Chapter 3

Overview of Current State of E-Voting Worldwide

Carlos Vegas
eVoting Legal Lab
carlos.vegas@europe.com

Jordi Barrat
eVoting Legal Lab
jordi.barrat@urv.cat

CONTENTS

3.1 Introduction

Several countries are currently using e-voting for elections and referendums and many others are conducting (or have conducted) feasibility studies. This chapter provides a general overview of e-voting implementation worldwide.

An appropriate classification and taxonomy is the very first step for overviews that refer to realities that vary a lot. And e-voting may encompass a wide range of e-enabled tools. As for this chapter, e-voting will include the casting and counting of votes. It is the definition used both by the Office for Democratic Institutions and Human Rights (ODIHR) and by the International Institute for Democracy and Electoral Assistance (IDEA). The term includes "the use of electronic voting systems, ballot scanners and Internet voting" (see p. 4-5 in [245]).

In 2015, the IDEA conducted a survey that intended to know the use of electoral Information and Communication Technologies worldwide (www.idea.int/elections/ict). Regarding e-voting, 19 countries confirmed its use "in politically-binding national elections (elections for public office or direct democracy initiatives),"[1] 16 countries "in politically-binding sub-national elections (e.g. elections for regional legislature or executive office etc.),"[2] four countries "in other elections with EMB participation (e.g., election of trade union leaders, non-binding referendums)"[3] and finally eight countries had abandoned e-voting.[4] Ninety-eight up to 249 countries did not reply to the survey.

This chapter does not intend to cover all cases or provide detailed lists. It will rather focus on some countries that, beyond their size, enable us to highlight particular features. All countries undertake similar and common steps, but each one also has to face legal and sociopolitical contexts that may lead to specific solutions. And such a comparison will provide a complete picture of the challenges that e-voting is facing nowadays worldwide.

The chapter chooses some cases that could be considered international references for either good or bad reasons. We will find good practices, but also negative approaches. At the end, the final outcome aims at being a more nuanced picture of the current challenges of any ongoing e-voting project. Particular features will be used as drivers for completing the whole comparison: the public nature of elections, the civic activism, the interaction between business and elections, the technical obsolescence, the political context and the voter's perception.

Given the table of contents of this book, where most chapters are authored by IT experts, this chapter compensates such an approach by stressing the importance of legal and sociopolitical issues. Any successful e-voting implementation needs a

[1] Armenia, Belgium, Bhutan, Brazil, Ecuador, Estonia, France, India, Mongolia, Namibia, New Zealand, Panama, Peru, Philippines, Russian Federation, Switzerland, UAE, USA and Venezuela

[2] Argentina, Australia, Bangladesh, Belgium, Bhutan, Bulgaria, Canada, India, Japan, Mexico, Mongolia, Peru, Philippines, Russian Federation, Switzerland and USA.

[3] Bolivia, South Korea, Panama and Switzerland.

[4] Netherlands, Kazakhstan, Germany, Finland, Norway, Paraguay, Romania, Ireland. The database also mentions the United Kingdom where e-voting has been piloted.

sound technical background, but it also requires an appropriate legal framework and a proactive society. These three pillars are interdependent and one weak point likely leads to the failure of the e-voting project.

3.2 The Public Nature of Elections

E-voting, actually any sort of e-enabled electoral tool, entails obscurity for a layman and addressing such a barrier has become a challenge for a definitive consolidation of electoral technologies. If compared with paper-based tools, evidence provided by e-enabled ones may be meaningless for a layman, due to their inherent technical complexity. While a paper recount can be understood and monitored by anybody, a computerized recount may provide correct final figures, but the procedure can only be understood by technical experts. Such inherent opacity of e-enabled tools somehow contradicts basic pillars of elections, which always rely on transparency and citizen oversight. And that is why using new technologies for electoral purposes will likely have to address particular concerns that are not present in other areas.

A decision of the German Constitutional Court in 2009 is considered a milestone. It had a direct impact on subsequent legal developments and e-voting implementations, like the Norwegian, the Estonian and the Swiss ones, that intend to provide better tools for election verifiability.

In March 2009 the German Constitutional Court banned voting machines that were in use for federal elections. They were machines supplied by Nedap, a Dutch vendor whose devices have also been implemented in the Netherlands and in France. Beyond other previous lawsuits that had had different outcomes (see p. 186 in [568]), this process was initiated by Ulrich Wiesner and his father regarding the 2005 federal elections. Despite the fact that there had been no major problems during the actual implementation of voting machines, the lawsuit intended to challenge the e-voting procedure as such. Once rejected by the Lower Chamber (Bundestag) as "obvious causeless" (see p. 186 in [568]), the suit ended with an outstanding decision of the German Constitutional Court based on the public nature of elections.

The Court highlighted that voting machines had an inherent shortcoming that was not linked with their actual performance. Even a successful implementation from a technical perspective would not be legally acceptable due to the fact that such devices do not comply with main democratic principles, namely the one that foresees the oversight of electoral procedures by different stakeholders, with no specialized knowledge being required. That is what the German Court called the public nature of elections: "every citizen should have the capacity to reliably monitor and understand, without specific technical knowledge, the central stages of an election" (§109; see also §119, 148 and 149). IT experts normally assume such important tasks as delegates, but the Court did not accept indirect confidence procedures.

The Court (BVerfGe, 2 BvC 3/07, March 3rd 2009) did not reject e-voting means as such. It only examined the Nedap's model and concluded that it did not com-

ply with German constitutional principles, but e-voting remains feasible and legally acceptable in Germany provided the relevant solution takes into account the requirements and conditions set up by the Court.

