-voting in South Africa is clearly impossible, moreover, as access to broadband is too limited while millions of voters have limited digital experience and literacy.

Under an e-voting system in South Africa, thus, registered voters will still need to go to polling stations to verify their identities and be granted access to that station's EVMs. Under a manual system, waiting times can be reduced by setting up many voting booths within each polling station, as the additional costs in setting up another cardboard booth equipped with a horizontal surface and a pencil for marking ballot papers are minimal. With EVMs, however, the cost of each machine is so high that polling stations may have only one (or only a few) available. This could make for even longer delays at busy polling stations than is currently the case and concentrates risk – the failure of a single machine could put an entire polling station out of action.

7.1 Increasing accessibility

Though this claimed benefit has nothing to do with greater accessibility, the IEC Discussion Document begins by saying that most of the academic experts it interviewed "view e-voting as inevitable and necessary given technological advancements and the modernisation of society". They note that many South Africans "already engage in online activities, like banking" and would be equipped to participate in pilot studies of e-voting. E-voting, these experts add, could "simplify the voting process", provided the system used is not a "complex" one. [121]

---

[119] Ibid.
[120] International Institute for Democracy and Electoral Assistance (International IDEA), 'Use of e-voting around the world': https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world.
[121] IEC Discussion Document, op cit, p. 64.

The academic experts thus cited said nothing about whether e-voting would increase accessibility. Instead, it is the IEC's own officials who have claimed that "electronic voting may be faster, which could enhance accessibility and voter participation".[122] Why e-voting would be significantly faster than marking a ballot paper with a pencil is not explained.

Civil society groups advocating for disabled people told the IEC that e-voting could help blind or partially sighted people who "could rely on their own earphones…in making audio choices in an electronic voting system". However, as these groups acknowledged, considerable voter education would be needed too. Among the general public, 64% said they believed e-voting could help the disabled. However, only 52% thought it might benefit those with lower levels of education and older persons, but failed to explain how this potential benefit could be realised. Against this background, the IEC document states: "[W]hile there is optimism about the potential of e-voting to enhance accessibility for people with disabilities, there are concerns about its effectiveness for other vulnerable groups."[123] This is hardly a ringing endorsement from either civil society or the general public of potential accessibility gains.

The IEC Discussion Document nevertheless concludes: "Overall, e-voting is seen as a means to facilitate openness, accessibility and voter participation in elections. It is also seen an inevitable step towards modernising elections. However, there is some division in opinion on the extent to which e-voting will indeed facilitate increased voter participation and accessibility." The main advantage would accrue to the disabled and would depend on EVMs including "an audio or Braille interface", for instance. [124]

7.2 Enhancing efficiency

Here, the IEC Discussion Document is more balanced. It nevertheless starts with an unsubstantiated claim that "e-voting systems streamline the voting process through a three-phase approach: registration, vote casting, and counting".[125] However, it then fails to examine whether these mooted gains – other than faster counting – have generally been achieved in practice. In addition, it omits to mention that machine counting can always be implemented, following a manual casting of ballots in the long-established way, by ensuring that all ballot papers have bar-codes which can be read by a machine (and later supplemented by a manual count, if needs be).

The IEC document goes on to acknowledge that there are in fact many obstacles to greater efficiency. These "significant barriers to electronic voting," it says, include "technical glitches, inadequate training of IEC personnel, and the country's digital divide". Also important are "frequent power outages and poor internet connectivity", along with low levels of "digital literacy". Security worries and "low public trust" are obstacles too, as are "concerns about the IEC's capacity" to implement an efficient e-voting system. [126]

[122] Ibid.
[123] Ibid, p. 65.
[124] Iibid.
[125] Ibid, p. 66.
[126] Ibid, p. 67.

Similar equivocation is evident in the IEC's summing up of the relevant arguments. It claims that e-voting is regarded as "a promising solution to enhance voter turnout, accessibility and efficiency", but cites no evidence to support this conclusion. It acknowledges "significant challenges such as technical glitches [and] inadequate training" – and ends by querying once again whether the public has sufficient "confidence in the IEC's ability to implement e-voting effectively".[127]

Again, this is hardly a ringing endorsement of e-voting. The IEC document nevertheless recommends "a gradual implementation of e-voting with careful piloting and testing". This approach "allows for identifying and resolving issues before a full-scale rollout" and so "ensuring that the system is reliable, secure and accessible".[128] But a careful pilot programme is unlikely to resolve fundamental technical, security and trust challenges. The implication is that the main purpose of the piloting programme would be to *pretend* that these problems had been overcome and so pave the way for the "full-scale roll-out" the IEC seems determined to implement.

7.3 Improving voter turnout

The material assembled by the IEC Discussion Document under this heading takes up a good three pages – but most of it has little to do with whether e-voting is likely to increase voter turnout. On the contrary, the document acknowledges, relevant data shows that e-voting has little long-term impact on turnout. It may have an initial "novelty effect", which encourages more people to participate at the start. However, says the IEC: "Research shows that an initial boost in voter turnout in the context of e-voting can fade, demonstrating that the long-term impact of e-voting on increased voter turnout may be minimal on aggregate."[129] Even among young voters, as earlier discussed, EVMs are not a sufficient drawcard to overcome voter apathy. They have little impact on voter attitudes as compared to other factors – including increasing doubts about the capacity of democracy to resolve deep-seated societal challenges.

The IEC document then moves on a host of issues irrelevant to likely turnout. These range from the "environmental and cost advantages from the reduced use of paper ballots" to the possibility of "fewer counting errors" and more opportunities for voters "to correct mistakes easily". The importance of voter trust is again highlighted, on the basis that "confidence in the IEC's competence increases support for e-voting, while doubts about its effectiveness and integrity can lead to hesitation". The document finally gets back to the point by noting that "if individuals believe that e-voting will make the voting process simpler, more secure and fairer, they are more likely to participate". Since this "requires support and buy-in from political parties", these "primary stakeholders in the electoral process will need to be consulted on their views of e-voting and how e-voting may impact them".[130]

Having failed to show that e-voting will increase voter turnout, the document goes on to assert that political parties will "need to be brought into the conversation about moving from a paper-

[127] Ibid, p. 68.
[128] Ibid, p. 68.
[129] Ibid, pp. 68 – 69.
[130] Iibid, p. 71.

based voting system to an electronic voting system".[131] In other words, the IEC again assumes that the shift to e-voting must be made, regardless of whether the objectives it lists are likely to be achieved.

7.4 Ensuring security and integrity

Here, the IEC Discussion Document acknowledges that various challenges have to be addressed. These include "maintaining voter privacy, preventing fraud, and securing the technology against cyber threats". The IEC seems to assume that this can be done by means of "advanced technologies, such as cryptography, blockchain and quantum mechanics". Paper audit trails are important too, it says, as they "can help detect errors and reduce voter anxiety, thereby increasing trust in the e-voting process". In addition, audits of "changes to electronic records, including timestamps and lists of modifications," can further enhance security.[132]

The IEC document also cites a suggestion (made by one of its "key informant participants") that public scepticism about the security of e-voting can be addressed by drawing a parallel with online banking. Since "almost everyone uses…and trusts e-banking, why wouldn't you trust e-voting? With e-banking, you risk losing money, but with e-voting, there's no financial loss". This is hardly a compelling analogy – especially as flawed e-voting could have the particularly serious result of facilitating a stolen election, as seems to have occurred in Venezuela in 2024. In addition, banks offering e-banking services have good reason to maintain the security of their systems, whereas a government with direct or indirect control over e-voting may have a strong incentive to skew the count in its favour. Hence, as the IEC Discussion Document correctly comments, a lack of trust "in the government" is also an important obstacle to e-voting.[133]

Having failed to show how security concerns can be overcome, the IEC document once again asserts that a phased approach and pilot testing will "ensure that the system is robust and reliable before being deployed on a larger scale". Again, this assumes that piloting will overcome all security problems. Again, it also assumes that "deployment on a larger scale" is what is needed.[134]

The IEC document also circles back yet again to the vital question of public trust. "Ensuring that the system is not tightly controlled by organisations aligned with specific political parties is essential for its credibility," it correctly comments. It also acknowledges that "confidence and trust in the IEC may be crucial in the adoption and acceptance of an e-voting system".[135] Again, however, its solution is the wrong one. It will not be enough, as the document suggests, for the IEC "to engage in a voter education campaign [and] allow voters to experience the technology firsthand through 'dummy' demonstrations".[136] In addition, the IEC has repeatedly given South Africans reason to doubt both its capacity and its political independence, which has further undermined public trust in it. Unless and until these major problems can be overcome, the IEC

[131] Ibid.
[132] Ibid, pp. 71 – 72.
[133] Ibid, p. 72.
[134] Ibid, p. 73.
[135] Ibid, pp. 73 – 74.
[136] Ibid, p. 74.

will not be trusted to implement e-voting – and increased voter education will not change this reality.

