Universiteit van Amsterdam

Instituut voor Informatierecht
Institute for Information Law

The right to trust your vote

Cybersecurity, human rights and electronic voting

December 2024

The right to trust your vote

Cybersecurity, human rights and electronic voting

Ot van Daalen and Nina Hoekstra

December 2024
Amsterdam

Institute for Information Law (IViR, University of Amsterdam), 2024

This report has been funded with a grant from the Methods and Interdisciplinary and Multi-disciplinary Research Fund of the University of Amsterdam. We are grateful to Rop Gonggrijp, Balázs Bodó and Els de Busser for their comments. All errors and omissions remain ours.

The core of this paper was written before the elections in the US on 5 November 2024. Developments that took place after the elections are not part of this paper.

Table of contents

1 Introduction and summary

Voting in elections in the past used to be done with pen and paper. But over the past decades, countries have switched to electronic voting machines (EVMs). Already from the outset, the use of these machines has been heavily criticised by information security experts, concerned about the possibility of election fraud and the undermining of voting secrecy. But experts also raised a more fundamental concern: it's next to impossible to scrutinise the internal workings of EVMs, and this, combined with the potential for tampering, could undermine trust in the outcome of elections.

Now, decades later, these concerns turn out to be warranted. The inscrutability of EVMs has provided politicians with an easy target for objecting to the outcome of elections – including in some of the largest democracies in the world, such as India, Brazil and the US. And the truth is: these objections could be well-founded – the nature of EVMs makes it impossible to verify these claims. This, in turn, is already sufficient to affect trust of the public in the outcome of the elections, a deeply problematic development, not only because it affects the legitimacy of ongoing elections, but also because trust takes time to earn while it can be lost rapidly, so trust in future elections is also at stake.

Still, EVMs are not going to go away any time soon. Many countries have adopted EVMs as the primary voting method and others show increasing interest in adopting them.[1] This means that these concerns remain relevant.

One of the perspectives which has not been explored in detail is how these concerns relate to human rights, in particular the right to vote. This is relevant, because it could provide an objective framework for assessing the legality of the use of EVMs in the voting process. This study aims to fill part of that gap, by answering the question whether the use of EVMs is compatible with the right to vote, as recognized by international human rights instruments.

We conclude that this is not so: the intransparent nature of EVMs makes it impossible to ascertain whether election results are correct, which is at odds with a core requirement of the right to vote, namely that elections be transparent. In fact, the transparency requirement implies that voting must be done on paper, and counted by hand, for one simple reason: paper for now is the only marking technology which can be subject to review by a lay observer.

This conclusion is relevant to governments considering or perhaps reconsidering the use of EVMs. It is also relevant to lawyers contesting results from elections done with these machines in courts. And finally, it provides a relevant insight into the relationship between human rights and trust in the context of information security: in cases where the level of required trust is high (as it is in elections), digital technologies will be ill-equipped to satisfy those requirements.

The scope of this report is limited. It is not about voting via the internet or other kinds of remote voting, not about other human rights aspects in relation to elections, and not about the relationship between EVMs and personal data. We will also not discuss how EVMs provide new ways to present voting options which could favour certain candidates, potentially nudging voters via "dark patterns". Furthermore, we will not touch on the broad range of information security-related concerns existing with regard to EVMs, instead focusing only on the more fundamental concern that the inscrutability of EVMs affects trust.

1 See IDEA, Use of E-Voting Around the World, 6 February 2023, idea.int.

One aspect which we will only touch on in passing is the principle that votes must remain secret to everyone except the voter. We discuss the requirement of voting secrecy only in relation to the requirement of transparency, and do not discuss the requirement itself in-depth. Suffice it to say, however, that the requirement of voting secrecy is also recognised in international human rights instruments, as we will see. So our conclusion that EVMs cannot fulfill the requirement of transparency while safeguarding voting secrecy should not be read to mean that voting secrecy must be watered down to allow the introduction of EVMs.

First, we discuss the human rights framework underlying the right to vote, focusing on international human rights instruments and relevant standards. Here, our conclusion is that transparency in elections is a prerequisite to trust in the outcome of elections, and as such it is a core requirement of the right to vote. Then we focus on how EVMs compare to a paper-based election process when it comes to transparency; we conclude there that EVMs have a fundamental problem satisfying this requirement. We then move on to discuss three case studies of the use of EVMs, namely in India, Brazil and the US. These cases demonstrate that the associated lack of transparency has undermined trust in the outcome of elections in those countries. We then close with observations on the role of EVMs in elections, and how the right to vote stands in the way of the use of EVMs.

2 The right to vote: requirements for elections

In this report, "voting" roughly refers to the process by which citizens select candidates for public office through formal elections, from casting the vote to counting it. Elections are an important part of representative democracies in Europe and North America since the 18th century, allowing citizens to participate both as voters and as candidates.[2]

Over the past decades, the thinking on how to design voting processes has developed significantly. For example, in many countries, voting initially was conducted in the open, often in front of a busy crowd.[3] It was only in the course of the 19th century that anonymity in voting, chiefly through the 'secret ballot', became increasingly important – and by now, this has become a globally recognised standard.[4]

2.1 International requirements for free and genuine elections

Voting not only has become a practice widely adopted by governments, it has since the middle of the 20th century also been recognised in various international and national instruments as a right. On an international level, the origin of the right to vote lies in the 1948 United Nations Universal Declaration of Human Rights (UDHR), which in Article 21(3) provides that:

> The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.

This provision does not, however, explicitly mention the right to vote, yet. This changed in 1966, with the adoption of the International Covenant on Civil and Political Rights (ICCPR). Under Article 25, every citizen must be provided:

> the right and the opportunity [...] to vote and to be elected at genuine, periodic elections, which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors.[5]

These two provisions are the international foundation of the right to vote. Similar provisions can be found in the European Convention on Human rights, the American Convention on Human Rights and the African Charter on Human and Peoples' Rights.[6] And the right has subsequently been developed further in guidelines and handbooks on electoral standards.[7] These electoral standards cover a broad range of topics, from election campaigns to voter discrimination.

---

2 S.P. Raikar, ´Representative democracy´, britannica.com 29 February 2024.
3 See 'Public Voting: Before the Secret Ballot', sociallogic.iath.virginia.edu.
4 Art. 25(b) ICCPR; Art. 23 ACHR; Art. 21 UDHR.
5 Art. 25(b) ICCPR.
6 See Article 3 of Protocol No. 1 European Convention on Human Rights (ECHR); Article 23 American Convention on Human Rights (ACHR); and Article 13 African Charter on Human and Peoples' Rights (ACHPR).
7 Key documents establishing and outlining electoral standards include (non-exhaustive and in a random order): International IDEA's International Obligations for Elections: Guidelines for Legal Frameworks (idea.int); the OSCE's Existing Commitments for Democratic Elections in OSCE Participating States (osce.org); the United Nation's Handbook on International Human Rights Standards on Elections (ohchr.org); the Carter Center's Elections Obligations and Standards (cartercenter.org); the NDI Guide for Developing Election Laws and Law Commentaries (ndi.org); the EODS Compendium of International Standards for Elections (eods.eu). For Europe, the European Commission for Democracy through Law (Venice Commission), Code of Good Practice in Electoral Matters, CDL-AD (2002)23 (rm.coe.int) is relevant, as well as the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE (1990), osce.org.

Our analysis focuses on only one principle within these standards, a principle particularly important when voting electronically: transparency. We chose this focus because transparency not only is a prerequisite for public confidence in elections – and thus legitimacy of the outcome – it also is one of the hardest things do well in the context of electronic voting, as we will see.[8]

2.2 Genuine elections require transparency

While transparency is often mentioned as a requirement in the context of elections, it is not mentioned explicitly in treaty obligations and other political commitments.[9] Rather, the principle can be constructed from the requirement that elections be 'genuine', read together with the fundamental right to seek, receive and impart information, also recognised in human rights instruments.[10]

The requirement that elections be genuine is broad in scope. It sets conditions for the election process – for example that elections must offer voters a real choice, and that internationally recognized fundamental rights, such as the rights to free (political) expression and protection from discrimination, must be fulfilled.[11] It also imposes requirements on the outcome, chiefly that the election results reflect the will of the people.[12]

The idea of transparency follows logically from this last requirement, that the will of the people is the basis of the authority of government. It is only possible to know whether this will is being honoured, when the process through which voting takes place is transparent.[13]

Transparency can be safeguarded in various ways, which have also been laid down in voting standards. In particular, the Venice Commission in its Code of Good Practice in Electoral Matters covered the transparency requirements relating to counting, transfer and tabulation of results in detail.[14] It for example notes that the presence of observers appointed by the candidates must be permitted during voting and counting, that these persons must have access to the records and that results must be transmitted to the higher level in an open manner (Art. 3.2(x), (xiii) and (xiv)).