Anyway, it is worth recalling that such machines did not include a paper trail, which is a component that might meet the Court's requirements. The decision was only based on a given e-voting model and thus future paper-trail implementations might be envisaged provided a previous assessment confirms their compliance with the Court's conditions. Actually the Court implicitly accepts that there could be acceptable measures taken to compensate the lack of publicity and direct citizen involvement (see §123).

Finally, the Court establishes an interesting comparison between e-voting and postal voting. It accepts the latter provided its benefits for the overall electoral system are sound enough, but the Court also assumes that postal voting will likely lessen some guarantees (e.g., the ballot will be handled without the direct supervision of electoral authorities, risk of impersonation). Therefore postal voting is admitted even though it does not comply with normal requirements. It is admitted "with the goal of ... achieving the highest turnout and therefore taking into account the principle of the universal suffrage" (§126).

The Court thinks that Nedap's machines do not provide similar benefits, but there might be other options like, for instance, internet voting (i.e., remote voting from unsupervised environments). Such a system and postal voting pursue the same goal and thus internet voting could benefit from the exceptional rules that the Court applies for voting by mail.

Legally speaking, it is worth recalling that the German Court has an important influence on other jurisdictions worldwide. Its case law is carefully analyzed. Taking into account such premises, other countries, like Norway, Estonia or Switzerland started using e-voting tools with a different approach, which aimed at complying with the public nature of elections.

All of them use internet voting and actually none is able to fully comply with the Court's requirements, since their systems still need specialized knowledge to be monitored, but different innovations enhance transparency and thus a greater independent and external oversight. Such countries are exploring how to provide enough citizen confidence though still requiring the active involvement of computer experts. Moreover, individual verifiability, whose use does not require special knowledge, also started being accepted in some cases.

Norway trialled internet voting in 2011 and 2013, at local and general elections. Voters could cast their ballots on the internet from uncontrolled environments during the advanced voting period. On election day only paper-based voting was possible.

The Norwegian government decided that openness would feature the project and it adopted some decisions that went far away from the normal procedure in other

countries: a procurement based on a competitive dialogue, an open-source license and the so-called return codes.

The supplier (Scytl) was chosen after a competitive dialogue scheme among different companies and the documentation was available online. First, such a procedure "enables the EMB to have a dialogue and gather crucial information from the vendors before the official tendering process starts" (see p. 34 in [580]). Therefore, a competitive dialogue normally leads to a better final decision and it also enables an improved in-house expertise, which still remains a weak point in many countries.

Second, this case of competitive dialogue also improved citizen awareness. The documentation was published and thus anybody could supervise the decision-making process. Moreover, the government and the supplier agreed on a customized open-source license. It read as follows:

"The ... Ministry ... and [the Vendor] hereby grant to you ... the right to copy, modify, inspect, compile, debug and run the software for the sole purpose of testing, reviewing or evaluating the code or the system solely for non-commercial purposes" (see p. 9, excerpt, in [580]).

Such a situation differs a lot from what could be found in other countries and what is still being used nowadays. In 2007, for instance, the Kazakh EMB refused to publish the report issued by the certifying authority, which is something usual (for France and Belgium, see Barrat, [71] and [72]), but surprisingly the criteria with which the compliance should be assessed were not published either (see p. 87 in [331]).

Granting access to such data intends to enhance public confidence on electoral procedures, but it has never been easy to achieve on the grounds that disclosing selected documentation could be detrimental to "le secret industriel et commercial ... [et] compromettre le bon déroulement des élections."[5] That is, for instance, the reasoning provided by the French CADA (Commission d'Accès aux Documents Administratifs). CADA is an advisory body whose mission consists precisely on deciding, in the light of the regulations on the access to public information, which documents can be actually disclosed.

However, as the Norwegian case proves, advanced disclosure policies are being adopted, thereby addressing the problems highlighted by the German Constitutional Court in connection with the public nature of elections.

Finally, regarding Norwegian return codes, a confirmation message (return code) is sent to a second device and its content could be matched with the list of codes that the citizen should have already received before election day. Such a list links each candidature to a given code and the citizen will be able to confirm that the code received afterwards coincides with his/her choice. Therefore, individual verifiability

[5] "the commercial and industrial secrecy ... [and] endanger the correct electoral management." Available at: www.ordinateurs-de-vote.org/IMG/jpg/cada.jpg [November 20th 2015]

is improved. The voter confirms that his/her ballot was cast as intended and recorded as cast.[6]

The Norwegian system had some weak points [543] and return codes did not cover the whole process (i.e., casting, recording, tallying), but the system still remains a fair example of transparency and individual verifiability,[7] which are basic requirements concerning the public nature of elections. Last but not least, it is worth mentioning the positive attitude of the Norwegian government, who always understood that proactivity and openness were minimum preconditions for a successful e-voting project.

Estonia was also aware of e-voting new trends. The Election Act has been amended and, among other changes, it created "the EVC [Electronic Voting Commission] to organize the Internet voting and verify the electronic voting results. The establishment of the EVC formalized the Internet voting management structure and increased accountability and transparency" (see p. 4 in [449]). Moreover, return codes were also included: "verification is done using a separate smart device (mobile phone or tablet), which reads a code displayed on the voter's computer screen upon completion of voting. The mobile device then temporarily displays the voter's choice, enabling the voter to confirm that his/her vote was recorded as cast" (see p. 5-6 in [449]). Despite such innovative measures, some weaknesses were highlighted regarding, for instance, external audits and access to relevant documentation (see p. 6-7 in [449]; see also other pre-election reports, [535]).

