Digital technology in elections
Efficiency versus credibility?

SUMMARY

Digital technology brings greater efficiency in many walks of life, and elections are no exception. Online databases hugely facilitate the task of creating and managing accurate and up-to-date electoral rolls. In less developed countries, whose citizens often lack reliable identity documents, biometric technology can help to identify voters, thus preventing fraud in the form of multiple voting.

However, for some aspects of election management, digitalisation is more controversial. Electronic voting machines count votes quickly and accurately. First used in the United States, they have spread to several Latin American and Asian countries. However, the intangible nature of digital processes makes detecting tampering more difficult; as a result, most European countries are sticking to tried-and-trusted conventional paper ballots.

Even more controversial is the idea of internet voting. On the one hand, allowing citizens the convenience of casting their vote online without the need to visit polling stations could help to reverse a worrying decline in voter turnout across the world. On the other hand, current technology does not allow internet voting systems to be fully secured against hackers, a major concern given the growing sophistication of cyber-attacks (for example, from Russia). To date, only Estonia gives all voters the option of online voting in national elections.

In this Briefing

- Benefits of digital technology in elections
- Standards for digital technology in elections
- Problems and solutions for electoral technology
- Technological options for electronic voting

In many countries, voting machines have replaced the traditional paper ballot.
Benefits of digital technology in elections

Compared to traditional paper-based procedures, digital technology offers multiple benefits at all stages of elections, from registering voters to counting ballots.

**Voter registration:** accurate voter registers are vital to enabling all eligible persons to exercise their right to vote and eliminating fraud. Digital technology considerably facilitates the process of creating registers. Most EU countries extract data from population registers to generate an electoral roll. In countries where electoral rolls are created from scratch, technology can also help; for example, voters register in Australia via an online form, whereas Tanzanians fill out a machine-readable paper form that is then fed into a scanner.

The difficulty of updating and cross-checking paper-based electoral rolls heightens the risk of including deceased voters or multiple records of the same person, creating opportunities for electoral fraud. By contrast, digital registers are more manageable.

Creating accurate voter registers is particularly difficult in countries where citizens lack identification documents – as many as 40% of those eligible to vote in low-income countries. The lack of a reliable method of checking identity allows many people to register more than once – in the Democratic Republic of the Congo (DRC), over 700,000 persons (1% of the total population) were found to have done so ahead of the 2011 elections. To prevent this, 45 countries (mostly in Africa) use fingerprint scanning. Paradoxically, some of the least developed countries in the world have become leaders in the use of biometric technology in elections, precisely because of the lack of reliable identity documents and population registers; Somaliland (see box) has even used iris scanning.

**Voter identity verification:** on the day of the vote, election workers need to check voter identity against the electoral roll. This becomes much easier if polling stations have access to accurate and up-to-date voter information in an online register, used in Norway, Mongolia and 17 other countries.

In many African countries, a lack of reliable identity documents is a problem not only at voter registration but on election day itself. Guinea, the DRC and Liberia are among several countries which deal with this issue by issuing voters with a special card when they register, which they can use to identify themselves at polling stations (a side benefit is that the cards can also be used as an identity document (ID) in other administrative procedures). In Kenya, Ghana or Nigeria, the card includes a fingerprint that is scanned at the polling station to check that the identity of the voter matches that of the cardholder. Altogether, 45 countries use biometric data for identification purposes, which can include fingerprints, facial photographs (in India) and signatures.

Multiple voting is a serious problem in many countries (for example Russia, where the practice is known as ‘carousel voting’). To prevent this, many countries (such as Malaysia) mark voters’ fingers with ink, which is not however completely indelible. Inking also makes abstainers conspicuous – a problem in countries where they may come under pressure from authorities keen to legitimise rigged elections by maximising turnout (as in Cambodia’s 2018 parliamentary election). Conversely, in 2014, some Afghan voters had their fingers chopped off for failing to comply with a Taliban call to boycott elections. Compared to inking, biometric identification provides a secure and discreet means of preventing multiple voting.