2.3 Court cases on transparency in elections

The importance of the transparency requirement has also been emphasised by courts. For instance, the European Court in Davydov used these considerations to underline the "importance of technical details, which can be crucial in ensuring an open and transparent procedure of ascertaining the voters' will through the counting of ballot papers and the accurate recording of election results throughout the system, from the local polling station to the Central Electoral Commission".[15] The Court considered that "the post-voting stages covering counting, recording and transfer of the election results form an indispensable part of the election process. As such, they should be accompanied by clear procedural guarantees, be open and transparent, and allow observation by members across the whole political spectrum, including the opposition, in order to ensure the realisation of the principle of the voters' freedom to express their will and the need to combat electoral fraud."

---

8 See for example P. Merloe, An NDI Guide for Developing Election Laws and Law Commentaries, Washington: National Democratic Institute for International Affairs (NDI) 2008, p. 11 (ndi.org).
9 Ibid, p. 13.
10 See for example Election Obligations and Standards: A Carter Center Assessment Manual, Atlanta 2023, p. 15 (eods.eu); Election Observation and Democratic Support (EODS), Compendium of International Standards for Elections, Brussels: Publication Office of the European Union 2016, p. 19 (eods.eu). See for freedom of expression e.g. art. 19(2) ICCPR.
11 Election Observation and Democratic Support (EODS), Compendium of International Standards for Elections, Brussels: Publication Office of the European Union 2016, p. 19 (eods.eu).
12 See United Nations Human Rights Office of the High Commissioner, Human Rights and Elections: A Handbook on International Human Rights Standards on Elections (2021) (eods.eu), par. 84 and references mentioned there.
13 P. Merloe, An NDI Guide for Developing Election Laws and Law Commentaries, Washington: National Democratic Institute for International Affairs (NDI) 2008, p. 14 (ndi.org).
14 See Venice Commission, Code of Good Practice in Electoral Matters, 2002.
15 ECHR 30 May 2017, Davydov and others v. Russia (Application no. 75947/11), par. 283-284.

Perhaps the most relevant court case in this context comes from the German Constitutional Court. This court in 2009 specifically underlined the importance of public scrutiny in the context of electronic voting.[16] It constructed a requirement for such scrutiny from certain provisions of the German constitution. According to the court, it follows from these provisions that Germany is a democratic state, and that all state authority is derived from the people, to be exercised through general, direct, free, equal and secret elections.[17] This means that "all essential steps of an election are subject to public examinability unless other constitutional interests justify an exception".[18] Conversely, a procedure where "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".[19]

According to the court, due to the significant impact of possible errors or deliberate manipulation, special precautions are necessary to comply with the principle of the public nature of elections.[20] The court explicitly mentions how classical election results with paper ballots are virtually impossible to falsify, in contrast to electronic voting computers that are much more vulnerable to manipulation and errors.[21] 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.[22] The voter cannot be required to rely on the functionality and technical integrity of the system, but rather must be able to personally verify whether their vote is recorded truthfully as a basis for counting.[23] It is therefore insufficient if the voter is solely informed by an electronic display that his ballot has been registered, and votes may not be stored exclusively on an electronic storage medium after the balloting.[24]

The court also pointed out that this cannot be compensated for by subjecting sample machines to verification before deployment by an official institution; the "monitoring of the essential steps in the election promotes well-founded trust in the correctness of the election certainly in the necessary manner that the citizen himself or herself can reliably verify the election event".[25]

16 Federal Constitutional Court of Germany, 2 BvC 3/07, 2 BvC 4/07, 3 March 2009.
17 See Art. 20.2 of Germany's Basic Law.
18 Federal Constitutional Court of Germany, 2 BvC 3/07, 2 BvC 4/07, 3 March 2009, par. 112.
19 Ibid, par. 113.
20 Ibid, par. 120.
21 Ibid, par. 120.
22 Ibid, par. 119.
23 Ibid, par. 121.
24 Ibid, par. 121 & 122.
25 Ibid, par. 125.

2.4 Trust in the outcome and the process is a central requirement for genuine elections

Before we discuss to what extent EVMs can in theory provide the level of transparency the right to vote requires, it is worthwhile to explore further exactly why public scrutiny and the principle of transparency are so important in the context of elections.[26] The main reason is that scrutiny contributes to trust – trust that the election process leads to an outcome which accurately reflects the will of the people. Voters must be convinced that the outcome is based on all the votes as they were intended to be to cast.

It is thus fair to say that transparency is a prerequisite for trust in elections. Transparency throughout the entire election process is crucial for citizens to understand and ultimately accept the process and its outcome as a true reflection of their will. Not only must the result be true to the votes cast, but the public must also be convinced that this is the case. When there are doubts of any kind about the reliability of the process, the system falters and democracy is at risk.

And while there are established processes for achieving transparency in paper voting, applying public scrutiny to e-voting technologies turns out to be much harder to achieve, as we will discuss below.

26 See also on this topic W. Pieters, 'Acceptance of Voting Technology: between confidence and trust', in: K. Stølen, W.H. Winsborough, F. Martinelli & F. Massacci (eds.), Trust Management, Berlin: Springer 2006, p. 283-297; A. Oostveen & P. Van den Besselaar, 'Trust, Identity and the Effects of Voting Technologies in Voting Behavior', Social Science Computer Review 2005; and P. Sztompka, 'Trust, distrust and the paradox of democracy', WZB Discussion Paper 1997, No. P 97-003, Wissenschaftszentrum Berlin für Sozialforschung (WZB), Berlin 1997.

3 Designing the voting process

3.1 Essential aspects of transparency

For a voting system to qualify as transparent and verifiable, voters need to be able to confirm three things with regard to their votes:

- First, they must be able to ascertain that their ballots have been cast as intended, meaning that the voter can check whether their ballot correctly expresses their intended vote, and must have the opportunity to correct or revise it.[27]

- Second, the vote must be recorded as cast, meaning that the voter is able to verify that their vote has been received by the ballot box without being altered, and convince themselves that their vote is included in the set of votes tallied.

- And finally, the vote must be counted as recorded: any member of the public (when provided with the data used and produced by the system) must be able to verify that the final tally accurately reflects the total of the ballots collected.[28]

This approach is usually called 'end-to-end (E2E) verifiability', which refers to systems that are designed to be fully auditable throughout their entire operation.[29]

Now, if auditability were the only requirement which electronic voting technologies would have to fulfill, this would already be a hard challenge – but a challenge which could potentially be achieved through some form of radical transparency, making it possible for everyone to verify that these requirements are being met.

But what makes this especially complex, is that these requirements are combined with the condition that nobody other than the voter should be able to determine how an individual voted, even with their cooperation.[30] This requirement, that votes in essence must remain secret for others than the voter themselves, makes electronic voting machines notoriously difficult to design and implement.[31]

3.2 Transparency in paper-based elections

In conventional paper elections, a number of measures are generally in place to fulfil these three requirements while still safeguarding voting secrecy.[32] For example, one commonly applied method to ensure transparency is by making the counting of votes and tabulating of the results accessible to the public for observation.

---

27 P.B. Rønne, P.Y.A. Ryan & B. Smyth, 'Cast-as-Intended: A Formal Definition and Case Studies', in: M. Bernhard et al, Financial Cryptography and Data Security, Berlin: Springer 2021, p. 251-262 (orbilu.uni.lu).

28 National Academies of Sciences, Engineering and Medicine, Securing the Vote: Protecting American Democracy, Washington: The National Academies Press 2018, p. 97 (nap.nationalacademies.org).

29 P.Y.A. Ryan, S. Schneider & V. Teague, 'End-to-End Verifiability in Voting Systems, from Theory to Practice', IEEE Security & Privacy 2015/3, no. 13 (core.ac.uk).

30 Ibid.

31 Dill, Schneier & Simons, 'Voting Technology: Who Gets to Count Your Vote?', Communications of the ACM 2003/46, no. 8, p. 31 (dl.acm.org).