Finally, in 2014 Switzerland approved a new regulatory framework that intends to consolidate a so-called second generation of e-voting systems, that is to say, projects that admit full universal and individual verifiability: "Eligible voters will receive codes with their voter identification card that will allow them to check that their ballot is recorded correctly and corresponds to their intention. From 2016, the Federal Chancellery also intends to provide universal verifiability, whereby any person or group can use mathematical means of verification" (see p. 6-7 in [450]).

Unlike in Germany, internet voting is used instead of voting machines by the above mentioned countries and therefore they differ on how to address the public nature of elections. With voting from uncontrolled environments it is not possible to implement some measures that are available for voting machines (paper-trail being the most obvious one). Return codes intend to simulate what a paper trail provides in a controlled environment, but return codes cannot achieve the same degree of universal and individual verifiability.

A Voter Verifiable Paper Audit Trail (VVPAT) entails different legal and managerial problems, namely based on the legal notion of what a vote is, either physical or virtual, and to which extent recounting mechanisms should be applied, but

[6] However, in 2011, a vote was not correctly recorded due to timeframe restrictions [75] and in 2013 a crypto mistake was discovered once the advanced internet-voting period had already started (see p. 8 in [448]).

[7] Universal verifiability is addressed by other means (e.g., disclosure of the source code, zero-knowledge proofs).

VVPAT directly addresses the challenge related to the public nature of elections too. If VVPAT is accepted, specific technical knowledge will not be needed anymore for supervising some key electoral steps. Paper trail machines are used in many countries (e.g., USA [283], Venezuela, Belgium).

In Venezuela, voting machines deliver a VVPAT that the voter has to insert in a traditional ballot box. At the beginning, management issues raised some concerns. Hausmann and Rigobón conducted a statistical analysis on fraud probabilities and concluded that the final outcome "is compatible with the hypothesis that the sample for the audit was randomly chosen *only* among those polling stations whose results had not been tampered with" (emphasis added; see p. 2, translated from Spanish, in [297]).

Despite being statistical (not proven) forecasts, the criticism highlighted a weak point and thus the electoral authorities improved the paper recount of a given percentage of machines. The sorting of polling stations will not be centralized anymore. At the end of election day, each precinct, where there may be several polling stations, will decide which machines will be submitted to a paper recount (see p. 39 in [138]). The solution addresses a potential manipulation, where only pre-selected and thus not tampered machines would be submitted to a paper recount. Random biases are still feasible with the new method, but their implementation is much more difficult.

The percentage of machines being audited increased a lot: 45% in 2005 and 59.32% in 2006. Such a strategy makes no sense from a statistical point of view, but "to extend the audit of closing to all electronic voting centers produced a positive result in the sense of improving the electorate's confidence, as well as that of the political class, in the transparency of the electronic vote and in the correct operation of the voting machines" (see p. 22-23 in [560]). However, there was still room for improvement. For instance, formal guidelines in case of discrepancies did not exist (see p. 42 in [138]).

Regarding Venezuelan e-voting case law, two lawsuits reached the Supreme Court. Both decisions tackled one of VVPAT's weak points, that is to say, the legal notion of what a vote is. A paper recount intends to enhance the overall verifiability, but discrepancies may appear and clear legal provisions should foresee which result prevails: the electronic one, the paper-based one or none (see p. 272 in [381]).

In Belgium, there had been *ticketing* experiences (see p. 8 in [201]) and recent petitions advocating for the reintroduction of VVPAT led to a new system that provides multi-purpose devices, which are able to be electronically counted and manually inspected: "the ... ballot [contains] two parts, a human-readable part and a machine-readable part ... like that, the voter has the opportunity to verify if the vote has been correctly registered; the voting paper would also serve as a VVPAT in the case of a necessary recount" (see p. 205-206 in [566]).

VVPAT introduction in other countries has created interesting disputes. India and Brazil may be used as references. Once a technical report [578] revealed that Indian EVMs were not tamper-proof, a Public Interest Petition was filed at the Delhi Court

advocating for the introduction of VVPAT. Despite its withdrawal by the local jurisdiction and the initial opposition of electoral authorities, the decision was appealed and the Supreme Court, "in its judgement dated October 8, 2013, ... held that the 'paper trail' is an indispensable requirement of free and fair elections and that the confidence of voters in the system could only be achieved through transparency which necessitated the need to introduce an accurate and verifiable system of voting" (see p. 99-100 in [68]). Eight Indian states used VVPAT in 2014.

On the other hand, VVPAT is not allowed in Brazil due to a Supreme Court ruling on November 6, 2013. For the time being, it is the final step of a long history where VVPAT has been subjected to pendulous modifications. Two parliamentary acts have been approved requiring VVPAT, in 2002 and 2009, but the former was modified only one year later and the latter was rejected by the Supreme Court in 2013. In addition, the opposition to VVPAT mainly comes from electoral authorities themselves ([118]).[8]

Finally, it is worth mentioning the *Association for Computing Machinery* (ACM) statement on e-voting systems, where VVPAT is clearly recommended: "voting systems should enable each voter to inspect a physical ... record to verify that his or her vote has been accurately cast ... Making those records permanent ... provides a means by which an accurate recount may be conducted" ([41], excerpt).

Concluding, VVPAT, a physical guarantee, appears as a key measure to overcome criticisms based on the public nature of elections. Its introduction makes sense if we take into account the discussions that have taken place in many countries, but such a conclusion also puts aside other potential strategies for enhancing electoral trustworthiness.