8 Limited public trust in the IEC

8.1 Problems accompanying many elections

8.1.1 The 1994 election

Though the IEC has been much praised for its conduct of the country's first non-racial election in April 1994 election, it failed in fact to ensure a free and fair election. In the run-up to the poll, it should have warned that no free and fair election could be held in the pervasive climate of fear resulting from some 1,500 political killings in the previous four months. It should also have pointed out that no fewer than 13 million people were living in 165 "no-go" zones in different parts of the country, of which more than half were ANC "liberated areas" effectively off-limits to rival parties.[137]

In addition, both the election itself and the subsequent count were so chaotic that no accurate result could be computed. At the ANC's insistence, there was no voters' roll and the inadequate safeguards put in place to stop people from voting more than once soon broke down at many polling stations. Moreover, in areas where the ANC's main black rival, the Inkatha Freedom Party (IFP), had long enjoyed significant support, millions of ballot papers went missing. So too did the IFP stickers that were supposed to be affixed to all the printed ballot papers before these were handed to voters. In practice, these shortages made it impossible for many people to vote for the IFP – or even to vote at all.[138]

The count was also flawed, for the IEC soon scrapped a rule requiring that the number of ballot papers issued to a polling station should be reconciled with the number of votes cast there. This made it impossible to check whether ballot boxes had been stuffed with manufactured votes. It also made it impossible to tell whether all the ballots legitimately cast had found their way back to counting stations. Other irregularities abounded, for many ballot boxes arrived at counting stations open or loosely pegged shut, while some ballots arrived in canvas sacks and not in boxes at all. Soon all the major political parties began to warn that these massive irregularities cast substantial doubt on whether the election could be accepted as free and fair.[139]

As the days ticked by and no election result was declared, a crisis meeting was held between the state president, FW de Klerk, ANC president Nelson Mandela, and IEC chairman Judge Johann Kriegler. Both political leaders began by berating the commission for a botched job, while Kriegler was said to have acknowledged that the elections were "a shambles". The meeting ended as an exercise in damage control. The *Weekly Mail & Guardian* claimed that

---

[137] Jeffery, A, *Countdown to Socialism: The National Democratic Revolution in South Africa Since 1994*, Jonathan Ball Publishers, Cape Town, 2023, p. 12.

[138] Ibid, p. 13.

[139] Ibid; Jeffery, A, *People's War: New Light on the Struggle for South Africa,* Jonathan Ball Publishers, Cape Town, 2019 (updated and abridged), pp. 267 – 268; *Business Day* 2, 6 May, *Sunday Times* 8 May 1994; Johnson, RW 'The Election, the Count, and the Drama in KwaZulu-Natal', in Johnson, RW and Schlemmer, L (eds), *Launching democracy in South Africa: The first open election, April 1994*, Yale University Press, New Haven and London, 1996, p. 291; *The Citizen* 3, 6 May, *Sunday Times* 8 May 1994.

Kriegler was forced to abandon any semblance of proper counting and to start negotiating an acceptable outcome with the different parties. However, Kriegler denied that the election result was based on horse-trading of this kind, saying that the "parties had entered into discussions on irregularities", but the final results were "totally and wholly based on our own count".[140]

In the end, the IEC accorded the ANC 62.6% of the vote, while the National Party was accorded 20.3%, the IFP 10.5%, the Freedom Front 2.2%, the Democratic Party 1.7%, and the Pan-Africanist Congress of Azania 1.2%. The ANC won all nine provinces except the Western Cape (where the NP won 53% of the provincial vote to the ANC's 33%) and KwaZulu-Natal (where the IFP won 51% and the ANC 32%). Kriegler declared that the results, as certified by the IEC, were "beyond review or appeal", while international monitors stated that the election, despite some obvious flaws, had been conducted in "a free and fair manner".[141]

8.1.2 The 1999 to 2019 elections

Though political violence dropped sharply after the ANC's victory in the 1994 election, intimidation increased sharply in the run-up to the 1999 general election. In this period, opinion polling showed a marked rise in the number of black people who said their neighbourhoods were controlled by parties trying to make sure that they voted in a particular way. The proportion of black South Africans expressing this view more than doubled from 18% in 1994 to 38% in 1996.[142] However, the IEC disregarded this too.

There was also intimidation, intolerance, and a degree of political violence in the run-up to the 2004 and the 2009 general elections. In 2009 the Congress of the People (Cope), which had broken away from the ANC after Thabo Mbeki's ouster as ANC and national president, was particularly targeted when it looked as if the new party might pose a major electoral threat to the ANC. Members of Cope were stigmatised by ANC leaders and supporters as "dogs", "cockroaches", and "snakes"'. A number of Cope rallies were disrupted, as were those of the IFP and the Democratic Alliance (DA), the successor to the Democratic Party. DA members were attacked in black towns, while some ANC and IFP office-bearers were killed in KwaZulu-Natal. Again, it was the IFP – which had already witnessed the killing of some 400 of its leaders and office-bearers in the decade before 1994[143] – which bore the brunt of these assassinations.[144]

The 2014 general elections, according to Dave Bruce of the Community Agency for Social Enquiry (CASE), were marred by three forms of "systemic" electoral manipulation for which the ANC was "primarily" responsible. First, many people faced "economic intimidation", for they were threatened with the loss of their social grants if they voted for opposition parties or told that these grants would stop if "a new party came to power". Second, opposition parties often

---

[140] Jeffery, *Countdown to Socialism*, pp. 13 – 14; Jeffery, *People's War* 2019, p. 270 – 271; *The Weekly Mail & Guardian* 6 May 1994.
[141] Jeffery, *Countdown to Socialism*, p. 14; Jeffery, *People's War* 2019, pp. 270 – 272; Report of the Secretary-General on the Question of South Africa to the UN Security Council, 16 June 1994, cited in Johnson, 'How Free? How Fair?', in Johnson and Schlemmer, *Launching democracy in South Africa*, pp 350–351, n13.
[142] Jeffery, A, *Chasing the Rainbow: South Africa's Move from Mandela to Zuma*, IRR, Johannesburg, 2010, p. 29.
[143] Jeffery, *Countdown to Socialism*, p. 81.
[144] Jeffery, *Chasing the Rainbow*, p. 29.

had their meetings disrupted by denying them access to booked venues or by parking vehicles, with loudspeakers blaring, outside meeting halls to drown out discussion. Third, the ANC abused tax revenues to fund its electioneering, which allowed it to outspend its rivals by a factor of four or five.[145]

A similar manipulation of voter concerns was evident before the 2019 general election. In January that year, for instance, an ANC district mayor in Limpopo stated that public employment would be reserved solely for those who voted for the ruling party.[146] According to Wits University political analyst Professor Susan Booysen, such "clientelism" had become so rife that people commonly "took photographs of their votes, so when they went for job applications they could show these as proof of how they had voted".[147]

8.2 The Tlokwe by-election and a defective voters' roll

Though the IEC has long brushed aside any concerns about the freeness and fairness of the country's elections, it proved unable to do so in 2013 – when several municipal by-elections in Tlokwe (Potchefstroom) were set aside as "irregular" by the Constitutional Court in *Kham* v *Electoral Commission of South Africa*. The Court intervened when it became apparent that the IEC had failed to record available voter addresses on the relevant section of the voters' roll, as it had been required to do for some ten years under a 2003 amendment to the Electoral Act of 1998. This omission had allowed about 1,000 people not resident in Tlokwe to be bussed into the area to vote, which had helped the ANC win all the by-elections. The Court found the by-elections "not free or fair" – and ordered that they be held afresh. It also instructed the Commission to record all available voter addresses in the future, so as to ensure that all registered voters were in fact ordinarily resident in their allotted voting districts.[148]

However, it soon became apparent that the IEC's failures went much further than the deficits evident in the Tlokwe section of the voters' roll. Shortly before the fresh by-elections were to be held in February 2016, the applicants in the *Kham* case – all of whom were former ANC members now standing as independent candidates – objected that the IEC had failed to obtain the addresses of more than 4,100 people registered to vote in Tlokwe. In response, the Electoral Court postponed the by-elections and instructed the IEC to include all available addresses on the voters' roll.

The Commission appealed to the Constitutional Court in a case known as *Electoral Commission* v *Mhlope*.[149] Here, the IEC disclosed that, "nationally, the voters' roll was missing more than 12.2

---

[145] David Bruce, 'Just singing and dancing?' Intimidation and the manipulation of voters and the electoral process in the build-up to the 2014 elections', Community Agency for Social Enquiry, April 2014, pp. 3 – 4; Martin Plaut, 'Democracy and violence – the threat to South Africa's elections', *Daily Maverick*, 8 February 2018, pp. 7, 9; iol.co.za, 9 April 2014; www.nelsonmandela.org, Factors affecting participation 2014 elections, p. 2.

[146] *Sunday Times* 20 January 2019.

[147] *Saturday Star* 20 April 2019.;

[148] IEC, 'Results of the municipal by-elections held on 11 December 2013, The African National Congress won all six (6) of the municipal wards contested in Tlokwe [Potchefstroom] Municipality: https://www.elections.org.za/content/About-Us/News/Results-of-the-municipal-by-elections-held-on-11-December-2013/#; *Electoral Commission of South Africa* v *Speaker of the National Assembly*, [2018] ZACC 46 ("the 2018 case), paras. 13, 15; *Kham v Electoral Commission* [2015] ZACC 37 ("the Kham case"), paras. 94 – 95.