**Vote casting:** illiteracy increases the frequency of invalid votes, as voters cannot read ballot papers or instructions on how to mark them. For example, in India (where 31% of adults are illiterate), large
numbers of ballots were previously discarded, due to mistakes such as not marking the ballot in the right place or in more than one place; in many elections the number of discarded votes was higher than the margin of victory, casting doubt on the validity of the result. User-friendly electronic voting machines introduced in 2003 have eliminated this problem; voters now only need to activate a button next to the relevant party logo, widely publicised during election campaigns. In systems where voters fill in and scan paper ballots rather than pressing a button on a machine, the scanner can be programmed to accept only correctly completed ballots.

Electronic voting systems can include safeguards against ballot box stuffing, formerly a common practice in remote parts of India, where criminals or political activists seized control of polling stations to stuff boxes with ballots for a favoured candidate. Voting machines, which are programmed to record a maximum of five votes per minute, have made such practices much harder, as stuffing takes an impractically long time, even if the machines fall into the wrong hands.

Electronic voting machines are often more accessible for disabled voters. In the United States, visually impaired voters can use an audio interface, while those with paralysed limbs can select candidates from a screen using head movements.

Vote counting: technology enables faster vote counting. In India, counting the results from voting machines takes between two and three hours per constituency, including the time needed for checks; which previously took days for paper votes. It also reduces the scope for human error and saves money through recruiting fewer poll workers.

Results transmission and tabulation are the processes of sending the results of the vote count from polling stations to a central polling office and aggregating them to give total results (at constituency or national level). With paper-based processes, collecting and calculating results from thousands of polling stations country-wide is often the slowest part of the process; with digital technology, results can be transmitted electronically (for example, over the internet or by mobile phone) and aggregated by computer, allowing at least preliminary results to be announced quickly (most countries also carry out paper checks before the final outcome is confirmed).

Standards for digital technology in elections

Like any other election, polls carried out with the help of digital technologies must comply with the general principles set out in Article 25 of the UN’s 1966 International Covenant on Civil and Political Rights: universal and equal suffrage and secrecy of the ballot. International standards addressing the specific characteristics of electronic voting and other voting technology do not yet exist. However, the Council of Europe’s recommendation on standards for e-voting (adopted in 2004, updated in 2017) is a useful reference. Among other things, it recommends that:

- voters should be reliably identified;
- voter interfaces should be easy to understand and use for all voters;
- voters should have the chance to confirm their vote before casting it;
- after casting their vote, voters should be able to check that it has been correctly cast;
- voting should be anonymous;
- all aspects of the vote must be fully transparent;
- electronic voting systems must be tested and certified by an independent body.

With regard to personal data held in voter registers, standards vary from one country to another; US and Canadian standards are more liberal, enabling political parties to conduct targeted campaigns based on data, whereas most European countries have greater restrictions on access to voter data.

Problems and solutions for electoral technology

Nearly all countries now use digital technology for at least some aspects of election management. Creating and managing voter registers, as well as transmitting and tabulating results have been digitalised in nearly all countries.
Conversely, electronic vote-casting has been less universally adopted; in developing democracies, where elections have often been marred by fraud, it is – rightly or wrongly – often seen as a means of ensuring a more credible poll. As a result, voting machines and other electronic voting systems are becoming increasingly widespread in Latin America, as well as in the Middle and Far East. In contrast, European countries are more reticent, preferring tried-and-trusted traditional methods, with a manual count of paper ballots to experimenting with potentially unreliable new technologies.

Main concerns

Reliability

Although it reduces the scope for human error, digital technology is not infallible. Biometric voter identification is a case in point. Venezuela uses digital fingerprint checking, in addition to photo ID cards, to authenticate voters; in 11% of cases, the system was unable to match voters' fingerprints with those recorded in the electoral roll. After experiencing a similar failure rate in trials, Pakistan decided not to use fingerprint scanning in the 2018 general elections, despite its success in identifying thousands of fraudulent multiple votes. Iris scanning is a more reliable biometric identification method, but it is also more expensive, and to date has only been used in Somaliland. Technology can also fail at other stages of the process. For example, in Kenya's August 2017 poll, electronic transmission software malfunctioned in many parts of the country, delaying results and raising suspicions of fraud that ultimately led to elections being annulled.