For instance, if the ACM statement is compared with the decision of the German Constitutional Court, it is to note that the former does not include the nuances underlined by the German Court, namely the paragraphs that foresee a potential reintroduction of e-voting solutions provided they protect other constitutional goods as important as the public nature of elections. The ACM is much more restrictive and one may wonder whether its statement is valid for democratic countries where not fully verifiable voting channels are accepted (e.g., postal voting).

It is also worth recalling that VVPAT has inherent constraints. It is helpful to compare the final results, but it provides no supplementary guarantees if other factors, as important as the results, are to be considered. VVPAT cannot guarantee ballots' randomization, an appropriate e-ballot layout nor a full deactivation of the voting machine after each voting session. Therefore, paper trail is helpful only to address some issues, but, beyond technical safeguards, a correct protection of the public nature of elections still needs further measures. A deeper and more nuanced understanding of what citizen electoral supervision exactly means is required (see [73] and p. 81 in [446]).

[8] https://www.youtube.com/watch?v=VKcJoMZHUmo [November 21st 2015]

3.3 Civic Activism

Civic activism is somehow "the other side of the coin" of the public nature of elections, whose details have been addressed above. The public nature of elections only makes sense if there are citizens, both individually and collectively, who care about what elections should be and monitor EMB's attitudes and decisions.

Moreover, civic activism has had great importance for e-voting development worldwide. While suppliers and EMBs have sometimes constituted limited partnerships that excluded civil society, specific NGOs initiated active protests that led to the reconsideration of some projects. The German and Dutch withdrawals, and other similar decisions, had likely not taken place without previous civic pressures. This section will present some significant cases: France, the Netherlands and Ireland. Shorter references will be made to Belgium and India as well.

The French association *Ordinateurs-de-vote*, whose motto is *Citoyens et informaticiens pour un vote vérifié par l'électeur* (Citizens and IT experts for a citizen verifiable ballot), is an NGO that started fighting against e-voting implementation when the French government took the decision, in 2003, to introduce e-enabled voting machines on the basis of an old article of the electoral code that allowed voting devices.

France is currently using both voting machines and Internet voting. Voting machines started being used in 2003 and right now there are three suppliers (i.e., indra, Nedap and ES&S) that are certified, although their actual use depends on each municipality. Internet voting is also used for overseas voters.

Despite the pressures of *Ordinateurs-de-vote*, the French electoral authorities have not accepted major changes. After the 2007 presidential and parliamentarian elections, when voting machines reached their largest use, civic and political criticism led to a moratorium (see p. 17 in [51]), but in 2015 the e-voting channel is still available and, what is more important, with no significant changes in terms of legal regulation or managerial improvements.

Moreover, after a controversial first stage (see p. 46-49 [51]), in 2012 a new Internet voting project was launched for overseas citizens. The Pirate Party is very actively filing complaints, but the courts have been rejecting them, the last one in July 2015, when the *Conseil d'État*, the highest judicial body for administrative matters, did not accept an appeal against data protection regulations (*Conseil d'État*, 10ème / 9ème SSR, decision 27th July 2015).

The Netherlands was a European e-voting pioneer. Voting machines that were supplied by Nedap and another local company, spread nationwide, except for the important exception of Amsterdam. Moreover, the Netherlands also used internet voting. But civic pressures reversed this path and the Netherlands came back to paper-based procedures.

As in France, in 1965 Dutch legislation foresaw specific paperless devices[9] for casting a ballot (article J32 Electoral Code; valid until 2010). The next two articles established some minimum requirements and delegated to the Executive further legal developments: one in 1989,[10] related to the overall electoral procedure, and another one in 1997, devoted to voting machines. (*stemmachines*).[11]

First trials took place in 1982 (see p. 330 in [416]), although massive implementations only occurred during the 1990s. Some pitfalls arose during this period and the system was fine-tuned accordingly. For instance, in 1998, the government was concerned with some aspects that would become crucial afterwards, both in the Netherlands and abroad. The government underlined "the need to narrow the risks arising from the total dependency on the companies who deliver the hardware and software" or "the need for more detailed regulations on the use of the software used to calculate the results" (see p. 330 in [416]). In 2002, new reports and updates addressed other doubts on the software that was used for the distribution of the parliamentary seats.

Despite all these incidents, Niemoller recalls that "the introduction and use of electronic voting machines in the Netherlands was rather uneventful, since all relevant actors agreed on the advantages of such a system (Nedap or other brands)" (see p. 331 in [416]).[12] It was thus a peaceful, long-lasting and settled e-voting system.

That is why, in 2004, the government decided to launch an internet voting program. The Rijnland Internet Election System (RIES) was used first for the internal elections of some water management boards, but in 2006 it was admitted as a voting means for overseas electors. Moreover, it is worth mentioning that the internet voting system included cutting-edge innovations that aimed at providing full verifiability though questioning the secrecy of the vote (see §III [328] and p. 15 in [427]). This pioneer experience was developed and improved by other countries later on, namely by Norway in 2011 [543].

When voting machines were ready to be adopted by Amsterdam, Rop Gonggrijp (b), in conjunction with the NGO Wij vertrouwen stemcomputers niet, managed to buy a Nedap voting machine and proved certain flaws that had been repeatedly denied by the electoral authorities [262].