[149] *Electoral Commission* v *Mhlope and others*, [2016] ZACC 15 ("the Mhlope case").

million addresses" that it arguably should have added to the roll since the 2003 amendment to the Electoral Act. Since it could not acquire all the missing addresses in advance of the local government election due to be held in 2016, it asked for time until 30 June 2020 to obtain all the necessary addresses.[150]

The majority judgment in the *Mhlope* case was handed down by Chief Justice Mogoeng Mogoeng. He found that the IEC had failed – ever since the December 2003 amendment to the Electoral Act – to "record addresses when new voters were registered or when voters sought to change voting districts". This failure "constituted unlawful conduct" under the Electoral Act. It also meant that "the IEC had compiled a common voters' roll in a manner that was at odds with the strictures not just of the law but also of the rule of law".[151]

Added Judge Mogoeng: "Unlawful conduct in relation to the compilation of the national common voters' roll…amounts to a breach of the rule of law…embedded in our Constitution by section 1(c) as the nerve-centre of our constitutional democracy." The IEC had also acted in conflict with the amended Electoral Act, which was "constitutionally compliant and unchallenged legislation". In doing so the Commission had acted "inconsistently with the constitutional prescript of legality and the rule of law, which was necessarily imported to and rooted in our Constitution in terms of section 1(c)".[152]

The Court also found itself in a difficult situation. The IEC had breached both the Electoral Act and the rule of law. However, it was also clearly impossible for it to obtain the 12.2 million outstanding addresses before the local government election due in August 2016. Hence, this election would either have to be "held on the basis of a defective voters' roll" – or it would have to be postponed, which would "create a constitutional crisis…with far-reaching implications".[153]

The way out of this conundrum was for the Constitutional Court to devise a "just and equitable" remedy, Judge Mogoeng decided. The court thus ordered that the 2016 local government election should proceed on time, "notwithstanding the defects in the national common voters' roll". It also "declared the IEC's failure to record all post-2003 available addresses on the voters' roll inconsistent with its rule of law obligations and thus invalid". However, it suspended this declaration of invalidity until 30 June 2018, so as to give the IEC time to obtain the millions of outstanding addresses. (The Court also ruled, however, that the necessary addresses would have to be added to the relevant section of the national roll before the Tlokwe municipal elections were held.)[154]

In suspending its declaration of invalidity, the Court knew it was condoning illegal conduct on the part of the IEC. However, it felt it had little choice but to accept this. Commented Judge Mogoeng: "[T]his is an exceptional case that cries out for an exceptional solution or remedy to avoid a constitutional crisis which could have grave consequences. It is about the upper

[150] *The 2018 case,* op cit, para. 20.
[151] The *Mhlope case*, op cit, para. 122.
[152] Ibid, para. 124.
[153] Ibid, paras. 131, 132.
[154] *The 2018 case*, op cit, paras. 21 – 23.

guardian of our Constitution responding to its core mandate by preserving the integrity of our constitutional democracy. And that explains the unique or extraordinary remedy we have crafted, of suspending the duty that flows from a constitutionally valid statutory provision."[155]

However, what this also meant is that the IEC – by disregarding its obligations under statute and the rule of law – had effectively held the Constitutional Court to ransom. Since the court was loath to plunge the country into a constitutional crisis by postponing the local government election, its only practical alternative was to allow this election to proceed with a defective voters' roll. The Court tried to limit the damage from this by ordering the Commission to obtain all available addresses from registered voters before allowing them to cast their ballots in the pending local government election. However, since registered voters could not lawfully be barred from voting – and many would not have thought to bring with them any evidence of where they lived – it was unlikely that adequate proof of residence would in fact be provided in many instances.

This was still not the end of the matter. By May 2018, it was clear that the IEC had obtained only some 75% of the available addresses and could not acquire the outstanding ones – a total of some 1.3 million addresses – before the 30 June 2018 deadline the Constitutional Court had set in the *Mhlope* case. The IEC therefore applied to the Court for an order giving it until late November 2019 to obtain the outstanding addresses: by which time national and provincial elections scheduled to take place around May 2019 would already have been held.[156] If this further suspension of the order of invalidity was not granted, the IEC warned, "those dissatisfied with the outcome of the 2019 elections might seek to challenge it by relying on the address shortfall. Even if challenges of this kind ultimately failed, they could imperil the public credibility of the results – and…this should be avoided".[157]

By contrast, added the IEC, the further suspension it was seeking would allow it to keep gathering addresses during the 2019 elections, when people wanting to vote would be motivated to come to polling stations and provide the necessary information. During this election, the Commission stated, it could also "activate its new registration technology which would help with collecting and retaining addresses". The 2019 elections could "then take place smoothly and credibly, without allowing missing address-based challenges". In addition, voter addresses were important only for local government elections, so "the extension would not cause material damage to any person or party".[158]

Independent candidates disagreed that voter addresses mattered little in national and provincial elections. Without addresses, they said, "there was a real risk that identity theft could be used in an orchestrated manner, allowing phantom voters to cast illegal votes". Since this would pose a serious threat to free and fair elections, they proposed a "two-envelope solution". On this basis, registered voters without addresses would be able to vote, but their votes would be placed in a separate envelope. This would allow their votes to be scrutinised if the election outcome was

[155] The *Mhlope* case, op cit, para. 137.
[156] The *2018 case*, op cit, paras. 24 – 32.
[157] Ibid, para. 37.
[158] Ibid, paras. 38, 39.

challenged.[159] Both the DA and the IFP objected too, the DA warning that "a party might win a majority in a particular province by only a handful of votes", in which case "incorrectly registered voters would be highly material".[160]

The IEC rejected these arguments, instead reiterating the need for a further suspension to avoid challenges to the legitimacy of the 2019 election. In response, the Court noted that legitimacy arguments could go two ways. The Commission was trying to forestall any challenge to the legitimacy of the 2019 election by suspending the *Mhlope* declaration of invalidity even further. However, allowing the Commission to proceed with the 2019 elections without the necessary addresses could also undermine the legitimacy of the poll. Said Judge Cameron: "Muzzling address-based voters' roll challenges – even wrong-headed challenges – would not help convince the public that elections are free and fair."[161]

Having weighed the relevant factors, the Constitutional Court agreed to suspend the declaration of invalidity in the *Mhlope* case until 30 November 2019. It also instructed the IEC to mark missing addresses on the voters' roll, require voters with incomplete addresses to supply these before casting their votes, enable political parties to scrutinise the addresses provided, and allow those dissatisfied to seek relief in the Constitutional Court.[162]

Again, the Court might have felt it had little choice but to allow what the IEC sought. Judge Cameron had begun his judgment by stressing the importance of the right to vote and the need to secure this "through rigorously enforced and scrutinised practical arrangements, including addresses". Addresses were important for two reasons, he went on: "First, they enable parties, especially in close contests, to track down individual voters to canvass them. Second, they enable a check on voter fraud by allowing candidates and parties to scrutinise the roll, voter by voter, location by location, to guard against bogus registrations, phantom voters and bussing-in – which is the large-scale transportation into a voting area, for vote-rigging purposes, of voters resident elsewhere".[163] In the end, however, the Court ordered a further suspension and so allowed yet more elections to take place with an admittedly defective voters' roll.

The main significance of the Tlokwe story and its wider ramifications has passed largely unremarked. The key issue is that the IEC failed to comply with the voter address requirement in the Electoral Act from the time the statute was amended in 2003 until after the 2019 national and provincial elections. That is a period of some 17 years. And yet the accuracy and validity of the voters' roll is the "single most important thing that guarantees our democracy", as the portfolio committee on home affairs has emphasised.[164]

[159] Ibid, para. 41.
[160] Ibid, para. 42.
[161] Ibid, para. 55.
[162] Ibid, para. 60.
[163] Ibid, paras. 6, 7.
[164] Parliament on updating voters' roll in line with Constitutional Court ruling, accessed September 9, 2025, https://www.gov.za/news/media-statements/parliament-updating-voters%E2%80%99-roll-line-constitutional-court-ruling-07-feb-2018

8.3 Flaws in Voter Management Devices (VMDs) and IEC data collation

In its 2018 application to the Constitutional Court, the IEC promised to obtain many of the missing voter addresses during the 2019 elections, when many people would be coming to polling stations to cast their ballots. It would be helped in doing so, it added, by "new registration technology" that it would soon introduce. In practice, however, this new technology was not ready in time for the 2019 elections. Instead, the IEC's new "voter management devices" (VMDs) were first used in the 2021 local government election – and then with limited success.