32 See aceproject.org for an overview and explanation of the different steps in the voting process. Of course, some local differences occur from country to country, but these differences mostly do not fundamentally change the requirements that are in place to generate genuine and reliable election results.

In addition, the ballot box is often shown to be empty by the polling staff before starting the election – to prevent votes being stuffed beforehand. The ballot box is then sealed, to prevent anyone modifying a ballot or removing it from the ballot box.[33] It then remains sealed in a publicly visible place, and polling workers ensure that only eligible voters can submit their votes. A voter who has deposited their vote in the ballot box can generally wait until the closing of the polls, to be confident that, when the seal of the ballot box is broken to start counting, their ballot is included in the batch.[34] And after unsealing, the votes are then counted.

In a fully paper process, the counting is done manually by checking the votes recorded on each paper ballot. This process typically involves teams of election workers who tally the results from each ballot box and record the totals.

In some cases, representatives from political parties or independent observers may also be present to witness the opening of the ballot box, oversee the counting process and verify the results.[35] Parties can also generally request a recount under certain conditions, in which case the votes are then recounted, until consensus has been reached.

Once all votes have been counted and tallied, election officials certify the results and announce the results of the election. Results are reported to the public and relevant authorities, and any disputes or challenges to the outcome are addressed through established legal procedures.

As we will see, it is difficult, if not impossible for e-voting systems to provide guarantees similar to those used for paper elections when it comes to transparency. First, it is useful to describe the different forms of electronic voting technologies currently in place.

3.3 The different forms of electronic voting

Electronic voting (e-voting) systems are systems which support the recording, casting or counting of votes in political elections with information and communication technologies.[36] For this report, we only focus on EVMs which do not use the internet. Broadly speaking, there are three classes of EVMs: Direct Recording Electronic (DRE) voting machines, Ballot Marking Devices (BMDs) and optical scanning systems, which each have a function in enabling voting, counting, or both.[37]

DREs are the only machines that exclusively use electronic means to collect and store votes. Voters use the machine's interface to make their selections. After having done so, voters typically have the opportunity to review their choices on a summary screen to ensure accuracy. If any errors are found, voters can correct them. Once satisfied with their selections, voters cast their ballots electronically by confirming their choices on the machine. The electronic system records and stores the votes in its internal memory.

When the polls close, the DREs subsequently tally the votes automatically. The results are then transmitted to a central database or election headquarters for aggregation and tabulation. Election officials may conduct audits and verification steps to ensure the accuracy and integrity of the electronic voting system. This may include comparing electronic tallies with paper records (if available), conducting post-election audits, and verifying the security of the voting machines.

---

33 See for example D.F. Aranha & J. Van de Graaf, 'The Good, the Bad and the Ugly: Two Decades of E-Voting in Brazil', IEEE Security and Privacy Magazine 2018/16, no. 6, p. 25 (researchgate.net).
34 Ibid.
35 'Elections are a Process', openelectiondata.net.
36 International Institute for Democracy and Electoral Assistance (IDEA), Introducing Electronic Voting: Essential Considerations, Stockholm 2011, p. 6 (idea.int).
37 See for an accessible overview R.K. Gambhir & J. Karsten, 'Why paper is considered state-of-the-art voting technology', brookings.edu 14 August 2019.

Ballot Marking Devices by contrast only take care of the first step of this process: the voting. With BMDs, voters can select their choice on a screen and the device then prints a (machine-readable) paper ballot containing the voter's choice. This produces a voter-verified paper audit trail, VVPAT. Rather than storing the selections electronically, the paper ballots are to be either counted by hand, or counted electronically by a separate optical scanner.

Finally, optical scanning systems only take care of the second step of this process: the counting. In this method, people cast their vote via paper, which are then counted by computers. Voters are given machine-readable ballot cards, so that an optical scanner can subsequently identify the mark made on the ballot and translate votes into digital data. The individual votes are recorded in a database and aggregated to electronically tally the total election results. The counting can either happen directly in the polling station, or the scanning is done centrally in special counting centres. This system provides a paper audit trail by design, which enables the option of comparing the paper ballots with the scanner's tabulation when a manual count is being done.

When compared to paper ballots, e-voting is often presented to have a number of benefits: it's faster in delivering the election results (especially with complicated electoral systems), it's more reliable (because human error in counting is excluded), and it prevents certain types of fraud like ballot-box stuffing.[38] Lengthy ballots may also be presented more conveniently, and e-voting may be more accessible for people with disabilities (e.g. audio ballots papers for visually impaired voters).[39] In the long term, cost-effectiveness is also cited as a perceived benefit.[40] This report will not review whether these are valid claims. What we do know, however, is that deploying electronic voting and counting technologies poses particular challenges when it comes to transparency.

3.4 Electronic voting increases risks of errors or fraud

As with any digital system, electronic voting technologies carry the risk of accidental design flaws or malfunctions. In fact, the complex nature of election software creates an increased risk for accidental bugs and vulnerabilities to be introduced in their development.[41]

But an even more serious concern than poor software development is the risk of deliberate tampering with EVMs, either through compromised insiders or by external attackers. Given the high stakes that are typically involved during elections for public office, the incentive to manipulate EVMs should not be underestimated.[42] And as with any other computer software and hardware, EVM systems are very much capable of being hacked.[43] While the implementation of e-voting technologies could reduce the risk of fraud by individual election officials at the polling station level, the digital and more centralised nature of these technologies increases the risks of concerted attacks against the voting infrastructure.[44]

This is why EVMs must be protected from these kinds of attacks throughout the entire supply chain. But even if the code that's supposed to be running an election system is audited beforehand, there is, fundamentally, no way to guarantee fully that this is the actual and only code that is running on the machine on election day.[45] And while you could think of some measures to counter or at least detect

38 ACE Electoral Knowledge Network, 'Encyclopaedia E-voting: Benefits, Risks and Costs', aceproject.org.
39 Ibid.
40 Ibid.
41 J.A. Halderman, 'Practical Attacks on Real-world E-voting', in: F. Hao & P.Y.A. Ryan (eds.), Real-World Electronic Voting: Design, Analysis and Deployment, Taylor & Francis Group 2017, p. 146 (jhalderm.com).
42 Ibid, p. 146 (jhalderm.com).
43 National Academies of Sciences, Engineering, and Medicine, Securing the Vote: Protecting American Democracy, Washington, DC: The National Academies Press 2018. nap.nationalacademies.org, p. 90-91.
44 International Institute for Democracy and Electoral Assistance (IDEA), Introducing Electronic Voting: Essential Considerations, Stockholm 2011, p. 16 (idea.int).
45 J.A. Halderman, 'Practical Attacks on Real-world E-voting', in: F. Hao & P.Y.A. Ryan (eds.), Real-World Electronic Voting: Design, Analysis and Deployment, Taylor & Francis Group 2017, p. 146 (jhalderm.com).

certain forms of vote tampering, such as creating backups and logs, the problem is that these all are based on the same kinds of electronics you're trying to monitor, and thus they could fail in the same way.

This means the theoretical possibility associated with EVMS that votes can be tampered with at scale is not far-fetched at all, and this is already sufficient for our analysis – it undermines trust in the EVMs, and thus the outcome of the results produced with those EVMs.

3.5 Electronic voting lacks transparency

This lack of trust is compounded by the fact that EVMs are essentially 'black box-systems': "the machine takes input from voters and produces output in a way that cannot be observed and verified by external observers or easily checked by election administrators".[46]

And the problem is; there is no way to design a fully transparent process where all these steps would be subject to external observation all the time. In the worst case, software for EVMs will generally be built on top of already existing software libraries and existing operating systems, consisting of millions of lines of already developed code which have not been subjected to scrutiny. Similarly, the hardware will generally be built from already existing off-the-shelf hardware. In the best case, software and hardware are built entirely from scratch. Even then, it will be exceedingly hard to determine whether the software and hardware, working together, will be doing what they are supposed to do on election day – and at the very least require observers with unique skills to assess the software and hardware.

Even if the design of the machines could be subject to audits beforehand which provide sufficient guarantees that all votes are counted in theory, the manufacturing of these machines at scale in practice introduces another fundamental issue in regard to observability. One could easily imagine some machines containing different software than designed, introduced by an attacker during manufacturing. And more fundamentally, there is no way to tell for external observers that the hardware used in the actual machines is exactly the same as the hardware envisaged in the design – this would require dismantling each machine to the point of destruction. Yet, this exactness is the kind of accuracy that is required for elections.