Gonggrijp proved that the machines could be used for voting and for other purposes as well. They could easily become chess boards, for instance. Regrettably, both Nedap and the electoral authorities had stressed that the machines were limited to only one function. On the other side, the electromagnetic radiation enabled any citizen, with an appropriate device, to know the content of a given ballot.[13]

[9] Thanks to the right of access to public information, data on these first mechanical voting devices available at: wijvertrouwenstemcomputersniet.nl/Wob-8_buit [November 21st 2015]

[10] https://www.kiesraad.nl/sites/default/files/Elections_Decree_0.pdf [August 28th 2015]

[11] wijvertrouwenstemcomputersniet.nl/images/f/fa/Regeling.pdf [August 28th 2015].

[12] Jacobs and Pieters also think that the voting machines were "uncontroversial" (see p. 3 in [320]) and only "isolated incidents and accusations" (see p. 10 in [320]) might be highlighted. They mention, for instance, the complaints filed by Hans Janmaat in 1998 or that voting machines might benefit the 31st candidate.

[13] www.youtube.com/watch?v=B05wPomCjEY [November 21st 2015]

An official assessment of the overall e-voting project was conducted and, after the report was published in 2007, [14] the Netherlands came back to a paper-based voting procedure. Voting machines as well as the internet voting project were forbidden. Right now, the Netherlands are discussing again how to use e-enabled tools for voting and counting procedures [69].

The Irish case is similar to the Dutch one. The e-voting project also failed due to the criticisms raised by Irish Citizens for Trustworthy E-voting (ICTE), a local NGO, but it differs from the Netherlands because the program was stopped at a very early stage.

Counting procedures face important problems in Ireland. The Single Transferable Vote (STV) increases voters' capacity, but it also entails a complex counting. It is a proportional system where ranked votes are used in multiple candidate constituencies. Once the quota is determined, the surplus of votes is reallocated taking into account the second choices of the voter. The time elapsed until the publication of the results as well as potential mistakes due to manual counts are challenges that have to be taken into account.

Having in mind that e-voting might ease STV counting and tabulation procedures, the government bought a number of Nedap machines, but, once the machines received and warehoused, e-voting could never be fully implemented. The machines were piloted in 2001 (see p. 4 [388]) and 2002 (see p. 13 in [163]), but in 2004 the system was finally withdrawn just when a massive implementation was foreseen.

ICTE was founded in May 2003 (see p. 13 in [163]). It opposed using voting machines by means of academic reports or parliamentary hearings. Such initiatives aimed at highlighting machines' vulnerabilities, with special emphasis on the absence of a paper trail. This successful strategy deliberately focused on "not ever getting distracted by side-issues. By refusing to engage in meaningless arguments over money wasted, various reports and so on, simply constantly re-iterating the need for VVAT proved very successful" (see p. 21 in [163]).

Thanks to the right of access to public information, security reports were delivered to ICTE. Despite not having further details on the audit process, nor the full source code, which actually the government did not have either, ICTE discovered some flaws that were accepted by Zerflow, one of the suppliers: potential interferences on the voting interface and doubts on the management of the keys that gave access to the voting machine (see p. 8-9 in [389] and p. 22-23 in [316]).

Some issues were fixed, but the campaign had already influenced relevant stakeholders and unexpected decisions were taken. After the first parliamentary hearings, the commission "asks Minister to suspend roll-out and all spending, but a week later reverses this decision" and the day after, the government buys seven thousand voting machines, a number that is increased a month later (see p. 17 in [163]).

[14] *Voting with Confidence*, The Hague: Adviescommissie inrichting verkiezingsproces, 2007. *wijvertrouwenstemcomputersniet.nl/images/0/0c/Votingwithconfidence.pdf* [August 28th 2015]

Civic protests arose and finally an independent commission was created. Its report, whose preliminary draft was published in April 2004, did not recommend e-voting implementation for the immediate European elections, to be held in June 2004. The final report, which was published two years later, made a distinction between hardware and software: "the Commission concludes that it can recommend the voting and counting equipment for use at elections in Ireland, subject to further work it has also recommended, but that it is unable to recommend the election management software for such use" (see p. 194 in [442]).

It is worth noting that the government had not launched a previous participatory process, a democratic tool which is normally aimed at gathering different opinions from the citizenry and the relevant IT groups. Actually the official attitude was not very proactive: that "researchers have had to repeatedly use Freedom of Information legislation and expend enormous amounts of time and money obtaining information on what should be the most public and accountable of processes is indicative of an attitude and mind-set which does not lead to well-rounded well-specified design requirements" (see p. 18 in [316]). Although such a strategy has been overcome by other countries later on, namely by Norway, low official openness still subsists in many countries and it represents a menace for e-voting projects.

The proactive socialization of e-voting initiatives, including their more technical components, is an efficient vaccine that may prevent what happened in Ireland. The project was quickly stopped few weeks before the European elections and there already were some irreversible consequences, like the Irish ownership of thousands of devices that would never be used. In 2012 voting machines were finally sold for recycling [392] and there have not been other e-voting initiatives in Ireland so far.

Beyond these three references to civic activism (France, Netherlands and Ireland), other initiatives could also be mentioned, like the Belgian PourEVA (www.poureva.be) or the Indian VeTA (www.indianevm.com).

Finally, academia and IOs (international organizations) could be included in this section devoted to stakeholders that aim to influence electoral management. The Council of Europe's Recommendation 2004(11), on legal, operational and technical standards for e-voting remains as the unique international official document so far. There also are other important guidelines, but either they are white papers or handbooks (e.g., OSCE/ODIHR, IDEA) or they are approved by private foundations (e.g., The Carter Center, NDI, IFES). Academia has also played a key role in e-voting evolution with active groups advocating for a better electoral framework.