The VMDs introduced by the IEC in 2021 were hand-held, touch-screen electronic devices. They were intended to replace the older "Zip-Zip" machines which had been in use since 1998. The Zip-Zip machines could read the bar-codes attached to paper ID documents and embedded in newer smartcard ID cards, but they could not capture data. Since the VMDs could both capture and upload information via the Internet, their introduction was hailed as a "game-changer" that would facilitate voter registration, help capture all necessary addresses, and prevent double voting by allowing voters to be tracked in real time.[165]

However, various technical and other problems accompanied the roll-out of the VMDs. In the 2021 municipal election, some 67,000 would-be voters were effectively disenfranchised because the VMDs failed to upload their details. This was either because the VMDs had malfunctioned, or because there was no reliable Internet connectivity at polling stations. These VMD defects were supposed to have been resolved by the time of the national and provincial elections in 2024, but in practice hundreds of the devices malfunctioned again. This caused major queues and long delays, with some people having to queue until well after midnight in order to cast their ballots.[166]

Commenting on the elections in a July 2025 report to the home affairs portfolio committee, the IEC said that the long queues experienced at some 800 polling stations (about 3.5% of the 23,300 polling stations established) had been caused by "coding issues" in one of the VMD applications, which had then been resolved.[167] Instead of simply accepting this, however, MPs on the portfolio committee questioned why defects evident in 2021 had not been resolved by 2024. According to the minutes of the meeting, "they expressed concern that similar issues had been raised in the 2021 elections and questioned the efficacy of system testing and the Commission's responsiveness to technical failures. They called for the IEC to ensure offline functionality and robust contingency plans".[168]

During the 2024 elections, there was also a two-hour period during which the electronic results dashboard at the National Results Operation Centre in Pretoria failed to record the voter tallies

---

[165] Maseko, M, 'Could failure of voter management devices jeopardise introduction of e-voting in SA?', News24.com, 8 June 2024: https://www.news24.com/opinions/analysis/analysis-could-failure-of-voter-management-devices-jeopardise-introduction-of-e-voting-in-sa-20240608.

[166] Ibid.

[167] Parliamentary Monitoring Group ("PMG"), '2024 National and Provincial Election Report and related matters: IEC briefing (with Deputy Minister)', Home Affairs Portfolio Committee, 15 July 2025: https://pmg.org.za/committee-meeting/41281/.

[168] Ibid.

coming in from polling stations. According to the IEC, "the glitch was caused by an error during an update". This error had "briefly disrupted the public-facing results dashboard", but there had been no impact on "the underlying data or result processing" in the Commission's "back-end systems". In the words of IEC chair Mosotho Moepya, the dashboard was "merely for display" and was separate from "the secure platform responsible for accurately capturing and recording the will of the voters". The overall system was "not compromised", thus, and "independent recalculation had confirmed the accuracy of captured results".[169]

However, concerns have also been raised at various times about IEC data collation. Opposition parties have complained of small discrepancies between election results, as counted at individual polling stations, and the outcomes then recorded electronically by the central counting station in Pretoria.[170] Though these disparities were generally too small to influence election outcomes, they might perhaps have had an impact in areas where electoral victories were narrow. (In the 2019 provincial election, for example, the ANC won control of Gauteng with 50.7% of the vote.) After the 2024 election, MPs on the home affairs portfolio committee stressed the need for more transparency in the audit process. They also requested more assurance from the IEC on how physical ballots were managed and verified.[171]

8.4 Cadre deployment to the IEC

Various provisions of the Constitution stress the need for the IEC to remain politically independent at all times. Among other things, the IEC is identified in Chapter Nine of the Constitution as one of the "state institutions supporting constitutional democracy". All such institutions are expected, as the Constitution says, to be "independent" and "impartial". They are "subject only to the Constitution and the law and…must exercise their powers and perform their functions without fear, favour or prejudice".[172] In addition, under section 190 of the Constitution, the IEC is responsible for "managing elections" in all three spheres of government (national, provincial and local) and must "ensure that those elections are free and fair".[173]

The Electoral Commission Act of 1996 further underscores the need for the Commission to function independently. Under this statute, the IEC must not only "ensure that any election is free and fair" but also "promote conditions conducive to free and fair elections".[174] The Act also states that the IEC's five commissioners must not, at the time of their appointment, "have a high party-political profile".[175]

All five IEC commissioners are appointed by the president, which could undermine their independence. Two safeguards thus apply. First, the president must act on the recommendation of the National Assembly, for which a 51% majority is needed. Second, the five people appointed

[169] Ibid.
[170] IRR, 'How ready will South Africa be for the 2024 elections?', September 2023: https://irr.org.za/reports/occasional-reports/how-ready-will-south-africa-be-for-the-2024-elections-1-2.pdf.
[171] Centre for Risk Analysis, *2024 Socio-Economic Survey of South Africa*, Institute of Race Relations, Johannesburg, 2025, p. 749; PMG, 2024 National and Provincial Election Report', op cit.
[172] Section 181(1), (2), Constitution of the Republic of South Africa, 1996 ("the Constitution").
[173] Section 190(1)(a), (b), Constitution.
[174] Section 5(1)(b), (c), Electoral Commission Act of 1996
[175] Ibid.

by the president must be drawn from a list of eight candidates nominated by a four-person panel. This panel comprises the Chief Justice of the Constitutional Court, the Public Protector, and one representative each from the Human Rights Commission and the Commission for Gender Equality. All these office holders are enjoined by the Constitution to perform their functions without "fear, favour or prejudice", which should further guarantee their – and the IEC's – independence. In practice, however, all of them, including a majority of the five commissioners, might well be ANC loyalists appointed under an ANC "cadre deployment strategy". This strategy aims to give the ANC hegemony over all "levers of power" in both the state and the broader society.

Cadre deployment by the ANC began as soon as the organisation came to power in 1994 but was given more structure and direction in 1997. In January that year the ANC's anniversary statement said the coming year should be used to "reaffirm the ANC cadre" and "consolidate the National Democratic Revolution" (NDR). The NDR is a Soviet-inspired strategy aimed at taking South Africa, by slow and incremental steps, from a free-market society to a socialist one over a period of some 30 to 40 years. Both the ANC and its allies in the South African Communist Party (SACP) are strongly committed to the NDR – which they have been implementing since 1994 – and see it as offering "the most direct route" to a socialist future.

In December 1997, the ANC's Mahikeng national conference followed up stressing the importance of developing "an army of conscious, committed and properly deployed cadres". It also passed a resolution demanding "maximum political discipline" from all ANC members and re-affirming the importance of "democratic centralism". (Under this principle, derived from Lenin, all ANC members must "defend and implement the decisions of the organisation's highest structures".)[176]

The Mahikeng conference mandated the ANC's national working committee (its highest decision-making structure between meetings of the national conference and national executive committee) to develop a comprehensive deployment strategy. This would be implemented by new "deployment committees" at national, provincial, and local levels. These committees were to oversee the deployment of cadres to various "areas of work on behalf of the movement, including the public service, parastatals, structures of the movement, and the private sector".[177] The committees were also to ensure that deployed cadres remained accountable to the party leadership at all times.[178]

The ANC's aims in this sphere were fully described in its *Cadre Policy and Deployment Strategy*, which was duly adopted in 1998 and published the following year. According to this document, the overarching aim of cadre deployment is to "win hegemony" for the ANC. Towards this end,

[176] Jeffery, *Chasing the Rainbow*, pp. 10 – 11.
[177] Myburgh, J, 'A monster we failed to strangle at birth', *Politicweb.co.za*, 9 November 2021: https://www.politicsweb.co.za/opinion/a-monster-we-failed-to-strangle-at-birth.
[178] Jeffery, *Chasing the Rainbow*, pp. 10 – 11.

as author RW Johnson has written, the ruling party needs "not only the 'correct policies' but also the 'correct people' in all 'key centres of power'".[179]

Many such centres must be targeted, for the aim is to "strengthen political and administrative control" over national and provincial legislatures, metropolitan councils, and public administration at all levels. The document also exhorts the ANC to "strengthen its leadership" in all parastatals and "statutory bodies" as well as in "all other sectors of social activity – including the economy, education, science and technology, sports, recreation, arts and culture, mass popular organisations…and mass communication".[180]

The strategy document emphasises the need for the ANC to maintain strict party control over all its cadres, who must act as they are directed and not "deploy themselves". Rather, the document adds, "a system of supervision and decision-direction…[must be] put in place to ensure that our army of cadres discharges their responsibilities in accordance with decisions which the movement has made". Cadres must also become "organisers who ensure that the policies and programmes of transformation are carried out" in all spheres, even where "there are people who don't share our vision".[181]

In November 1998 the ANC's national working committee established the national deployment committee for which its strategy document called. This committee was headed by Jacob Zuma and dominated by the SACP, as Zuma and all its other members, with two possible exceptions, were past or current members of the Communist party. The ANC also began implementing the pervasive deployments for which the document had called.