In addition, during the elections, the observation of the functioning of an EVM is fundamentally impossible as well. An observer cannot ascertain that what is shown on a screen of an EVM is what is recorded in the record – they essentially will have to rely on assurances that the development process resulted in trusted software, which then was translated into trusted machines.

One measure which is often suggested to provide a semblance of transparency is the voter-verifiable audit trail (the VVPAT), which in theory could allow for the possibility of detecting errors in voting software.[47] Auditing the VVPAT has a very limited function, however, because if EVMs cannot be trusted in the first place, auditing the outcome via VVPATs is only useful to demonstrate that EVMs cannot be trusted, not that they can in fact be trusted. Moreover, if an audit confirms an EVM cannot be trusted, the most sensible solution would be to manually count the entire VVPAT.[48]

In addition, paper audit trails are only relevant in the first step of the process: providing verification that the ballot was cast as intended by the voter. That is insufficient because what really matters is whether the

46 International Foundation for Electoral Systems (IFES) & National Democratic Institute for International Affairs (NDI), Implementing and Overseeing Electronic Voting and Counting Technologies, Washington 2013, p. 46.
47 R.L. Rivest & J.P. Wack, 'On the notion of 'software independence' in voting systems', nist.gov 28 July 2006, p. 5.
48 Which also means that, if one agrees with the conclusion that EVMs cannot be trusted anyway, the VVPAT should be the primary form of voting and counting. Which would also mean that the intermediary step of using the EVMs can be discarded altogether.

ballots are accurately included in the final tally.[49] If this later step also involves an EVM, this leads to the same problem of inscrutability discussed above.

There are several other reasons why the utility of VVPAT audits is limited at best. On a practical level, the effectiveness of a paper trail in enhancing transparency and verifiability depends largely on voters' willingness to actually verify their ballot. On a procedural level, meaningful use of VVPAT systems also involves establishing a statistically sound random sample size and a selection procedure for determining that the votes must be counted by humans. Given that election outcomes can vary wildly, it is next to impossible to predict on the basis of previous voting patterns whether a voting outcome contains a discrepancy. Furthermore, the threshold for determining whether it is necessary to do a manual count is easier to determine in a two party-system like the United States, but is difficult to determine in multi-party voting systems. Additionally, procedures must be in place for resolving any discrepancies between the manual count and the electronic result.[50] In practice however, post-election verification processes may be minimal.

3.6 Interim conclusion

As noted above, international standards require that all electoral activities should be conducted in a 'wholly transparent manner'.[51] This means that each step can be subjected to scrutiny.[52] Several measures have been developed to enable such transparency and thus increase trust in paper-based voting.

When EVMs are used in elections, they play a crucial role in determining the outcome, automating the voting step, the counting step, or both. That's why it is essential to be able to examine the inner workings of such machines, in order to establish trust in the results obtained through them.

However, EVMs lack basic transparency. In traditional elections, actions like marking a ballot and depositing it in a ballot box are open to direct observation by voters and others.[53] However, with EVMs, these steps occur inside the machine, making them invisible to the public. Measures aimed at providing a certain understanding of the internal workings of these EVMs, for example through audits, do not provide the same degrees of assurance as direct observation by public observers. This is particularly problematic because EVMs are such an interesting target for attacks.

Through three case studies, the next chapter illustrates the risks associated with this development. These examples demonstrate that EVMs not only fail to meet the human rights-required conditions for transparency in theory, but that this also undermines trust in the outcome in practice.

49 D. Castro, 'The U.S. should ban paperless electronic voting machines', Communications of the ACM 2008/51, no. 10, p. 29-33 (dl.acm.org).
50 International Institute for Democracy and Electoral Assistance (IDEA), Introducing Electronic Voting: Essential Considerations, Stockholm 2011, p. 24 (idea.int).
51 See: Human Rights and Elections: A Handbook on the Legal, Technical and Human Rights Aspects of Elections, New York & Geneva: United Nations Centre for Human Rights 1994, par. 102 (ohchr.org).
52 International Foundation for Electoral Systems (IFES) & National Democratic Institute for International Affairs (NDI), Implementing and Overseeing Electronic Voting and Counting Technologies, Washington 2013, p. 41 (ndi.org).
53 Ibid.

4 EVMs do not comply in practice with requirements

As noted in the introduction, many countries have considered using EVMs in the past, but some have since suspended the practice. For example, in the Netherlands, various types of (electronic) machines were the primary voting method for a period of over thirty years (ca. 1970-2007).[54] But in the run-up to the 2006 elections, critics raised a number of concerns, and after a thorough investigation, an independent commission recommended a return to paper voting, after which the EVM disappeared from the Dutch electoral scene. A similar fate befell the voting machine in Germany. After a trial period of seven years, the German Constitutional Court as discussed above declared e-voting unconstitutional after the 2005 election.[55] The implementation of e-voting was cancelled after conducting unsuccessful try-outs in other countries, such as Finland, the United Kingdom, Ireland, Italy and Norway.[56]

There are also countries which have a relatively long tradition of electronic voting and continue using them. We pick three: India, Brazil and the USA. These countries serve as valuable case studies, as all three countries started experimenting with electronic voting early on, and they are large democracies. For each country, we look at the type of e-voting technology used and discuss the challenges the technology has posed, and still poses today.

4.1 India

4.1.1 Historical background

With a population of over 1,4 billion people, of which about 950 million have the right to vote, India is by far the largest democracy in the world.[57] In May 2024, national elections took place again. The huge population, combined with a fairly complex multi-party system, makes organising elections a challenging task.

Before the introduction of EVMs, India used paper ballots that were counted manually. This led to a relatively high amount of invalid votes; in the last paper elections in 1999, over 7 million votes had to be invalidated.[58] Besides being inefficient, the paper system was also expensive: there were high costs involved in printing the ballots, storage, transportation across the country and hiring staff to count the votes. Finally, it was claimed that there were significant risks of electoral fraud and corruption – one of the major problems India faced during election time was 'booth capturing'. Criminal groups were directed by political parties to occupy polling stations and stuff the ballot box.[59]

This is why the Indian government started experimenting with EVMs early on. In 1983, they were first used in the Delhi Metropolitan Council Election. In 2004, e-voting was adopted on a national scale as the

54 In the 2006 municipal elections, 97.7% of Dutch municipalities voted using EVMs, see: Eindrapport Commissie Korthals-Altes, Stemmen met vertrouwen: Adviescommissie inrichting verkiezingsproces, Den Haag 2007, p. 29 (kiesraad.nl).
55 International Foundation for Electoral Systems (IFES) & National Democratic Institute for International Affairs (NDI), Implementing and Overseeing Electronic Voting and Counting Technologies, Washington 2013, p. 107 (ndi.org).
56 S. Risnanto e.a., 'E-voting Readiness Mapping for General Election Implementation', Journal of Theoretical and Applied Information Technology 2020/98, no. 20, p. 3281. See: Table 1: E-voting implementation.
57 There are authors who are critical of the notion that India should be considered a democracy; see e.g.: M. Tudor, 'Why India's Democracy Is Dying', Journal of Democracy 2023/34, no. 3, p. 121-132 (journalofdemocracy.org).
58 M. Herstatt & C. Herstatt, 'India's Electronic Voting Machines (EVMs): Social construction of a 'frugal' innovation', Working paper 2014, no. 86, p. 9, see figure 1 (econstor.eu).
59 Ibid.

primary voting method.[60] In the 2024 elections, over 3 million voting machines divided across 1,2 million polling stations have been deployed.[61] Paper votes are confined to remote areas only.

4.1.2 Indian EVMs

The Indian voting machines initially consisted of two units, a control unit and a balloting unit, connected by an insulated cable. The control unit is manned by a polling officer, while the balloting unit is placed in the voting booth. Instead of handing the ballot paper to the voter, the employee presses a button on the control unit, which then allows the voter to cast his/her vote on the balloting unit screen.[62]

For a long time, the Indian e-voting system did not provide any paper trail. However, this system was contested before the Indian Supreme Court, and the Court considered that "the paper trail is an indispensable requirement of free and fair elections.", and concluded that "the confidence of the voters in the EVM can be achieved only with the introduction of the paper trail."[63] This, together with political pressure, resulted in the introduction of a VVPAT in 2013.