3.4 Business as Usual

Different activities can be identified along the electoral cycle, but voters always are the most important players. The whole process is conceived to guarantee their free political expression. EMBs, IOs, NGOs, academia, judges, media or political parties shape a complex picture with mutual interactions and finally private companies are

also involved in a market that differs a lot from other business areas. That is why understanding the correct role of suppliers is a precondition for any e-voting project. Moreover, it is worth recalling that e-enabled elections will likely need much more support from private companies than other traditional electoral tools. Software development, IT maintenance and similar issues need highly specialized companies and therefore nowadays EMBs are much more dependent than a couple of decades ago.

If salesmen do not understand the specificities of the electoral market or if EMBs' in-house expertise remains weak, the outcome will likely be an unbalanced and unfair dialogue between a public institution and a private company. And such a situation normally leads to contracts that do not take into account the whole range of interests that should be considered. Private interests will be carefully protected whereas public values, that is to say, those linked to democracy and human rights, will be underestimated.

Three perspectives, with three different case-studies, will help us understand these problems. First of all, post HAVA period will show us how easy money becomes a bad ally. Second, the Peruvian EMB represents a good example of an e-voting strategy having in mind the importance of in-house expertise. Finally, Non-Disclosure Agreements (NDAs) reveal complex trade-offs between suppliers and EMBs. The Finnish case will be very instructive.

The Help America Vote Act (HAVA), approved in 2002, aimed at modernizing US electoral organization, but voting machines had a long history behind them. HAVA only intended to improve something that was already in use. For instance, lever devices had been adopted "by the 1930s, essentially [by] all of the nation's larger urban centers" [327], punch cards as well as scanners were incorporated in the 1970s and finally Direct Recording Electronic (DRE) voting machines shyly appeared in the 1970s [327].

E-voting pitfalls had already appeared, but the US 2000 presidential elections, where the Florida recount faced several problems,[15] made evident that a structural improvement effort was really needed. After this scandal, US authorities decided that the updating of the electoral management was the only way to avoid similar problems and HAVA was approved with such a goal.

HAVA created the Election Assistance Commission (EAC), which is a federal body that enhances coordination among state and federal EMBs. Approving guidelines, sharing good practices or conducting research activities provides a better knowledge of US electoral management and thus a better starting point for its improvement.

HAVA also foresaw federal funds with the aim of modernizing election management nationwide and obviously e-enabled tools appeared as the most appropriate so-

[15] After being appealed, the Supreme Court [*Bush v. Gore* 531 U.S. 98 (2000)] did not authorize a new recount and validated the results. Punch cards were highly criticized. The so-called *butterfly ballot* had a specific layout where the columns, with the names of the candidates, and the relevant holes overlapped. Democrats should punch the third hole despite having the second candidature on the left column. As a result, some electors presumably misvoted for Buchanan.

lutions. Many counties started a quick IT updating, but civic and academic awareness also increased. Avi Rubin led one of the most significant stages when he had access to Diebold machines' source code [493]. Rubin concluded that Diebold machines had a number of vulnerabilities that threatened electoral integrity. Such criticisms were not welcomed by the company, but the overall perception had already shifted. It seemed that voting machines did not include appropriate security measures and that some companies only aimed at taking advantage of HAVA's economic benefits. Among other factors, weak in-house expertise as well as limited financial autonomy also prevented EMBs from having reasonable forecasts (see p. 8 in [109]).

The activities of the Election Assistance Commission (EAC), new voluntary federal guidelines and an improved awareness of all stakeholders managed to address some problems. However, the discussion remains open in the US, partially due to initial errors [329].

The US experience shows that advanced in-house expertise is the only way to counterbalance the role of suppliers. Should the relevant EMB develop internal know-how on e-voting issues, with new staff hired and appropriate training activities, the suppliers would immediately adapt their sales protocol. They would quickly realize that superficial and non-nuanced arguments would no longer make sense. But it is not an easy task. Financial autonomy, reasonable timelines and a clear institutional commitment are needed to achieve EMB's advanced expertise.

The Peruvian experience is limited when talking about public office elections, but paradoxically the local EMB has an extensive background in the assessment and implementation of different e-voting solutions.

Binding experiences began in 2011, in a single municipality (Cañete), slowly continued in 2013, including a Lima district, and widened in 2014, when e-voting was used by various districts of Lima and Cañete provinces as well as by Callao (see p. 12 in [180]).

But trials had begun in 1996 (see p. 28-31 in [444]), with a first binding implementation for a school board (see p. 66-67 in [443]). The Peruvian EMB started using e-voting for a wide range of non-public office elections, either binding or not, for training purposes and for social familiarization. It is worth mentioning that voting machines had also been used by political parties, for their internal elections, which is an excellent means of socialization and eases future implementations. If political parties pioneer such new technologies, with a satisfactory outcome, they will likely accept them in other cases.

Almost two decades later, institutional maturity and awareness increased a lot and that is why the Peruvian case is important. The Oficina Nacional de Procesos Electorales (ONPE) constantly pursued greater in-house expertise and many outputs can be mentioned.

In terms of e-voting management, it is worth noting the evolving nature of the technical solutions used by the ONPE. It combined agreements with international suppliers with in-house technical solutions and partnerships with local academia. In-

stitutional autonomy has not been lost. Moreover, research, a key parameter to assess institutional capacity, always accompanied practical issues, as the series of working-papers shows (for instance, [443] and [444]). *Elecciones*, an academic journal, also included a number of contributions with e-voting analysis. The eighth issue appeared a long time before the first binding implementation and the last issue reviews what has been done in recent years.