In 1998 ANC cadres were deployed to senior positions in the army, the police, and the intelligence services; government departments at national and provincial levels; municipalities under ANC control; important state-owned enterprises (SOEs), including Eskom (electricity) and Transnet (railways and ports), and the National Economic Development and Labour Council (Nedlac).[182]

Before long, ANC loyalists were also deployed to institutions whose independence was expressly guaranteed by the Constitution: the South African Reserve Bank, the National Prosecuting Authority, the auditor general, and the public protector. Though some of the people appointed to these posts showed a commendable level of independence, others compromised their autonomy by rigidly following the party line. In addition, in the words of Dr James Myburgh, editor of Politicsweb.co.za, all these individuals were "part of an ANC leadership which approved a policy of seizing control over all state institutions". They knew that "they had been deployed to give effect to that policy" and that their future careers were "dependent on the further extension

[179] Helen Suzman Foundation's Focus 15, Third Quarter 1999; Johnson, RW, 'A new Broederbond, only more ambitious', *Politicsweb.co.za*, 7 July 2022: https://www.politicsweb.co.za/opinion/a-new-broederbond-only-more-ambitious; see also Joel Netshitenzhe, 'The National Democratic Revolution – Is it still on track', *Umrabulo*, 4th Quarter, 1996, pp. 4 – 6.
[180] Helen Suzman Foundation's Focus 15, Third Quarter 1999; Johnson, 'A new Broederbond': https://www.politicsweb.co.za/opinion/a-new-broederbond-only-more-ambitious.
[181] Ibid.
[182] Jeffery, *Chasing the Rainbow*, p. 12

and consolidation of ANC power".[183]

Deployment committees, including the national one, worked in secret. No record of their decisions was made public until 2022, when the Zondo commission inadvertently[184] released the minutes of various meetings of the national deployment committee, held between 2018 and 2020. These minutes were a fraction of those presumably drawn up over more than two decades (though President Cyril Ramaphosa claims that no minutes were kept between 2012 and 2017, when he chaired the national deployment committee as the ANC's deputy president).[185]

According to Dr Leon Schreiber, then DA shadow minister for public service and administration, the minutes of a mere three meetings held by the national committee in 2018 give some idea of the scale of the deployments made. They show that the committee had "reserved positions for 'ANC cadres' and 'firm supporters of the ANC' on the boards of SANParks, the Small Enterprise Development Agency (SEDA), Transnet, Denel, SAA, the South African Forestry Company (Safcol), the Airports Company of South Africa (Acsa), Sanral, and the National Advisory Committee on Innovation".[186]

By Schreiber's calculation, the minutes of various other meetings show that "dozens of directors general and deputy directors general of state departments, and 50-plus appointees on state boards, funds, regulators, commissions, agencies and even the Government Printing Works, were not only nominated by the ANC committee but appointed to office afterward".[187] The minutes further indicate that the committee "pre-selected" five judges: two for appointment to the Constitutional Court, one for the Supreme Court of Appeal, one for the Northern Cape high court, and one for the Labour Court.[188] This suggested that Mr Ramaphosa had lied to the Zondo commission of inquiry into state capture in testifying that judicial appointments lay beyond the remit of the deployment committee.[189]

Mr Ramaphosa had claimed in his testimony to Judge Zondo that the national deployment committee made no final decisions at all. It merely made non-binding recommendations regarding certain senior appointments – primarily in the public service and SOEs – while leaving

---

[183] Ibid.
[184] The minutes were posted on the commission's website as part of a bundle of documents relating to Ramaphosa's testimony, Davis, R, 'How President Ramaphosa and ANC leaders misled South Africa about the party's cadre deployment committee', *Daily Maverick*, 15 January 2022: https://www.dailymaverick.co.za/article/2022-01-15-how-president-ramaphosa-and-anc-leaders-misled-south-africa-about-the-partys-cadre-deployment-committee/.
[185] Davis, 'How President Ramaphosa', ibid: https://www.dailymaverick.co.za/article/2022-01-15-how-president-ramaphosa-and-anc-leaders-misled-south-africa-about-the-partys-cadre-deployment-committee/.
[186] Statement issued by Dr Leon Schreiber MP - DA Shadow Minister for Public Service and Administration, 7 January 2022:https://www.dailymaverick.co.za/article/2022-01-15-how-president-ramaphosa-and-anc-leaders-misled-south-africa-about-the-partys-cadre-deployment-committee/.
[187] Leon, T, 'As cadre deployment took root, civil society failed to see the writing on the wall', *Business Day*, 16 January 2022: https://www.businesslive.co.za/bd/opinion/columnists/2022-01-16-tony-leon-as-cadre-deployment-took-root-civil-society-failed-to-see-writing-on-wall/.
[188] Schreiber, L, 'DA wins battle to make cadre deployment records public', DA newsroom, 4 January 2022: https://www.da.org.za/2022/01/da-wins-battle-to-make-anc-cadre-deployment-records-public.
[189] Davis, 'How President Ramaphosa', op cit: https://www.dailymaverick.co.za/article/2022-01-15-how-president-ramaphosa-and-anc-leaders-misled-south-africa-about-the-partys-cadre-deployment-committee/.

it to the relevant institutions to accept or reject the proposals made.[190] However, the minutes released by the commission show the opposite. They indicate that it is the deployment committee that generally decides, with the relevant appointing authorities largely confined to rubber-stamping what the committee wants. Ministers sometimes go so far as to "reserve" posts for the deployment committee to fill at its discretion.[191] In other instances, ministers are barred from proceeding with proposed appointments unless the deployment committee has given its approval.

Cadre deployment to public administration is *prima facie* in breach of the Constitution, which states that "no employee of the public service may be favoured or prejudiced only because that person supports a particular political party or cause".[192] The strategy also clashes with the Constitution in a host of other spheres.

Parliament is supposed to reject unconstitutional bills, for example, but the ANC MPs deployed to the legislature are answerable to the ANC's senior leaders and are expected to do their bidding, rather than honour their oaths to uphold the Constitution. The National Prosecuting Authority is supposed to "exercise its functions without fear, favour, or prejudice" but its deployed cadres have generally been loath to prosecute ANC leaders implicated in crimes ranging from corruption to political assassination. The Constitution requires state procurement to be "transparent, competitive and cost-effective",[193] but in practice cadres at all three spheres of government have often been awarded tenders at inflated prices, thereby enriching themselves and boosting the ANC's patronage powers.

Cadre deployment is the reason for these clashes, writes Dr Myburgh, for it has "created a 'dual authority' with 'ostensible authority' lying in the Constitution and Parliament and 'real authority' [lying] in the party".[194] These dual lines of authority help explain why ANC cadres in supposedly independent institutions find it difficult to "perform their duties without 'fear or favour' and 'subject only to the Constitution and the law'" when this obligation is "overridden by the 'maximum political discipline' demanded by the party leadership".[195]

This "dual authority" lies at the heart of cadre deployment and is vital in advancing the NDR. It explains the ANC's determination to retain the strategy, even though the Zondo commission found that "it is unlawful and unconstitutional for a President of this country and any Minister, Deputy Minister or Director-General or other government official, including those in parastatals, to take into account recommendations of the ANC Deployment Committee…or any political

[190] Ibid.
[191] Statement issued by Dr Leon Schreiber MP - DA Shadow Minister for Public Service and Administration, 7 January 2022.
[192] Section 197, Constitution.
[193] Sections 195, 2, 179, 217, Constitution.
[194] Myburgh,"A monster we failed to strangle": https://www.politicsweb.co.za/opinion/a-monster-we-failed-to-strangle-at-birth
[195] Ibid.

party in deciding who should be appointed to a position in the public service or in organs of state or parastatals."[196]

The Zondo commission also found that cadre deployment is inconsistent with five clauses in the Constitution. It identified these clauses as Section 195(1)(b), which requires "a high standard of professional ethics to be promoted and maintained" in public administration; Section 195(1)(d), which mandates that public administration be "development-oriented", Section 195(1)(f), which states that public administration must be "accountable"; Section 195(1)(h), which calls for "transparency" in public administration; and Section 197(3), which states that "no employee of the public service may be favored or prejudiced because that person supports a particular political party or cause".[197] The Commission's report also indicated that cadre deployment – by prioritising party loyalty over other considerations – contravened fundamental constitutional requirements and was "a significant enabler of state capture".[198]

However, Judge Zondo's strictures against cadre deployment have since been weakened by a poorly reasoned judgment of the Pretoria high court in February 2024. Here, the DA had cited the Zondo report and other evidence in requesting the court to strike down the ANC's cadre deployment strategy, as it applies to the public administration. However, the Pretoria high court found the DA had failed to prove its case and dismissed it with costs.

The court echoed the ANC's perspective in describing the cadre deployment strategy as "a contract" between the ANC and its members in which the DA, as an outsider, had little standing to intervene. It also described the strategy as "a political party policy" which any court should be reluctant to pronounce upon. In addition, it dismissed the DA's accusation that cadre deployment was unconstitutional, saying "the DA had failed to point to any clause of the policy which offended the Constitution".[199]

According to the court, the Zondo report, when properly read, had made no finding on the constitutionality of the strategy. On the contrary, the commission had merely said it "*would be unlawful*" for public officials to take into account the "*recommendations*" of *any* political party when making decisions on who should be employed in the public service. In addition, though President Ramaphosa had admitted to Judge Zondo that the policy had been abused on occasion, such abuses did not suffice to show unconstitutionality. Moreover, the DA wanted the court to take judicial notice of what the Zondo commission had said about cadre deployment, but it had failed to meet the relevant requirements. The doctrine of judicial notice

[196] Judicial Commission of Inquiry into State Capture Report: Part VI, Vol 2, 'State capture established, President Ramaphosa's Evidence and the Role of the ANC and Parliamentary Oversight', ("the Zondo Report"), Part 6, Vol 2, para 657: https://www.gov.za/sites/default/files/gcis_document/202206/electronic-state-capture-commission-report-part-vi-vol-ii.pdf.