The Indian VVPAT is provided through a system attached as an add-on to the existing EVMs, allowing voters to verify their votes being cast – in theory, that is, because in practice this may be difficult, which we discuss below. This is done by printing a slip containing the serial number, name and symbol of the candidate. This is shown through a transparent window for about seven seconds. Then, the slip falls in the sealed box with a beep, indicating that the vote is cast.[64]

After a random selection, the slips are used for counting and verification by comparing them with the electronic count reflected in the EVMs. The Indian Election Rules provide that if there is a discrepancy between the votes displayed on the control unit and the counting of the paper slips, the count of VVPATs shall prevail.[65]

4.1.3 Critique and controversies

While the electronic voting system in India has been in place for a number of years already, significant concerns remain. Not only are Indian machines theoretically susceptible to manipulation, there are also real concerns of voter fraud with these machines.[66]

Cybersecurity experts have raised these concerns in 2010. At that time, Hari Prasad, Alex Halderman and Rop Gonggrijp demonstrated that the EVMs used by India at that time were vulnerable to fraud.[67] These models have since been replaced by an updated version, but in 2019 Prasad claimed again that these might still be susceptible to hacking.[68] In particular, he observed that the visual display that appears on the VVPATs after the voter has expressed their choice on the EVM is meant to remain visible for seven seconds, but instead vanishes after just three seconds – less than half of the duration.[69] This four second gap would, theoretically, enable a second vote to be cast later, according to Prasad.[70]

---

60 C.B. McCormack, Democracy Rebooted: The Future of Technology in Elections, Washington: Atlantic Council 2016, p. 9 (atlanticcouncil.org).
61 A. Bhaumik, 'Election Commission to set up 12 lakh polling booths', deccanherald.com 26 January 2024.
62 'Frequently Asked Questions on Electronic Voting Machines', ceomanipur.nic.in
63 Subramanian Swamy v. Election Commission of India (2013), par. 29, electionjudgments.org
64 'Frequently Asked Questions: EVM and VVPAT', ceomadhyapradesh.nic.in
65 Rule 56(D)(4)(b) of Conduct of Election Rules, 1961.
66 See for a somewhat different conclusion Avgerou, Masiero & Poulymenakou, Journal of Information Technology 2019/34, no. 3, p. 263-289.
67 See: H.K. Prasad, J.A. Halderman, R. Gonggrijp et al., 'Security Analysis of India's Electronic Voting Machines', indiaevm.org, 29 April 2010.
68 K. Saini, 'EVMs and the Need for Greater Electoral Transparency', thewire.in 27 September 2023.
69 M. Jay, 'Why is the EC stonewalling Hari Prasad and questions raised on EVMs?', nationalheraldindia.com 16 April 2019.
70 'VVPAT Has a Coding Problem But EC Refuses to Listen: Hari Prasad Vemuru of TDP', The Quint, youtube.com 18 April 2019.

There have also been recurrent reports of election irregularities involving these machines.[71] For example, in the 2009 elections, EVM malfunctions were reported in more than 15 constituencies.[72] Among other things, there were mentions of voters pressing a button for one candidate, but a light would flash for another.[73] In 2017, it was also reported that the number of votes counted via the EVM and eventually counted did not match.[74]

As a result, the leaders of 21 opposition parties filed a petition at the Indian Supreme Court to direct the Election Commission of India (ECI) to verify at least 50% of the votes cast in each constituency using the VVPAT machines for the 2019 elections. At the time, the Election Commission was conducting physical matching of VVPAT slips for about 4,124 EVMs across 479 voting booths, which accounts to less than 0,44% of EVMs in the whole country.[75] The Supreme Court ordered to increase the number of EVMs that are subjected to the verification of paper trails from 1 to 5 per constituency, which is the equivalent of around 2% verification and much less than the 50% that the petitioners had pleaded for. The court noted explicitly that it was not questioning the accuracy of election results, but that the increase would lead to 'greater satisfaction among the political parties and the electorate of the country'.[76]

In 2023, the NGO Association for Democratic Rights then filed a petition at the Supreme Court for raising the number of VVPATs verification to 100%.[77] In addition, the organisation pleaded that the print-out of the VVPAT slips must be handed over to the voter who, in turn, must be able to deposit them in the sealed VVPAT Box.[78] All petitions were, however, denied by the Court, considering that "the suspicion that the EVMs can be configured/manipulated for repeated or wrong recording of vote(s) to favour a particular candidate should be rejected.''[79]

The auditing processes in place for EVMs have been met with criticism as well. Currently, the Technical Evaluation Committee (TEC) of the Election Commission of India is solely responsible for auditing the EVMs, which is the same body that is responsible for designing the system and writing its software.[80] This issue was addressed before the Indian Supreme Court in 2023, but the petition requesting an independent audit into the source code of the software used in EVMs was dismissed as well.[81]

Finally, in the months before the 2024 elections and afterwards, concerns about irregularities with the EVMs continued to persist.[82] Protestors believed that the party of the prime minister, Narendra Modi, would selectively manipulate EVMs to win the elections. One candidate, Rahul Gandhi, repeatedly warned about the risks of EVMs, calling them a “black box”, also referring to a media report that one candidate was able to “unlock” an EVM with her phone.[83]

So at the very least, an important takeaway is that the use of EVMs has given opposition candidates a powerful argument to publicly contest the outcome of the elections in India.

---

71 P. Agarwal, 'More transparency needed on malfunctioning EVMs', deccanherald.com 1 July 2022.
72 H.K. Prasad, J.A. Halderman, R. Gonggrijp et al., 'Security Analysis of India's Electronic Voting Machines', indiaevm.org 29 April 2010, p. 6.
73 Ibid.
74 'EVM tampering issue: A timeline of previous allegations of voter fraud', indianexpress.com 9 May 2017.
75 A. Mathur, 'Supreme Court orders EC to increase VVPAT verification from one EVM to five', indiatoday.in 8 April 2019.
76 Supreme Court of India 8 April 2019, (C) No. 273/2019 (Chandrababu Naidu v Union of India), p. 8For full decision, see: scobserver.in
77 Supreme Court of India 24 April 2024, (C) No. 434/2023 (Association of Democratic Reforms Vs. Election Commission of India).
78 M.G. Devasahayam & M. Pracha, 'In a Democracy, Paper Ballot Is the Gold Standard for Elections. Per Law, Use of EVM Is an Option', thewire.in 15 March 2024.
79 'Supreme Court Judgment On EVM-VVPAT Verification: Live Updates', livelaw.in 26 April 2024.
80 K. Saini, 'EVMs and the Need for Greater Electoral Transparency', thewire.in 27 September 2023.
81 M. Jain, 'SC Refuses to Hear Plea Seeking Audit into Source Code of Software Used in EVMs', thewire.in 22 September 2023.
82 'VCK stages protest against using EVMs in LS election', thehindu.com 23 February 2024.
83 See ‘Row in Mumbai over ‘unlocking’ of EVM’, The Hindu, 16 June 2024; and ‘EVMs in India are 'black box', nobody allowed to scrutinise them: Rahul Gandhi’, The Hindu 16 June 2024.

4.2 Brazil

4.2.1 Historical background

Electronic voting has a significant history in Brazil, with the country being one of the first to adopt EVMs on a large scale.

Although there were variations in the Brazilian paper voting process between different types of elections in the country (such as presidential, gubernatorial, and legislative elections), the size of the country and its population, invariably made it a complex organisational undertaking. For the legislative elections, for example, the large number of candidates running made it impossible to design a paper ballot that included the names of every competitor, so you had to manually write down the candidate you were voting for.[84] This led to high numbers of invalid votes, with over 40% declared invalid in the 1990 elections.[85] Another important reason for adopting electronic voting machines was to combat fraud and corruption in the tabulation process.[86] The lengthy tabulation period after election day created opportunities for corrupt vote counters that were allied with electoral candidates to manipulate the outcome.[87]

Already in the 1980s small-scale experiments were conducted, aimed at exploring the feasibility of using electronic systems to streamline the voting process and improve accuracy in tabulating election results. The first large-scale use of electronic voting in Brazil occurred in 1996 during municipal elections. The success of these initial deployments paved the way for broader adoption in subsequent elections. In 1998, Brazil became the first country to organise national elections using electronic voting machines. It has since become the country's exclusive voting method.