The Observatorio del Voto Electrónico en Latinoamérica (OVELAT) represents another initiative worth mentioning. Launched in 2011 and funded by the United Nations Development Programme (UNDP), it aims at being the Latin American meeting point for e-voting stakeholders. Finally, the ONPE also held two international conferences, in 2008 and 2013, the latter with the support of the Organization of American States (OAS).

Concluding, ONPE's strategy enhances a full e-voting package that includes the implementation itself as well as other initiatives. They have very different profiles, even modest ones, but all of them pursue the same goal: an informed public opinion and an advanced in-house expertise on e-voting issues.

Right now, Peruvian electoral authorities still envisage a future nationwide deployment (see p. 28 in [180]), but no new steps have been adopted. There is a positive citizen perception, but threats have also been identified, like the digital gap and an overall political distrust. Therefore ONPE aims at conducting new research and being aware of experiences worldwide (see p. 27-28 in [180]).

Finally, one should pay attention to Non-Disclosure Agreements (NDAs) and Finland is a good example for assessing transparency and the access to public information by independent experts. Upon agreement with the government, the Mathematical Department of the University of Turku conducted an audit whose report was published before the elections, but both Electronic Frontier Finland (EFFI) and an IT expert "refused to participate as they were not willing to sign the non-disclosure agreement required by the IT suppliers" (see p. 175 in [38]).

NDA's assessments are extremely illustrative since they are evidence of actual trade-offs between public and private interests. NDAs reveal the battle underlying any voting project that is managed by a private company [74] [284]. When citizens and electoral authorities focus on how to disclose and understand e-voting features, suppliers may be reluctant in order to protect their investments. In relation to the Finnish case, EFFI recalls that "TietoEnator, a Finnish company acting as a system integrator, required non-disclosure agreements that would have severely constrained the auditors' possibilities to publish their findings. The Ministry of Justice tried to arbitrate a better non-disclosure agreement, but were unsuccessful" (see p. 4 in [562]). In addition, in 2008 the Ministry of Justice had denied EFFI's petition founded on the right of access to public information. The Ministry argued that it was impossible to reveal data related to the "implementation of the security arrangements of information and communications systems... unless it is clear that the target of the security arrangements would not be compromised by their release." Likewise, "official documents that should be kept secret include documents containing information

on a [sic] private trade or professional secrets as well as documents containing other comparable private business information" (see p. 3-4 in [562]).

E-voting praxis also evolves and transparency became a precondition for some significant cases afterwards [580]. Some suppliers also adapted their internal rules once acknowledging that elections are a specific market and need special rules. As already stated, Norway, for instance, was a good reference. Its government granted access to all relevant data [543].

Right now (October 2016), Finland is reconsidering whether to use e-enabled tools. In 2013, a working group was created and its final report, which was published in April 2015, recommends "an experiment with internet voting... in connection with the advance voting in consultative municipal referenda during a fixed-term of four years" (see p. 180 in [38]). Further uses, namely for parliamentary elections, are postponed.

3.5 Outdated Technologies

E-voting technologies have been in use for the last two decades at least and, given the evolving nature of this field, it is worth wondering how software and hardware will be adapted to new IT and legal standards. Moreover, the term e-voting encompasses a wide range of technologies so future adaptations will likely not be taken in a homogeneous way. Each model will face different needs. Updating could even be impossible for certain hypotheses, due to technical obsolescence.

Significantly, the US Report and Recommendations of the Presidential Commission on Election Administration,[16] published in January 2014, acknowledged the importance and challenges of outdated e-voting technologies: "a large share of the voting machines currently in operation were purchased ... as part of HAVA's provisions ... Those machines are now reaching the end of their natural life cycle" (see p. 63 in [164]). This section will analyze how some countries address such a challenge. Beyond the USA, already mentioned, in 2012 Belgium substituted its old e-voting computers and in the 1990s Venezuela also managed to replace scanners by DRE. Finally, legal frameworks have some particular features regarding technical updating.

In Belgium, e-voting was trialled in 1991, in two areas (see p. 6 [200]), but a real implementation only began in 1994 and reached up to 44% of the electorate. Such a figure depends on the municipalities, which have the final decision on whether to use voting machines. Two models were certified by the federal government: Digivote, that covered about 85% of the market, and Jites, used by the rest of the municipalities (see p. 13 in [200]). It is worth noting that the introduction of voting machines cancelled paper-based ballots. The voter had only one option.

Problems appeared (e.g., Schaerbeek) and criticisms arose mainly due to civic

[16] https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf [September 22nd 2015]

activism led by Pour une Étique du Vote Automatisé (PourEVA). And improved guarantees were introduced such as the creation of the Collège d'Experts, which is a significant innovation because similar entities hardly exist in other countries. The Collège is an independent body whose members are nominated by the parliamentary assemblies. The Collège issues a non-binding report that is delivered to the relevant assembly after each election. Such reports represent excellent starting points for the analysis of the Belgian case.

Despite such a problematic history, Belgium managed to not only maintain the system, but substitute an outdated solution by a new one that fits much better contemporary standards. The old machines have been in use since the 1990s and thus there were increasing managerial burdens. Each election required new software, but the hardware remained unchanged. It was warehoused by each municipality.

In May 2014, an important incident occurred and somehow confirmed the necessity of an updating that had begun a couple of years before. Several Jites's mistakes prevented counting all the ballots. As the Collège recalls, "this control mission has been by far the most difficult one" (see p. 6 in [202]; translated from French) and it stresses that "the bad quality of the source code entails de facto problems for its maintenance. Moreover, such a source code needs to be updated every election ... The '2014 elections bug' is partly due to Jites's gaps that had already been highlighted" (see p. 57 in [202]; translated from French).