Protection from electoral fraud

When electoral authorities are corrupt or negligent, digital technology does not provide an instant fix against fraud. In Venezuela's 2017 election, for example, turnout was allegedly overstated by at least one million votes (out of a population of 32 million). In the DRC in 2011, over 700,000 voters were able to register twice (see above); when election authorities' failure to carry out a timely audit meant that the electoral roll could not be amended in time for elections in the same year.

Far from preventing electoral fraud, digitalisation could even facilitate it in some cases. This particularly applies to electronic voting machines. Critics of such devices point out that, with paper ballots, large-scale physical tampering can easily be spotted by election observers, provided they have reasonably unrestricted access to polling stations. In Russia's 2011 parliamentary elections, election officials were caught on camera apparently stuffing ballot boxes in an effort to swing the vote in favour of the ruling United Russia party. In contrast, electronic manipulation of invisible digital processes inside voting machines can be much harder to detect, especially when there is no back-up system recording the vote on paper. For this reason, opposition politicians in the DRC are suspicious of the country's plan to introduce electronic voting machines for the December 2018 presidential election.

Electronic voting systems are also vulnerable to external attacks; attempts by Kremlin-linked hackers to break into electoral computers from over 20 US states during the 2016 presidential election have raised awareness of this problem. Admittedly, proven cases of electronic tampering are rare, but the fact that they are seldom detected does not mean that they do not occur.

Civil society activists have repeatedly demonstrated the vulnerability of electronic voting systems. In 2006, the Dutch 'We do not trust voting computers' movement refuted manufacturer's claims that voting machines were tamper-proof by reprogramming them to play chess. The following year, studies carried out in California and Ohio on machines from a range of manufacturers found serious security flaws. In Indian voting machines, vote-recording and vote-counting functions are hard-wired into circuits, instead of being run on software, thereby preventing reprogramming; nevertheless, in 2010, hackers were able to illicitly obtain and physically modify an Indian machine to be controlled from a mobile phone. Such experiments show that, once hackers understand how voting machines work, they can develop compromising procedures, requiring a few minutes of
physical access, perhaps where machines are stored between elections, or even in the privacy of the voting booth. Attacks of this nature may be virtually undetectable, even by election staff or observers with specialist training; for example, software installed by hackers on voting machines can be programmed to erase itself after modifying the vote.

Computer scientists have criticised the poor quality of electronic voting software on many machines, which makes them vulnerable to such attacks. However, they also acknowledge that the complexity of such programmes, which typically contain hundreds of thousands of lines of code, make elimination of all security flaws virtually impossible. Physical safeguards (such as tamper-proof seals on voting machines) are also not infallible.

Unaddressed security concerns have led several countries to abandon electronic voting. In 2007, the Netherlands decided to return to paper ballots after a decade of using voting machines, one year after the Irish government dropped its electronic voting project, despite having spent over €50 million on equipment.

Voting machines are not the only vulnerability. Tabulation processes have also been targeted by hackers, for example in South Africa's 1994 election. Election officials had to tabulate results manually after it was found that, in an apparent attempt to thwart an electoral victory by Nelson Mandela's African National Congress, the computer processing the votes had been set to transfer votes to three right-wing parties.

**Auditability of electronic voting**

When the only record of a vote is digital, there is a risk of it being lost irretrievably, due to hacking, as explained in the previous section, or malfunction (for example, in a 2008 California election where a software bug deleted 200 votes). For this reason, back-up systems providing a physical record that can be checked whenever there are doubts as to the digitally recorded result are useful.