4.2.2 Brazilian EVMs

Today, there are some 550,000 EVMs distributed across approximately 460,000 polling stations throughout the country.[88] Brazil uses a DRE system, doing both the voting and the counting exclusively with a machine. The machine consists of two terminals: one used to authenticate voters, and one for casting votes.

The two terminals are physically connected with a cable, but experts warn that this is a fatal design flaw, as it allows for attacking voting secrecy: "by logging chronologically the data registered by both devices and combining them, one can perfectly deduce who voted for whom."[89]

After the polls close, the EVM produces a tally printout, a physical document containing totals for each candidate per machine. These partial results are stored on USB drives and transmitted to a central place where they are combined to generate the official election outcome, which is usually determined in only a matter of hours.[90]

---

84 R. Schneider & K.N. Senters, 'Winners and Losers of the Ballot: Electronic vs. Traditional Paper Voting Systems in Brazil', Latin American Politics and Society 2018/60, no. 2, p. 47; For instance, in the 1998 elections, 1,265 candidates competed for a position in the state legislature and 661 candidates competed for a position in the federal legislature in the state of São Paulo, footnote 3, p. 57. For presidential and gubernatorial elections however, voters cast their vote by selecting a candidate from a predetermined list, see p. 42.

85 T.J. Power & J.T. Roberts, 'Compulsory voting, Invalid Ballots and Abstention in Brazil', Political Research Quarterly 1995/48, no. 4, p. 797.

86 International Foundation for Electoral Systems (IFES) & National Democratic Institute for International Affairs (NDI), Implementing and Overseeing Electronic Voting and Counting Technologies, Washington 2013, see: Figure 6 - The Rationale for E-voting in Brazil, p. 83.

87 Ibid.

88 T. Jokura, 'Brazil's electronic voting machine comes of age', revistapesquisa.fapesp.br August 2021.

89 D.F. Aranha & J. Van de Graaf, 'The Good, the Bad and the Ugly: Two Decades of E-Voting in Brazil', IEEE Security and Privacy Magazine 2018/16, no. 6, p. 27.

90 Idem, p. 23.

4.2.3 Critique and controversies

Many of the concerns voiced by Indian experts regarding the use of EVMs have also been raised in Brazil. One major difference, however, is that the Brazilian device does not feature any type of paper trail. VVPATs were briefly experimented with in 2002, but they were discontinued already one year later.[91] Instead, a purely digital substitute is employed, in which each individual vote is recorded as data in a random order in the voting machines' electronic memory.[92] While this data can be used afterwards to count individual votes, there is no way for voters to verify whether their vote is cast or recorded as intended – the vote can be undetectably changed.[93] A bill by the Brazilian Congress in 2018 to reintroduce the VVPAT was suspended by the Supreme Court because paper records would violate ballot secrecy.[94] This means Brazil currently is the only country in the world to use a fully digital voting system, without paper backups.[95]

Critics highlight that the lack of a paper trail creates a reliance on the integrity of the software, which is challenging to audit for potential manipulation.[96] The Tribunal Superior Eleitoral (TSE), responsible for overseeing elections in Brazil, develops the software used in electronic voting machines internally.[97] However, access to both the voting equipment and its software is significantly restricted.

Although there are strong calls from electronic voting advocates for the source code to be made publicly available, the TSE has chosen to not release it. They assert that keeping the software's details confidential helps shield it from potential attacks. But many experts argue that this notion of "security through obscurity" is not a reliable strategy for safeguarding security.

In order to satisfy the persistent calls for increased transparency, the TSE started organizing hackathons in 2009, where a select group group of pre-approved researchers are given the opportunity to find vulnerabilities in the systems' security mechanisms and provide suggestions for improvement.[98] In addition to the hacking challenge, the TSE also introduced a form of auditing by having between three and five EVMs in each state randomly selected and submitted to a public ceremony, to verify whether the machines are recording the votes cast.[99]

4.2.4 Brazil's 'stolen' elections of 2022

Even after 25 years, this debat is still very much alive. In recent years, this debate was largely fuelled by Bolsonaro, who was the Brazilian president from 2019 to 2022. Bolsonaro has been a vocal critic of the e-voting system used in Brazilian elections. After not achieving victory in the first round in 2018, he claimed to have been cheated by the electronic voting machines, even continuing after he won the elections.[100] Bolsonaro claimed that they are 'easy to rig' by hackers and advocated for the adoption of printed paper ballots as a backup to verify the accuracy of the electronic results. However, the TSE reaffirmed its confidence in the paperless electronic voting system and dismissed Bolsonaro's claims.

Especially in the months leading up to the 2022 elections, with the polls showing Bolsonaro falling behind left-wing opposition candidate Lula da Silva, he started raising concerns again about the fairness of

91 D.F. Aranha, M.M. Karam, A. de Miranda, F.B. Scarel, 'Software Vulnerabilities in the Brazilian Voting Machine', in: D. Lekkas & D. Zissis (eds.), Design, Development, and Use of Secure Electronic Voting Systems, Pennsylvania: IGI Global 2014, p. 149-175.
92 Ibid.
93 Ibid.
94 Ibid, p. 336.
95 ' Brazil Counted All Its Votes in Hours. It Still Faces Fraud Claims', nytimes.com.
96 D.F. Aranha & J. Van de Graaf, 'The Good, the Bad and the Ugly: Two Decades of E-Voting in Brazil', IEEE Security and Privacy Magazine 2018/16, no. 6, p. 30.
97 Ibid, p. 336.
98 Ibid.
99 NDI & IFES, Case Study Report on Brazil Electronic Voting: 1996 to Present, ndi.org, p. 248.
100 N. Froio, 'Brazil adopted electronic voting years ago. Some say they still don't trust it', restofworld.org 2 October 2022.

Brazil's electronic voting system.[101] The debate about the integrity of the electronic voting system and subsequent calls for electoral reforms became major themes in the lead-up to the 2022 elections. Bolsonaro managed to mobilise a large group of his supporters, which resulted in several demonstrations in various cities across Brazil. In Rio de Janeiro for example, thousands gathered chanting and holding signs like "AUDITABLE VOTE NOW!".[102] The protests attracted both supporters and critics of Bolsonaro, which led to some instances of counter-protests and clashes between opposing groups.

Bolsonaro narrowly lost the 2022 election to the current Brazilian president.[103] Bolsonaro never admitted defeat. In the weeks following the results, protest emerged with tens of thousands of Brazilians gathering across the country to denounce what they see as an unfair or stolen election.[104] A collective turnout of well over 100,000 people has been reported, with protesters in at least 75 cities.[105]

Two weeks after the elections, a highly anticipated report on the voting process was published by Brazil's military, concluding that no evidence of irregularities was found, but that it could not rule out voter fraud either due to the EVMs.[106] To many pro-Bolsonaro Brazilians, the report served as further evidence the president's loss should be questioned.[107]

On 8 January 2023, one week after Lula was inaugurated, several hundred Bolsonaro-supporters stormed government buildings in an attempt to overturn the presidential election. Protesters stood on the roof of Congress building with a banner that made a single demand: "We want the source code."[108] Some 1,400 protesters were arrested following the event.

Brazil's highest electoral court subsequently barred Bolsonaro from running for public office until 2030.[109] In addition, he is facing several criminal investigations regarding his suspected role in inciting an uprising after his rejection of the elections result. But Bolsonaro's message is still popular: in February 2024, almost 1,5 years after losing the 2022 elections, an estimated 185,000 people rallied in a huge demonstration in São Paulo to express their support for him.[110]

Even after his electoral defeat and subsequent political disqualification, Bolsonaro continues to make his claims. Bolsonaro has stated that 'there is no way to prove the elections were or weren't fraudulent'.[111] The impossibility not only of substantiating but also of refuting his claims is precisely what makes them problematic. The Brazilian election results cannot be verified, leaving room for the opposition to undermine trust in the results of the election.

101 Ibid.
102 D. Álvarez, 'Election body targets Bolsonaro after he fails to show fraud', apnews.com 3 August 2021.
103 D. Jeantet & D. Rodrigues, 'In Brazil, Bolsonaro voters protest against his defeat', apnews.com 15 November 2022.
104 Ibid.
105 J. Nicas, 'Refusing to Accept Defeat, Bolsonaro Backers Call on Military to Intervene' nytimes.com 8 January 2023.
106 Ibid.
107 Ibid.
108 J. Nicas, 'Brazil Riot: Pro-Bolsonaro Riots Laid Bare Threat to Brazilian Democracy', nytimes.com 10 January 2023.
109 'Brazil's Bolsonaro barred from running for office until 2030', nbcnews.com 1 July 2023.
110 F. Campos Mello & M. Savarese, 'Supporters of Brazil's Bolsonaro stage huge demonstration to defend him amid investigations', apnews.com 26 February 2024.
111 D. Álvares, 'Election body targets Bolsonaro after he fails to show fraud', apnews.com 3 August 2021.