[197] Zondo report, ibid.

[198] Ibid.

[199] *Democratic Alliance* v *African National Congress and others* [2024] ZAGPPHC 154, paras. 10, 12, 13, 16: https://www.politicsweb.co.za/documents/cadre-deployment-the-high-court-judgment.

allowed for "the admission into evidence of notorious and well-established facts" – and this test was not fulfilled.[200]

The DA, the court went on, had also sought to rely on some of the leaked minutes of the Deployment Committee (as earlier described) to show that the committee did more than merely recommend. But the ANC had denied this, saying the committee "did not dictate to government who should be employed". The court could not dismiss "the ANC's version off-hand as palpably implausible", especially as the DA had failed to place any admissible evidence before it. "The correct approach was to bring to court a specific challenge against a specific appointment, with evidence of unlawful interference by the [Deployment] Committee". But this the DA had not done.[201] The court concluded that "the ANC, like any other political party, is entitled to influence government decisions, including the appointment of senior staff to public administration, as long as the bright line between state and party is observed".[202] How well that "bright line" had in fact been maintained the court seemed reluctant to probe.

The DA sought leave to appeal against this ruling to the Supreme Court of Appeal, but the Pretoria high court ruled against it. (This obliges the DA to seek leave from the appeal court itself if it wants to proceed.) Handing down its decision in April 2025, the Pretoria high court stressed that an appeal is allowed only where there is "a reasonable prospect" of success or "some other compelling reason" why the appeal should be heard. Compelling reasons include "conflicting judgments on the matter under consideration", along with "important questions of law…[and] discreet issues of public importance".[203]

Given the salience of the Zondo findings on cadre deployment – and the likely contribution of the strategy to state capture, corruption and dysfunction in governance – "compelling reasons" were surely evident. But the Pretoria high court dismissed the DA's application on the basis that there was "simply no prospect that another court would come to a different conclusion". Here, the court reiterated that the DA had "fail[ed] to plead a valid constitutional attack", which had made it difficult for the ANC even to be "aware of the case they had to answer". By contrast, the court made no attempt to assess to what extent the Zondo report might be seen as "a conflicting judgment" on the same issues. Nor did it examine the "public importance" of cadre deployment or the various "questions of law" which it raises.[204]

The implications of cadre deployment for the independence of the IEC are profound. Gwede Mantashe, minister of mineral and petroleum resources and a former ANC secretary general, told the Zondo commission: "The strategic deployment of comrades is an important part of the ANC's strategy to control the levers of power in the state."[205] In addition, the strategy expressly

[200] *Democratic Alliance* v *African National Congress and others* [2024] ZAGPPHC 154, paras. 21 – 26, emphasis supplied by the IRR.
[201] Ibid, paras. 32 – 36.
[202] Ibid, para. 40.
[203] *Democratic Alliance* v *African National Congress and others*, [2025] ZAGPPHC 11 April 2025, paras. 3, 4, 17, 15: https://www.saflii.org/za/cases/ZAGPPHC/2025/374.html.
[204] Democratic Alliance v African National Congress and others, [2025] ZAGPPHC 11 April 2025, paras. 3, 4, 17, 15: https://www.saflii.org/za/cases/ZAGPPHC/2025/374.html
[205] Zondo report, op cit, para. 581.

extends to "independent statutory committees", such as the IEC.[206] Moreover, the IEC's control over the voters roll, the conduct of elections and the counting of ballots makes it arguably by far the most important of all the Chapter Nine institutions in sustaining ANC legitimacy and ANC rule. At the same time, IEC commissioners are also supposed to be politically non-partisan – which gives both the ANC and IEC incentives to downplay or conceal any links between the two.

8.5 Public trust in the IEC

Opinion polling by the Institute for Justice and Reconciliation (IJR) and Afrobarometer, two civil society organisations, show a major decline in public trust in the IEC since 2011. In a report published in November 2024, the IJR said that trust in the Commission had been "relatively stable" until 2011 but had sharply diminished since then. This decline, it said, was linked to "growing concerns about the transparency and fairness of elections, as well as the perceived ineffectiveness of electoral reforms".[207]

In 2011 to 2013, added the IJR, 9% of respondents had trusted the IEC "not at all", while 18.5% had trusted it "just a little". By contrast, in 2021 to 2023, the proportion trusting the IEC "not at all" had risen to 39%, and that trusting it "just a little" to 25%. Hence, in the 2021 to 2023 period, a combined 64% – or almost two-thirds of respondents – had little or no trust in the Commission. By contrast, the proportions trusting the IEC "somewhat" had declined from 37% in the earlier period (2011 to 2013) to 20% in the later one (2021 to 2023). At the same time, the proportions trusting the IEC "a lot" had dropped from 32% in the earlier period to 8% in the later one. In the 2021 to 2023 period, thus, only 28% (less than a third) had any trust in the Commission at all, down from a total of 69% in the earlier period.[208] That a mere 8% trusted it "a lot" was particularly telling.

Opinion polling by Afrobarometer, whose polling team is led by the IJR, paints a similar picture on the degree of public trust in the IEC. In June 2023, Afrobarometer reported on various other electoral issues too. Its most recent polling (carried out in November and December 2022) showed that almost all respondents (92%) thought that elections worked "not very well" (28%) or "not at all" (64%) in "ensuring that voters can remove from office leaders who did not do what the people want". Surprisingly, however, a similar proportion (also 92% in total) thought that elections worked "fairly well" (31%) or "very well" (61%) in ensuring that "members of Parliament reflect the views of voters". In addition, just less than half (49% in total) thought the 2019 election had either been "completely free and fair" (29%) or "free and fair with minor problems" (20%). A significant percentage (14%) either did not know or could not understand the question.[209]

---

[206] Ibid, para. 593.
[207] Govindasamy, P, 'Citizens' perceptions of trust and corruption in government institutions in South Africa', Institute for Justice and Reconciliation, IJR Policy Brief, No 46, November 2024, pp. 1 – 2: https://www.ijr.org.za/home/wp-content/uploads/2024/11/800985_A_IJR-PB-Trust-and-Corruption-02.pdf.
[208] Ibid, p. 2.
[209] Afrobarometer, 'South Africans support elections but doubt their efficacy, have little trust in Electoral Commission', News Release, Durban, 13 June 2023, pp. 2 – 3: https://www.afrobarometer.org/wp-content/uploads/2023/06/News_release-South-Africans-support-elections-but-distrust-Electoral-Commission-Afrobarometer-13jun23-1.pdf.

In addition, as Afrobarometer notes, "fewer than half (47%) expressed confidence in ballot secrecy, saying it was "not very likely" (17%) or "not at all likely" (30%) that powerful people could find out how they voted. But almost as many (43%) considered it "somewhat likely" (21%) or "very likely" (22%) that their ballots were not secret.[210] These latter findings are worrying.

Already, thus, there is considerable public distrust of the IEC. Yet, as the Commission has stressed, the success of electronic voting depends in considerable measure on public confidence in the institutions responsible for conducting e-elections. In South Africa, that public confidence is almost entirely lacking. This will deepen public resistance to the proposed new system. Many people will question why a familiar manual voting system which most voters find easy to understand is now to be replaced by an opaque electronic one that most cannot comprehend. Public fears that votes will no longer be secret are likely to increase. So too will concerns that the new system will expand the IEC's control over two crucial steps – the casting of ballots and the counting of votes – and this at a time when the ANC has become highly vulnerable to further election losses. That a mere 8% of voters currently trust the Commission "a lot" will make the changes harder still to accept.

9 The constitutionality of electronic voting in South Africa

Various provisions of the Constitution are relevant in assessing the consistency of electronic voting with the constitutional text. Among other things, section 190 obliges the IEC to "ensure that elections [for national, provincial and municipal legislative bodies] are free and fair". Under Section 19 of the Bill of Rights, dealing with "Political rights", everyone is "free to make political choices", while "every citizen has the right to free, fair and regular elections for any legislative body". In addition, "every adult citizen has the right (a) to vote in elections for any [such] legislative body…and to do so in secret". At the same time, section 7(2) requires the state to "respect, protect, promote and fulfil the rights in the Bill of Rights". Moreover, any court or tribunal, in interpreting the Bill of Rights under section 39, must not only "promote the values that underlie an open and democratic society based on human dignity, equality and freedom" but also "promote the spirit, purport and objects of the Bill of Rights". [211]

Various founding provisions of the Constitution are relevant too. According to section 1, the Republic of South Africa is founded on the values of "universal adult suffrage, a national common voters' roll, regular elections and a multi-party system of democratic government, to ensure accountability, responsiveness and openness". Section 2 identifies the Constitution as "the supreme law of the Republic", adding that "law or conduct inconsistent with it is invalid and the obligations imposed by it must be fulfilled". In addition, under Section 3, "all citizens are equally entitled to the rights, privileges and benefits of citizenship", as well as to its "duties and responsibilities".[212]

[210] Afrobarometer, ibid, p. 1.
[211] Sections 190(1)(b), 19(1) to (3), 7(2), 39(10(a), (2),1996 Constitution.
[212] Sections 1(d), 2, 3(2), 1996 Constitution.