Paper voting records can take the form of a printout generated by voting machines after the vote has been cast (known as a voter-verifiable paper audit trail, VVPAT), or a paper ballot completed by the voter and read by a scanner. Arguably, combined electronic and paper-based vote recording is more secure than purely paper-based or electronic recording, as both systems would have to be compromised simultaneously. For this reason, VVPATs in electronic voting systems are recommended by the Council of Europe, and compulsory in 32 US states and the District of Columbia.

However, despite the obvious security benefits of electronic systems generating an auditable paper trail, they are far from being a universal standard. Paperless systems are still used by a quarter of US voters, in Brazil, Namibia and India, among other reasons, due to their lower cost (however, in 2017 India announced plans to add a VVPAT to its voting machines).

**Verifiability**

Related to auditability is the concept of verifiability, meaning that voting processes can be checked not only by election workers and monitors, but also by voters themselves. Traditional voting procedures are partially verifiable; voters can easily see that they have correctly marked their ballot papers and fed them into the ballot box. Given that boxes are typically locked, they can also feel reasonably confident that their ballots are secure until boxes are emptied for counting. In contrast, voting computers are 'black boxes'; ordinary voters do not understand how they work, and therefore have no way of knowing whether their vote has been correctly recorded. On this basis, Germany's constitutional court ruled in 2009 that the type of voting machine in use at the time was not sufficiently transparent; since then, the country has returned to using paper ballots.

Electronic systems ensuring a paper trail offer more verifiability than purely paperless systems; although the primary means of recording the vote is still electronic, voters at least know that election workers will check paper records in the event results are challenged. However, for developers of new electronic voting technology, the ultimate goal is an end-to-end verifiable voting (E2EVV) system.
Such systems would eliminate electoral fraud by enabling voters to verify not only that their vote is cast as intended, but also correctly recorded and counted – something that neither traditional paper ballots nor electronic systems are currently capable of delivering. In theory, the simplest way to achieve such a goal would be to publish voters’ names and their choices, but this would contradict the principle of ballot secrecy. Scantegrity, developed by the Massachusetts Institute of Technology, is one of several systems developed to avoid this problem; it replaces voter names and choices with randomly allocated codes, which voters are allowed to take home if they wish. Once all votes are counted, voters can use their codes to check online that their vote was recorded correctly; moreover, anyone can check the complete tally to ensure that it is mathematically correct. Developers of the system calculate that even if only 2% of voters take advantage of the opportunity to verify the vote that is enough to foil attempted electoral fraud.

Scantegrity has been used in binding political elections (in 2009 and 2011, municipal elections in the Maryland city of Takoma Park); however, a study found that the complexity of this and other E2EVV systems makes them difficult for voters to use, and adoption is slow.

Testing and certification

Given their vulnerability to electoral fraud, new technology should be thoroughly tested before being certified for use. The Council of Europe recommends that tests be carried out not only by manufacturers but also by an independent and competent body. In the United States, such tests are run by independent laboratories accredited by the election assistance commission. Unfortunately, the effectiveness and impartiality of such tests have often been questioned by researchers, who found serious security flaws in equipment that had been certified for use.

Tests can be more effective when they bring in outside persons, such as activists who are keen to highlight flaws overlooked by official testing bodies. In 2010, the US District of Columbia invited the public to test its proposed internet voting system; the system was abandoned after being infiltrated by hackers. India’s electoral authorities were less receptive to criticism, repeatedly and categorically rejecting claims of flaws in voting machines; in 2010, an activist who proved otherwise was arrested for theft. In an attempt at more openness, in June 2017, India’s electoral commission invited computer experts to attempt to break into its machines; however, sceptics complained that conditions at the ‘hackathon’ were too restrictive to allow real testing.

Trust

Digital technology often meets resistance when it fails to win voter and political party trust. In Venezuela, one-quarter of voters suspected that fingerprinting checking devices could be used by authorities to trace how they had voted; similar concerns were expressed in Armenia.

In many countries, electronic voting machines’ failure to win trust has led to civil society resistance and the abandon of electronic voting – particularly in European countries such as Ireland, the Netherlands and Germany, but also in Paraguay.