4.3 United States of America

4.3.1 Historical background

Electronic voting in the United States has a complex and varied history, with different jurisdictions adopting different e-voting technologies at different times. Several types of e-voting are used in the U.S. today, including DRE voting machines, optical scan systems and hybrid systems that combine electronic and paper-based components. Nearly all ballots in the U.S. are currently counted with some assistance of computers.[112]

Before the widespread use of electronic voting systems, many jurisdictions in the United States used mechanical lever machines for voting. These devices are considered an early form of automated voting technology, but they were purely mechanical and did not incorporate electronic components. In the latter half of the 20th century, this was followed by voting via punch cards. In this system, voters used a stylus to punch a hole into a pre-printed, machine-readable ballot, with each hole representing a candidate or choice. At the end of election day, the ballots were counted using a card reader, providing quick election results. However, their propensity to cause invalid or incorrect votes because of inaccurate punches led to the early elimination of the punch-card system.

In the early 2000s, in many states punch cards and lever-based voting systems were replaced by DRE voting machines (typically without a paper trail): about a third of all votes were cast on DRE machines in the period 2006 to 2016.[113] But the widespread adoption of DRE voting machines led to controversies and security concerns of their own. Critics raised issues regarding the lack of a voter-verified paper audit trail.[114] There were also concerns about the vulnerability of DRE machines to hacking, tampering, or technical malfunctions that could potentially impact election outcomes.

The 2016 election cycle was a wake-up call in this reagrd. The Senate Intelligence Committee revealed that the Russian government had targeted election systems in all 50 states.[115] In its report, the committee described 'an unprecedented level of activity against state election infrastructure' intended largely to search for vulnerabilities in the security of the election systems.[116] Even though, according to the report, Russian actors were in a position to delete or change voter data in some states, the committee found no evidence that they actually did.[117] Regardless, the mere discovery of Russian interference already has had an undermining effect on the public confidence in U.S. democratic institutions and voting processes.[118]

The growing concerns about foreign interference in elections led to a rapid decrease in DRE voting machines in subsequent years. In 2024, DREs are deployed in the lowest numbers since their introduction to the U.S. market – most states replaced the DRE systems with ballot marking devices.[119] And while some smaller jurisdictions count the paper ballots also by hand, a large majority is electronically counted using optical scanners.[120] After filling in their choice, ballots are scanned, either at the polling place or later at a central location.[121] The scanner translates the mark made on the ballot into digital data to aggregate and tally the total election result.

---

112 ´Voting Technology´, electionlab.mit.edu 21 April 2023.
113 M. Zdun, ´Machine Politics: How America casts and counts its votes', reuters.com 23 August 2022.
114 See e.g.: D.L. Dill, B. Schneier & B. Simons, 'Voting and Technology: Who Gets to Count Your Vote?', Communications of the ACM 2003/46, no. 8. dl.acm.org
115 D.E. Sanger & C. Edmondson, 'Russia Targeted Election Systems in All 50 States, Report Finds', nytimes.com 25 July 2019.
116 Ibid.
117 'Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election', intelligence.senate.gov, p. 22.
118 Ibid, p. 5.
119 See: verifiedvoting.org
120 Ibid.
121 'Voting Equipment', verifiedvoting.org

4.3.2 Critique and controversies

One lawsuit in Georgia illustrates the problematic nature of using EVMs. In this state, a long-running lawsuit (Curling v. Raffensperger) relates to the permissibility of the ballot marking device used there, the Dominion ImageCast X.[122] Georgia is a key swing-state and was considered one of the vital battlegrounds in deciding the 2024 election.[123] In most of the U.S., voters mark their ballots by hand, while BMDs like the Dominion ImageCast X are used for voters with certain disabilities. Georgia, by contrast, is one of only two states casting their vote with a BMD.[124]

The plaintiffs, an election integrity NGO and a handful of Georgia voters, are urging the state to abandon the existing e-voting system and return to using hand-marked paper ballots.[125] They argue that Georgia's system is so vulnerable and susceptible to hacking and errors that it infringes on the constitutional rights of voters.[126] The system concerned is a touch-screen device that allows voters to select their ballots on-screen and print them to an attached laser printer.[127] The printed ballot consists of a QR code and a human-readable text, but the votes are counted using the QR code.[128]

This constitutes a serious design flaw. The voter cannot verify whether the QR code contains the same information as the text.[129] Ultimately, the information in the barcode is what counts, as many scanners will only be able to scan the QR code when tabulating the results, not the human-readable vote. There are examples of elections where a hacked or misconfigured BMD printed votes where the barcode and the human-readable portion didn't correspond.[130] Experts therefore argue that barcodes should not be used to encode votes. Instead, they argue the vote should be marked on paper in human-readable form only.[131]

University of Michigan computer scientist Alex Halderman was consulted as an expert witness in the Curling v. Raffensperger court case. In his security analysis he identified several serious vulnerabilities in the Dominion voting equipment that can be exploited to subvert all of its security mechanisms.[132] "The most critical problem we found," Halderman wrote, is a "vulnerability that can be exploited to spread malware from a county's central election management system to every ballot-marking device in the jurisdiction."[133] This makes it possible to perform large-scale attacks voting equipment, without physical access to each machine.[134]

More importantly, Halderman notes in his report that "even if such an attack never comes, the fact that Georgia's BMDs are so vulnerable is all but certain to be exploited by partisan actors to suppress voter participation and cast doubt on the legitimacy of election results."[135] This is, unfortunately, not an imaginary concern, as we will see.

---

122 US District Court for the Northern District of Georgia, Civil Action N. 1:17-CV-2989-AT (Curling v. Raffensperger). epic.org.
123 T. Pratt, 'Georgians may vote with pen and paper after years of debate and Trump associates' hacking', theguardian.com 9 January 2024.
124 J.A. Halderman, ' Security Analysis of the Dominion ImageCast X', freedom-to-tinker.com 14 June 2023.
125 J.C. Timm, 'Georgia's controversial electronic voting machines face their biggest test yet', nbcnews.com 1 February 2024.
126 J.A. Halderman, 'Security Analysis of Georgia's ImageCast X Ballot Marking Devices: Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al.' 1 July 2021, p. 4.
127 Idem, p. 9.
128 K. Brumback, 'Critics blast Georgia's plan to delay software updates on its voting machines', apnews.com 15 June 2023.
129 A. Appel, 'Suggested Principles for State Statutes Regarding Ballot Marking and Vote Tabulation', freedom-to-tinker.com 18 March 2024.
130 K. Skoglund, 'Election Problems in Northampton County, PA in November 2023', securiosa.com 15 November 2023.
131 A. Appel, 'Suggested Principles for State Statutes Regarding Ballot Marking and Vote Tabulation', freedom-to-tinker.com 18 March 2024.
132 J.A. Halderman, 'Security Analysis of Georgia's ImageCast X Ballot Marking Devices: Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al.' 1 July 2021, p. 9.
133 J.A. Halderman, ' Security Analysis of the Dominion ImageCast X', freedom-to-tinker.com 14 June 2023.
134 Ibid.
135 J.A. Halderman, 'Security Analysis of Georgia's ImageCast X Ballot Marking Devices: Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al.' 1 July 2021, p. 8.