Under Section 42(3), "the National Assembly is elected to represent the people and to ensure government by the people under the Constitution". Similar provisions apply to provincial legislatures, which must "ensure that provincial interests are taken into account in the national sphere of government". At the same time, municipalities must "provide democratic and accountable government for local communities".[213]

These provisions underscore the importance of democratic, accountable and representative government in South Africa. They expressly give all citizens the right to "free and fair elections", while simultaneously imposing on the IEC an obligation to manage all elections in all spheres of government in a manner that "ensures free and fair elections". The Electoral Commission Act of 1996 further reinforces the constitutional obligations thus resting on the IEC, as does the Electoral Act of 1998.

Section 5 of the Electoral Commission Act requires the IEC to "manage" elections, "ensure that any election is free and fair" and "promote conditions conducive to free and fair elections". According to the statute, the IEC must also "promote knowledge of sound and democratic electoral processes" and "compile and maintain voters' rolls".[214] Against this background, the Electoral Act of 1998 provides a more detailed legal framework for the conduct of elections in all three spheres of government. It sets out the rules and procedures that the IEC must follow to ensure an election is free and fair. It also provides for the management of the voters' roll and includes (in Schedule 2) an electoral code of conduct that obliges all political parties and individuals contesting an election to promote political tolerance and to foster free campaigning and open political debate.[215]

The IEC Discussion Document notes that "South African electoral law currently mandates [or requires] the use of paper ballots" and also of "manual counting". This is set out in the Electoral Act of 1998, as well as in the Local Government: Municipal Electoral Act of 2000. As the IEC document acknowledges, the current wording in both statutes "leaves no possibility for legal e-voting". Hence, "legislative changes would…be required before the IEC could begin to experiment with, trial and pilot e-voting systems in elections". This, as earlier noted, explains why the IEC tried to smuggle into the Electoral Amendment Act of 2020 clauses that would have allowed the Commission to "prescribe a different voting method", regardless of "anything to the contrary contained" in the principal statute or "in any other law".[216]

The IEC Discussion Document goes on to claim that "Section 19 'Political Rights' in the Bill of Rights in the South African Constitution 1996 is broadly phrased and contains no language that might preclude electronic voting". In its view, it is only sub-section 19 (2) which is "pertinent here" and this states: "Every citizen has the right to free, fair and regular elections for any legislative body established in terms of the Constitution."[217]

---

[213] Sections 42(3), (4), 109, 152(1)(a), 1996 Constitution.
[214] Section 5, Electoral Commission Act of 1996.
[215] Joosub, I, 'Ensuring Free and Fair Elections in South Africa: A critical analysis', FW de Klerk Foundation, 8 July 2024: https://fwdeklerk.org/ensuring-free-and-fair-elections-in-south-africa-a-critical-analysis/.
[216] IEC Discussion Document, pp. 52, 54.
[217] Ibid, p. 54.

This assertion disregards many other constitutional guarantees, as earlier set out. It also brushes over the vital points raised by the Federal Constitutional Court in Germany in 2009 in its ruling on the constitutionality of electronic voting. These points go to the heart of what is needed for representative democracy and the right to free and fair elections. This is so not only in Germany but also in South Africa, which has similar constitutional provisions in key respects.

This judgment has already been described at some length (see *Section 5.4* above), but its core points merit repeating here. Said the court:[218]

- "in a representative democracy", the election of the people's representatives "constitute[s] the fundamental act of legitimisation";
- election monitoring is vital to "ensure that the delegation of state power to the people's representati[ves]…does not suffer from a shortcoming";
- "each citizen must be able to comprehend and verify the central steps in the elections reliably and without any special prior technical knowledge";
- in manual voting systems, "manipulations or election falsifications…are only possible with considerable effort and with a very high risk of discovery, which has a preventive impact";
- by contrast, electronic machines have an "amenability to error" which is "difficult to recognise" and are susceptible "to manipulation" that can have a major impact with "relatively little effort";
- the functioning of electronic machines "cannot be examined from outside or by persons without special computer knowledge";
- yet "the voter may not be required to trust solely in the technical integrity of the system" or to "rely on its functionality…without the possibility of personal inspection"; so
- electronic voting machines must be able to "print out a visible paper report of each vote cast" which can be checked by the voter and is then "collected to facilitate subsequent checking".

In other words, electronic voting cannot adequately ensure representative democracy, the freedom to make political choices, the right to vote in secret in free and fair elections, and the equal and universal franchise rights of all citizens *unless* the electronic machines incorporate a fully comprehensive paper audit trail. This must be provided via a VVPAT system which prints out every ballot cast and allows every voter physically to inspect this paper record so as to ensure that his or her vote has been accurately captured on the printed document. All these printed voting records must then be placed in sealed ballot boxes so that they can all be counted manually should the need arise.

This comprehensive paper audit trail is essential to address the problems with electronic voting that the German court so aptly summarises. However, once this vital paper trail has been produced, questions must arise as to why extremely costly electronic voting machines are needed too. In other words, the introduction of an electronic voting system – if it is to be done in

[218] Federal Constitutional Court, Judgment of the Second Senate of 3 March 2009, paras. 109 – 213, 120 – 124.

a way that complies with guaranteed rights and democratic values – must involve an expensive duplication of election processes. The potential errors and/or deliberate manipulations to which electronic machines are vulnerable must be counter-balanced by paper records that can be checked by voters. Manual counting is also needed, as this alone is open to scrutiny by voters without specialist technological expertise.

This costly duplication helps explain why only 34 countries out of the 174 states included in the database of the International Institute for Democracy and Electoral Assistance (International IDEA) – 19% of the total – use electronic voting. In addition, as International IDEA points out: "In 11 countries (6%), e-voting has been abandoned and one of the main reasons is the concern about trust and security of the vote."[219]

10 The vital need for an objective cost/benefit analysis

The IEC's Discussion Document acknowledges that the Commission's attempt to introduce electronic voting via the Electoral Amendment Act of 2020 was roundly rejected by citizens, other stakeholders and many Members of Parliament. It also notes that there were widespread concerns at that time about "the potential risks and costs of electronic voting". To address these concerns, the document goes on, "a detailed cost-benefit analysis study must be implemented". This study, it adds, could be "conducted by a team constituted under the auspices of the Department of Home Affairs in conjunction with the IEC".[220]

A cost-benefit analysis is indeed required. However, it must also be an expert, comprehensive and objective study if it is to have any value. If it is as simplistic – and as biased in favour of e-voting as the IEC's Discussion Document – then it will serve no purpose other than to obscure the true costs and consequences of electronic voting. What is needed, thus, is for the government's policies on socio-economic impact assessments and evidence-based rule-making to be implemented in full instead of being largely ignored, as the IEC has so far done.

10.1 Guidelines for the Socio-Economic Impact Assessment System

According to the government's *Guidelines for the Socio-Economic Impact Assessment System (SEIAS)* – which were developed by the Department of Planning, Monitoring, and Evaluation in May 2015 and took effect in September that year – the SEIA system seeks to ensure that "the full costs of regulations and especially the impact on the economy" are fully understood before new rules are introduced.[221]

As the Guidelines state, the SEIA system must be applied at various stages in the policy process. Once new legislation has been proposed, such as legislation replacing the manual voting system, "an initial assessment" must be conducted to identify different "options for addressing the problem" and making "a rough evaluation" of their respective costs and

---

[219] International Institute for Democracy and Electoral Assistance (International IDEA), 'Use of E-Voting Around the World', 6 February 2023: https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world.
[220] IEC Discussion Document, p. 54.
[221] Department of Planning, Monitoring and Evaluation, 'Socio-Economic Impact Assessment System (SEIAS), Revised Impact Assessment: National Health Insurance Bill', 26 June 2019 (2019 SEIAS Assessment); *SEIAS Guidelines*, p. 3, May 2015.

benefits. Thereafter, "appropriate consultation" is needed, along with "a continual review of the impact assessment as the proposals evolve".[222]

A "final impact assessment" must then be developed that "provides a detailed evaluation of the likely effects of the [proposed law] in terms of implementation and compliance costs as well as the anticipated outcome". When a bill is published "for public comment and consultation with stakeholders", this final assessment must be attached to it.[223]

Unfortunately, however, the government often disregards its own SEIA system in developing new legislation. This is what happened in 2020, when the Electoral Laws Amendment Bill was put before Parliament without a SEIA report or adequate consultation. Worse still, this Bill sought to empower the IEC to bypass Parliament, ignore conflicting laws, and introduce e-voting by regulation – none of which was disclosed to the public, as a proper SEIA report should have done.