Claims of technological malfunction are often politically motivated – for example in India, where losing parties have a tendency to blame voting machines for poor results. Whether or not such accusations are unfounded, they can seriously undermine voters’ trust in democratic processes. Kenya’s August 2017 elections had to be annulled after delayed results led to suspicions of fraud.

For digital technology to win essential voter trust, the conditions outlined in the preceding paragraphs – adequate security, transparent checks and testing – should be met. Election monitors should be given access to technical systems used at all stages of the electoral process, from voter registration through to tabulation. In addition, to give voters time to get used to electronic voting, the Council of Europe recommends introduction ‘in a gradual and progressive manner’. Indeed, this was the approach followed in Belgium, which in 1991 tried out voting machines in two constituencies before gradually adding more locations.
Practical considerations

Cost efficiency

Digitalisation entails multiple costs: purchasing equipment, training staff, updating software to deal with evolving cyber-threats, and secure equipment storage between elections. In countries with high labour costs, such expenditure can be offset by personnel savings, but in developing countries, the outlay may never be recovered. For example, in 2006, the DRC spent over US$40 million on biometric registration kits. With such sums at stake, there is significant scope for corrupt practices, for example in the DRC’s procurement of registration equipment. Furthermore, given that funding is limited, heavy IT expenditure diverts resources that could perhaps be better used to deal with fundamental challenges faced by many developing countries, such as election-related violence and vote buying.

Despite the costs, digital technology can be a worthwhile investment for developing countries. By eliminating multiple voting, biometric identification can help to secure acceptance of the results and reduce the risk of post-election violence (for example, in Nigeria’s 2015 elections).

Logistical constraints in developing countries

In developing countries, electoral equipment is transported and used in hot and dusty conditions, by voters who are often illiterate and have limited experience of electronic devices. To deal with such problems, Indian voting machines have a simple and robust design, and an easy-to-use interface; they are also cheap to manufacture, compared to the more sophisticated devices used in Europe and North America. For these reasons, Indian-made machines are also used in Namibia, which became the first African country to adopt electronic voting in 2014.

Given erratic power supplies and internet connections, battery-powered devices which work offline are the norm – for example, India’s voting machines or the authentication equipment used in several African countries (e.g. Nigeria). In the majority of developing countries with digital electoral rolls (for example: India, Brazil, Nigeria), polling stations use an offline list that works without an internet connection, rather than accessing a central online database. Most also have printed lists, in case electronic equipment fails. The value of having a paper back-up was demonstrated in Kenya’s 2013 election, when electronic voter identification devices failed to work in most polling stations.

Technological options for electronic voting

Optical scan

Optical scan technology was first used in 1962, in California. In the USA, over half of voters now fill out their vote by pen on a machine-readable paper ballot and insert them into a secure ballot box. The vote is read by an optical scanner, either before the paper is fed into the ballot box, or afterwards, when the box is opened by election workers.

Optical scanning has several advantages. For voters, the procedure is very similar to the conventional method of filling out a paper ballot and putting it in a secure box; it is therefore easy to use, and may also seem more trustworthy. Paper ballots are kept for possible recounts in case the electronically recorded result is questioned.

Direct recorded electronic

Also pioneered in the USA (where they were first used in 1975), direct recorded electronic (DRE) voting machines have an interface – typically a touch screen, or physical buttons – on which voters record their votes. The absence of paper ballots simplifies electoral organisation, as there is no need to print and transport them in advance. The interface can offer options (such as different languages or font sizes) making it easier to use for certain voters. DRE machines are globally the most widespread option, used in the United States, India, Brazil, France and Belgium among other
countries. However, the lack of an auditable hard-copy record has undermined the credibility of some DRE machines; in the United States, their use has declined from 38% coverage of the electorate in 2006, to around one quarter in 2016.