4.3.3 U.S.'s 'stolen' elections of 2020

Like his Brazilian counterpart Bolsonaro, Donald Trump has a longstanding history of casting doubt regarding the integrity of the U.S. election process and reliability of e-voting systems, even before he entered politics. On election day in 2012, when Barack Obama was re-elected for a second presidential term, Trump tweeted: "Pay close attention to the machines, don't let your vote be stolen".[136] And back in 2016 when Trump first ran for president, he already declared that the election was 'rigged'; after winning the election, Trump still refused to accept that he lost the popular vote, insisting that more than 3 million illegal votes were cast against him.[137] In the 2018 midterm elections, again he went on to make allegations of 'electoral corruption' and votes appearing 'out of the wilderness'.[138]

With election denial claims by now being a key part of his political campaigns, Trump went into the 2020 elections claiming that "the only way we're going to lose this election is if the election is rigged".[139] By sowing seeds of mistrust in the electoral process in advance of election day, Trump primed his supporters to expect fraud, on which he could then blame any potential electoral defeat. Ultimately, only 22% believed that the election would be 'free and fair'.[140] After election day, while votes were being tallied, thousands of protesters marched and rallied across U.S. cities, calling on officials to 'count every vote'.[141] In several cities, groups of pro-Trump protesters, some of them armed with guns, crowded outside vote-counting centres chanting 'stop the count'.[142]

After officially losing the 2020 elections to Joe Biden, Trump's claims of widespread electoral fraud and rigged voting machines that supposedly cost him his victory became more frequent. He never accepted the results of the election and instead filed over 60 unsuccessful lawsuits in an attempt to overturn the outcome.[143] He actively called on his followers to take to the streets through messages such as: "This Fake Election can no longer stand. Get moving Republicans."[144] Driven by these theories of voting fraud, post-election protest emerged throughout the country in the two months after election day.

Trumps inciting rhetoric about a rigged election reached its climax when a mob of his supporters forcibly stormed the U.S. Capitol on January 6, 2021, after Trump addressed them at a political rally in front of the White House. In his speech he urged the crowd to ´fight like hell´ and to ´stop the steal´ in an effort to stop the Congress from certifying the 2020 election results.[145] Approximately 10,000 people came onto Capitol grounds, at least 2,000 entered the Capitol building.[146] Five people died and 150 police officers suffered injuries.[147]

Just hours after the insurrection at the Capitol ended, Congress reconvened to confirm president-elect Biden's victory. Nearly 150 Republican members of U.S. Congress objected against certification and instead voted to question and overturn the 2020 election results in one or more U.S. states.[148] This didn't stop Biden´s election from being certified, but the objections show that the election denial-movement had taken hold, not only among the American people, but in Congress as well.

---

136 D.J. Trump, twitter.com 6 November 2012.
137 A. Seipel, 'Trump Makes Unfounded Claim That 'Millions' Voted Illegally For Clinton', npr.org 27 November 2016.
138 H. Yen & C. Rugaber, 'AP Fact Check: Trump's rhetoric on voter fraud is misleading', apnews.com 12 November 2018.
139 G. Sargent, 'Trump just repeated his ugliest claim about the election. Why isn't it bigger news?', washingtonpost.com 15 September 2020.
140 Yahoo News/YouGov poll, docs.cdn.yougov.com September 2020, p. 55.
141 M. Singh, ''Count every vote': protesters take to streets across US as ballots tallied', theguardian.com 5 November 2020.
142 'Stop the vote' and 'count the votes', say protesting Trump supporters', theguardian.com.
143 W. Cummings, J. Garrison & J. Sergent, ' By the numbers: President Donald Trump's failed efforts to overturn the election', eu.usatoday.com 6 January 2021.
144 D.J. Trump, twitter.com 15 December 2020.
145 T. Westphal, 'Violence and the 2020 General Election', Stanford-MIT Healthy Elections Project, web.mit.edu 10 March 2021, p. 4.
146 O. Rubin, A. Mallin & W. Steakin, '7 hours, 700 arrests, 1 year later: The Jan. 6 Capitol attack, by the numbers', abc7.com 6 January 2022.
147 C. Cameron, 'These Are the People Who Died in Connection with the Capitol Riot', nytimes.com 5 January 2022.
148 C. Canipe & J. Lange, 'The Republicans who voted to overturn the election', reuters.com 4 February 2021.

These kinds of developments seriously threatens American's faith in the machinery of democracy. A poll conducted by ABC and Ipsos after the events of January 6, 2021, showed that 41% of the American public is not confident in the integrity of the U.S. election system.[149] Almost one third of the respondents found that Joe Biden's victory in the 2020 presidential election was not legitimate.[150]

In the run-up to the 2024 elections, the Brennan Center for Justice identified 14 different tactics deployed throughout the 2022 midterms-cycle.[151] Among these are 'discrediting voting machines' and 'tampering with sensitive voting data and equipment'. Trump and its allies in their 2024 election campaign regularly claimed that EVMs could not be trusted.[152] After Trump won the election, his campaign went silent.[153] Meanwhile, computer scientists after the elections urged Harris' campaign to ask for a recount in some states using EVMs to ensure election verification.[154]

In 2016, foreign cyberattacks and influence campaigns were a main concern. Today, the rise of a large group of people denying the outcome of the elections, stemming from efforts to fuel distrust in U.S. elections, put democracy at risk. The aftermath of the 2020 U.S. elections and 2022 Brazilian elections demonstrated how discrediting aspects of the electoral process can trigger an uprising with life-threatening consequences. It is therefore key to explore how the voting process can be designed in a way that respects human rights and ensures that people have trust in its outcome.

149 ABC News/Ipsos Poll, ipsos.com December 2021.
150 Ibid.
151 L. Miller & W.R. Weiser, 'The Election Deniers' Playbook for 2024', Brennan Center for Justice, brennancenter.org 3 May 2023.
152 See for example D. Hakim, N. Corasaniti & A Berzon, Trump's Allies Revive Debunked Voting Machine Theories, NY Times 23 October 2024.
153 S.A. Thompson, J. Rutenberg & S.L. Myers, After Trump Took the Lead, Election Deniers Went Suddenly Silent, NY Times 6 November 2024.
154 See letter to VP Harris, 13 November 2024, freespeechforpeople.org

5 Conclusion: paper for now is the only technology compatible with human rights requirements

International human rights law imposes an obligation for countries to hold 'genuine' elections that reflect the free will of the voters. Transparency is one of the key elements to ensure that elections are genuine – voters and observers must be able to verify that the results of the election represent the will of the people. Not only is this required by human rights instruments, it is also important for ensuring stable transitions of power.

As we discussed, a grave concern with e-voting technologies is their lack of transparency: electronic voting and counting technologies are in essence 'black box'-technologies. It is not sufficient to merely observe what is happening during the casting of the vote. This is even further complicated by the requirement that votes remain secret. Not the voters, nor the election officials or poll workers can fully understand the internal mechanics of EVMs used during voting.

As a result, the public necessarily relies on trust in others, often indirectly chosen by those in power: EVM vendors, their employees, auditors, and other people who may have access to the machines.[155] But elections are at the core intended to replace those in power. So there is an inherent tension between using EVMs and organising genuine elections.

Furthermore, this trust in the outcome of elections is highly fragile – it takes only a number of allegations of fraud or irregularities to undermine this.[156] And, as noted above, the problem is that these allegations cannot be refuted conclusively either.[157] So while it is very well possible that every vote cast on an EVM is accurately recorded and counted, people questioning those results will remain as long as EVMs are used in elections. We have also seen how this played out in the 2020 U.S. elections and the 2022 Brazilian elections.

This means that, when it comes to elections, blind trust in technology is simply not an option: voters and candidates have the right to ensure that elections are genuine, implying they must be done using technologies you can trust. At present, the only way of achieving this level of trust is by using paper, counted by hand. Paper voting for now is the only technology which is fully verifiable and leaves a clear audit trail.

And while it is true that no system is perfect, the process which relies solely on hand-marked and hand-counted ballots generally manages to reach a high level of accuracy and reliability, with low risks of large-scale fraud. The risk that someone is able to commit fraud on a statistically significant scale in a paper-based election is small, given that it requires an extreme level of collusion and secrecy among those doing the counting – it is at any rate much smaller than the risk of error or fraud in EVMs.

Put simply: the right to vote means the right to inspect your vote, which also allows you to trust your vote. For now, paper-based voting is the only way to ensure this.

---

155 D.L. Dill, B. Schneier & B. Simons, 'Voting and Technology: Who Gets to Count Your Vote?', Communications of the ACM 2003/46, no. 8, p. 29.

156 International Foundation for Electoral Systems (IFES) & National Democratic Institute for International Affairs (NDI), Implementing and Overseeing Electronic Voting and Counting Technologies, Washington 2013, p. 57.

157 J. Blanc, 'Electronic Voting', in: International Foundation for Electoral Systems, Challenging the Norms and Standards of Election Administration, IFES 2007, p. 15.

IViR - Institute for Information Law
P.O. Box 15514, 1001 NA Amsterdam, the Netherlands

https://www.ivir.nl/