10.2 National Policy Development Framework of 2020

The Electoral Laws Amendment Bill was put before Parliament before the government had developed its *National Policy Development Framework* ("the Framework"). This was approved by the Cabinet in December 2020 to help give effect to the *National Development Plan: Vision 2030*.

The Framework echoes the SEIA Guidelines in stressing the need to "encourage the public…to participate in policy making".[224] It also lists some of the key requirements for proper public participation. "Consultation with stakeholders should commence as early as possible," it says. All relevant stakeholders should be identified, including "those who will benefit when [existing] problems are addressed" and "those who will bear the cost of implementation of the proposed intervention".[225]

Policy-makers must also identify and counter all "barriers to active participation" and ensure that "consultation is infused in all aspects of the policy-making cycle". They must consider different policy options and give adequate thought to "which policy solutions would best achieve the public policy objective". They must "inform and engage stakeholders" on "the nature and magnitude of a policy issue", along with its likely "impacts and risks".[226]

The Framework also seeks to improve policy development by "inculcating a culture of evidence-based policy making".[227] All assessments made by policy-makers must be "informed by the best available evidence, data, and knowledge".[228] In addition, policy-makers must be willing to adjust their proposals in the light of the evidence provided. As the Framework stresses, "*policy-makers must not impose their preconceived ideas…and pre-empt the*

[222] *SEIAS Guidelines* p. 7.
[223] *SEIAS Guidelines*, p. 11.
[224] Ibid, p. 19.
[225] Ibid, pp. 19 – 20.
[226] Ibid, pp. 19 – 20.
[227] National Policy Development Framework, 2020, p. 3.
[228] Ibid, p. 20.

outcome of the policy consultation process."[229] This in turn means that "policy-makers need to be willing to be persuaded and acknowledge the input of stakeholders with a view to creating a win-win policy outcome". They must avoid any impression that "the consultation process is staged, managed, cosmetic, token and a mere compliance issue". Instead, they must "strive to produce an outcome based on bargaining, negotiation, and compromise".[230]

Now that the Framework is in place, any cost/benefit analysis of electronic voting must comply in full with what it says on public participation and evidence-based decision-making. Instead of simplistically asserting, as the IEC Discussion Document does, that "e-voting is seen as inevitable and necessary due to technological advancements and societal modernisation",[231] any proper analysis must take full account of all the evidence *against* making this shift.

As various analysts have pointed out, a constitutionally compliant electronic voting system with a comprehensive paper audit trail is not necessarily faster than manual voting. The initial electronic tally may be swift, but when a VVPAT system is introduced, the process becomes a hybrid one in which a substantial percentage of the paper ballots must also be manually counted. Where trust in the election management body is as low as is the current level of trust in the IEC (only 8% of voters trust it "a lot"), then a full manual recount is often needed. This hybrid system is likely to just as time-consuming as a purely manual system – if not even more so. It may in fact extend the period required to declare a result that has an acceptable level of legitimacy as legal challenges and manual audits take considerable time to complete.[232]

The argument that electronic voting machines save money in the end – despite their initial high costs – is also unconvincing. Upfront costs are heavy, especially when VVPAT printers and associated hardware must also be acquired. In addition, these machines – which may have to remain in use for 20 to 30 years to help cover purchase and set up costs – must always be securely stored and properly maintained by technical experts. This generally requires software updates and hardware repairs as well as often complex diagnostics. As machines age, moreover, vulnerabilities are likely to emerge that are difficult to counter.[233]

At election times, the machines must be transported to polling stations across the country, tested for glitches on their arrival, effectively cleared of all electronic ballots previously cast, and protected against unauthorised access, both physical and electronic. Properly preparing the machines to receive and accurately tally electronic ballots is thus a complex and costly exercise in itself. The VVPAT system must also be properly prepared and implemented, which

[229] Ibid, emphasis supplied by the IRR.
[230] Ibid.
[231] IEC Discussion document, pp. 86.
[232] Duigan, An introduction to vulnerabilities in electronic voting, op cit; Gemini AI,"E-Voting versus Paper Ballot", Thakur, C., 25 April 2024, Durban University of Technology, Available from: https://www.dut.ac.za/e-voting-versus-paper-ballot/#:~:text=The%20key%20challenges%2C%20however%2C%20are,elevates%20suspicion%20of%20electoral%20interference..
[233] Duigan, op cit; Gemini AI, Verified Voting, "The price of voting: Today's Voting Machine Marketplace", March 2021, Available from: The Price of Voting: Today's Voting Machine Marketplace – Verified Voting (pp. 32-41 and 45-50).

involves considerable costs on paper, ink, logistics and personnel.[234] What is needed, in effect, the simultaneous deployment of both an electronic and a manual system – which means that many election costs are duplicated.[235]

11 The way forward

The IEC Discussion Document claims that "there would appear to be consensus that South Africa is ready for a form of electronic voting, supported by sufficient technological infrastructure. E-voting is seen as inevitable and necessary due to technological advancements and societal modernisation. It has the potential to enhance accessibility, voter participation and efficiency, particularly for persons with disabilities".[236]

None of these claims is true. In making them, the IEC confirms its prejudgement of the issues and its persistent bias in favour of electronic voting. That bias pervades the IEC Discussion Document. Instead of providing an honest and evidence-based assessment of e-voting, the document brushes aside the many problems with electronic voting in international experience. It repeatedly omits important information and analysis. It continually makes assumptions and assertions that it cannot substantiate. Despite the many pages it devotes to this exercise, it fails to marshal any convincing arguments for a shift to electronic voting. Yet it nevertheless claims that the case for the shift is so compelling that its implementation should now begin.

In addition, the IEC declines to acknowledge that an electronic voting system cannot meet the constitutional demand for "free and fair elections" unless it is fully backed up by printed receipts of all votes cast and a manual counting system for tallying these. Yet a hybrid system of the kind required would be enormously expensive. It would also fail to provide any advance on the manual system that South Africa already has. At the same time, the heavy costs involved in introducing and implementing this hybrid system would place a substantial and unnecessary burden on the fiscus at a time when the government needs to cut back on public spending to avoid a looming debt trap.

The simple truth is that manual voting systems have many advantages over electronic ones, as Mr Duigan has said. To cite him once again, "for the classic secret ballot to function [in a manual system], there need only be a secret booth, a sealed box, a legible ballot, and an impartial system of oversight for counting. For an electronic system, similar concepts apply (albeit in a virtual sense), but at each stage, the 'parts' of the system are far greater in quantity, and the failure of any one part can compromise the validity of a ballot, or even an entire election."[237]

---

[234] "Election Security Spotlight – Chain of Custody is crucial for Election Offices", n.d., Centre for Internet Security, Available from: https://www.cisecurity.org/insights/spotlight/election-security-spotlight-chain-of-custody-is-crucial-for-election-offices.

[235] Gemini analysis, Castro, D., "Stop the Presses: How Paper Trails Fail to Secure e-Voting", September 2007, Available from: Stop the Presses: How Paper Trails Fail to Secure e-Voting. (p

[236] IEC Discussion document, pp. 86.

[237] Duigan, *An introduction to vulnerabilities in electronic voting*, p. 6.

Moreover, in a manual system, "traditional safeguards for ballot security have the advantage of being legible to the entire public, and violations of protocol are easy enough for anybody to comprehend. Violations are less ambiguous and easier to detect." By contrast, "electronic systems can be harmed in a much more systematic way, and much more covertly, than traditional electoral systems".[238] Interfering with electronic systems requires a high level of technical expertise, which means that relatively few people have the capacity to do it. It also means, however, that equally few people have the technical competence to guard against it or to assess whether manipulation has in fact taken place.

These factors explain why only 34 countries – 19% of the 174 states included in the database of the International Institute for Democracy and Electoral Assistance (International IDEA) – have opted for electronic voting. By contrast, 81% of these states have chosen to continue using manual systems. There is no convincing reason why South Africa should go against what the 81% majority prefers.

In 2020 the IEC tried to give itself the power to introduce electronic voting by smuggling clauses to that effect into the Electoral Amendment Act of 2020. Those clauses were roundly rejected by the public and other organisations and had to be withdrawn. Now the IEC is using a supposedly more transparent approach to analyse the arguments for electronic voting – but its obvious bias is evident throughout the lengthy discussion document it has devised.

The time has come for the Commission – which a mere 8% of South Africans now trust "a lot" – to halt its long-standing attempts to foist e-voting on the country. The IEC has repeatedly shown that it cannot be relied upon to "ensure a free and fair election" under an electronic voting system. It should abandon its obvious stratagem to increase its control over the count in the crucial elections that lie ahead – and so help keep the ANC in power despite the party's falling support.

South African Institute of Race Relations NPC **30 September 2025**

[238] Duigan, ibid, pp. 9 – 10.