To remedy this defect, many modern DRE devices also print voter choices (often onto a paper roll, of the type used in cash registers). However, this is not entirely satisfactory: voting information is printed in small letters, making it difficult for voters (and election officials, in the event of a recount) to read; the printed record retains votes in the order in which they were cast, theoretically enabling identification of voters; and few voters bother to check that their vote has been correctly recorded, giving electoral fraud a better chance of passing undetected.

Internet voting

Internet voting (sometimes referred to as i-voting, as distinct from the broader concept of e-voting, which refers to electronic vote counting and recording) is a much more radical departure from traditional procedures than either of the two above options, as it allows electors to vote from home, without having to visit a polling station. For this reason, it presents specific benefits and risks, and remains highly controversial; several countries have piloted online voting, but Estonia is the only country to use it for all categories of voter in national elections.

Online voting potentially improves voter turnout

Since 1980, the average percentage of citizens turning out to vote in national parliamentary elections across the world has declined from 76% to 66%. In EU countries, a similar decline can be seen in turnout for elections to the European Parliament. Insofar as they reflect scepticism towards democratic institutions, these trends are worrying. In this context, internet voting could, at least in theory, help to boost turnout by making voting more convenient for those who find it difficult to get to a polling station. In many countries (for example, the USA), young people are particularly reluctant to vote and online voting might be a more appealing option for them.

Whether this happens in practice is unclear, as limited data are available. In Estonia (see Figure 1), the only country to have used this technology at national level over a longer period, i-voting has certainly proved popular. Since 2005, the first time that the technology was used, when just 2% of votes were cast online, the share of i-votes has steadily increased to reach 32% in the most recent local elections (2017). However, the effect on overall turnout is much less clear; participation in 2009 local and European elections rose considerably, but most of the initial gains have since been lost, perhaps suggesting that the ability of i-voting to draw in new voters declines once the novelty effect wears off.

Results from other countries are equally inconclusive. In 2007, the UK trialled i-voting in municipal elections; the percentage of voters choosing to vote online was mostly quite low (as little as 3.4% in one case). Around one quarter of online voters declared that they would not have voted if online voting channels had not been available. However, with only five

Internet voting in Estonia

Estonia is the only country in the world to offer internet voting to all categories of voters in national elections (it is also available for local and European elections). Despite continuing cybersecurity concerns, online voting has become highly popular, representing 32% of votes cast in 2017 local elections.

Estonia offers particularly favourable conditions for i-voting:

- **ID cards** come with a chip and a card reader, making them suitable for online authentication;
- the country (‘e-Stonia’) prides itself on being one of the world’s most advanced digital societies, in which online services are highly trusted and have become the default option for most public and private-sector transactions.

![Figure 1 – i-voting and turnout in Estonia](image)
local councils participating in the trial and a lack of comparable data from a longer period, it is impossible to say whether overall turnout benefited. A 2017 study on Switzerland also failed to find any significant impact.

**Saving money**

In countries such as Switzerland and Estonia where internet voting has been trialled, it has been offered as an alternative rather than a replacement for traditional voting. Expenditure on internet voting systems is therefore additional to polling station operating costs. Conversely, these additional costs can easily be offset: if enough people vote online, fewer staff are needed at polling stations to receive voters and count ballots. In 2007, Estonia’s national electoral committee put the costs of developing and implementing i-voting over four years at just €400 000; it also estimates that in 2017, i-voting saved 11 000 working days; the net cost savings are therefore considerable.³ From a financial point of view, i-voting is a particularly attractive option for countries which hold frequent elections or referenda (such as Switzerland).

**A convenient way of voting**

Internet voting is a convenient solution for voters who are physically unable to reach polling stations. Some US states allow armed forces personnel and overseas voters to vote online. The Australian state of New South Wales allows this option for voters who are out of state on polling day, as well as certain categories of disabled person and those who live more than 20 kilometres from the nearest polling station.

**The main argument against i-voting: security risks**

Despite all the potential advantages, i-voting has made very little headway, mainly due to the risk of hacking. Many personal computers or mobile devices used to vote online are poorly defended; in 2014, an estimated one-third were infected with malware, potentially enabling ill-intentioned persons to spy on voters or worse, vote for them. An even bigger risk is that hackers could attack electoral authorities’ servers to manipulate the results. Even very well-defended systems are not invulnerable: hackers have found security flaws in systems belonging to Google and Microsoft, and even the Pentagon. Although there is no evidence that Estonian internet voting has been compromised, it would be an obvious target for Kremlin-linked hackers. In 2014, cybersecurity experts therefore recommended that Estonia discontinue i-voting, arguing that i-voting could not be made safe. Australia’s electoral authorities have ruled out i-voting for federal elections given the risk of ‘catastrophically compromising our electoral integrity’.

Security objections can also be made against postal voting, used by many countries as a solution for voters unable to vote in person (or even, in the US states of Oregon, Washington and Colorado, as the main voting method). However, while there is a risk of individual postal votes falling into the wrong hands, it would be very difficult for election fraudsters to intercept such large numbers as could be possible with votes sent over the internet.

Advocates of i-voting argue that even if it cannot be made fully secure, risks can at least be reduced to an acceptable level, in the same way as online banking and shopping. However, large-scale electoral fraud has the potential to undermine trust in democracy – a more serious consequence than the economic losses caused by financial fraud. Moreover, it is far more difficult to detect: online bank clients are more likely to notice money missing from their accounts, than any direct impact of their vote being hijacked, and in the absence of a paper back-up, election workers cannot audit the results.

To remedy this defect, since 2013, Estonians can check that their votes have been cast as intended, using E2EVV technology (see above). Voter verification cannot prevent fraud, but it can at least help to detect it. However, there are limitations, critics point out the verification software is not fully secure, and in any case only a small minority of voters (4% in 2017 local elections) bother to check.
Other problems with i-voting

I-voting potentially compromises ballot secrecy, as it is impossible to guarantee that nobody is watching voters as they submit their ballots. It therefore opens the door to voter coercion or even vote buying. To exclude this possibility, Estonia allows citizens to re-cast their votes an unlimited number of times during a seven-day period, or, after the expiry of that period, to override their internet choice by voting in person. Internet voting potentially discriminates against persons who are less comfortable with digital technology or lack access to high-quality internet services. It also removes the traditional symbolism of voters heading for polling stations as a public expression of citizenship. However, neither of these arguments applies where i-voting merely complements rather than replaces voting in person – which is still the preferred option, even in Estonia.

EU position: EU electoral monitoring guidelines emphasise the need for observers to assess the use of technologies such as biometric identification and electronic voting machines – but also acknowledge that a full technical analysis is likely to exceed their capacity.

The EU election observation mission reports vary in their assessments of digital electoral technologies. EU observers in Peru praised the country for its 'largely successful' partial introduction of electronic voting in 2016; however, at the 2017 Kenya election, they were more critical, noting that technology was 'extremely controversial', and emphasising the need for digital systems to be 'tried and tested, secure and publicly accountable'.

European Parliament resolutions of November 2015 on reforming EU electoral law and of March 2017 on e-democracy in the EU recognise the potential of technology to enhance democracy by enabling certain groups (for examples, expatriates or disabled people) to vote, but also insist on the need to prevent fraud and ensure voter secrecy.

ENDNOTES

1 In almost all countries, voters must be registered to be eligible to vote. Registration can be active (citizens have to apply individually to register), or passive (state authorities compile the voter register themselves using civil status records or other public sources).


DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.


Photo credits: © Lisa F. Young / Fotolia.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)
Figure 2 – Countries that use electronic voting (Use of optical scanning or direct recorded electronic technology to record and/or count votes in politically binding elections)

Electronic voting has fallen out of favour in most European countries, but is gaining ground in Latin America, as well as the Middle and Far East.

Several countries have experimented with internet voting, but only Estonia has used it extensively.

Source: International Institute for Democracy and Electoral Assistance, International Foundation for Electoral Systems,