In 2012, Smartmatic had already replaced some e-voting systems. Maintaining the asymmetric geographical distribution that existed before, new voting machines were accepted by Flemish municipalities and two areas within the Brussels region, but they were not deployed in Wallonia.

A massive substitution is not an easy task, at least from a legal perspective and for training capacities. Legally speaking, e-voting entails complex regulations and, taking into account that there are many different e-voting platforms, either the higher legislation keeps a generic approach, with only basic principles that hardly frame further decisions, or a given e-voting solution is depicted in detail, which might make more difficult upgradings or substitutions.

A highly detailed procurement was used in Belgium. A university consortium had been asked by the government to conduct an e-voting comparison worldwide, to assess the weakest points of the Belgian system and to propose new methods. The so-called BeVoting Report suggested up to five new solutions and the government chose one, on which the procurement was based. The government also asked the Council of Europe to conduct an assessment on the compliance of the five suggested methods with international technical, legal and operational standards.

As a result of this analytical approach, the distinction between voting machine and e-ballot box was maintained. Such a separated system is closer to the traditional paper-based one since there still are both voting booths and ballot boxes. Moreover, the voter can use different voting machines to check whether his/her token contains the correct value. As stated above, the new system includes a twofold token that combines a human-readable paper trail with a computer-based code.

Training may also become a barrier when e-voting replacements take place. Well-trained officials are crucial in any electoral process, whether e-enabled or not, and obviously new e-voting systems will likely need a certain time to achieve the degree of familiarization that the previous system already had.

Three years later, Belgium is still using e-voting and the new Smartmatic solution seems consolidated. However, the incident with the other machines in 2014 increased the overall criticisms and the petitions to reintroduce paper-based procedures. The asymmetric deployment of voting machines does not facilitate a systematic picture of Belgian evolution, but what is not doubtful is that the replacement took place successfully, which is the only feature that this section intended to highlight.

Venezuela is another interesting example of substitution of voting technologies. From 1999 to 2003 scanners were used nationwide as a first e-enabled tool for electoral procedures. However, in 2003 Venezuela decided to shift from e-counting to e-voting.

Finally, recent generations of e-voting platforms include new features and shaped new scenarios that have to be legally framed. Verifiability (e.g., return codes), transparency (e.g., source code disclosure, better NDAs), sharing institutional tasks (e.g., independent commissions) or fair procurements (e.g., competitive dialogue) need a specific legal approach. Also, regulations become obsolete and need regular updates.

3.6 The Political Context

The electoral management cycle as such is a technical concept that could remain protected from political influences, but the subject itself, that is to say, running elections and thus deciding who will hold the parliamentary majority and/or the cabinet, is closely related to political inputs. Any e-voting implementation should be aware of such a mutual interaction and adopt the relevant measures to avoid improper influences.

The interaction between the political context and election management may follow different patterns. We will highlight three cases. The assessment of the sociopolitical framework should be the starting point for any e-voting deployment. Given that electoral technologies always need to rely upon a trustworthy background, social cohesion and the political context may either strengthen or weaken such a precondition. Second, politics have priorities that may not match what e-voting actually needs. Honesty, transparency, non mass media-driven decisions or long-term programs ease e-voting implementations, but sometimes politics does not adhere to such parameters. Third, it is worth recalling that the final decision always belongs to representative institutions. Second-rate projects may remain in use provided a political consensus subsists and excellent e-voting programs may be hindered by political pitfalls.

Regarding the overall political context, Venezuela and Switzerland both provide paradigmatic case studies. Venezuela is an excellent example of how voting machines continue being used despite Venezuela's extremely political polarization. On the other hand, Swiss political and social cohesion, which is strengthened by a leading civic culture, has a clear impact on the development of the internet voting project.

The first modern Venezuelan technical electoral update took place in 1999 and was based on Indra's scanning machines (see p. 262-263 in [381]). Paper continued in use, but scanners led to an adaptation of ballots' size and, what is more important, a training program. Voters learned how to properly mark the ballots and thus avoid further problems with the scan (see p. 263 in [381]).

Just four years later, in 2003, Venezuela shifted its strategy and began using DREs, which were bought from a local company, Smartmatic. First pilots were accompanied by complaints about the secrecy of the vote and deliberate tampering.

In relation to the secrecy of the votes, concerns had two origins. First, voting machines had been deployed in conjunction with fingerprint devices. In 2006, for instance, voters were identified with biometric machines and, once their fingerprints had been recorded, voters could go to the relevant polling station. However, fingerprint machines were not connected to voting procedures and actually voters were identified again at the polling station by traditional means (i.e., ID card). Thus, the right to vote did not depend on the biometric control, but such an arrangement raised suspicions.

Second, personal data management became suspicious due to the so-called "Tascón list", that is to say, the citizens who had supported a recall referendum in 2004, but, in electoral terms, there was no link between the list and voting procedures.

Paper trail and software also raised some concerns and, as stated above, measures were taken for enhancing citizen confidence. As a result, further disagreements rather focused on strictly political issues and not on e-voting as such. Anyway, adding new parameters, like mixing biometric identification with voting procedures, entails new concerns and such innovations will have to prove to be mature enough and win social acceptance.

Switzerland is a very different case. First of all, only internet voting from uncontrolled environments is admitted and, despite being a pioneer, there are legal constraints that prevent quick deployments. Only three projects (Geneva, Neuchâtel and Zurich) have been authorized so far and the extension to other cantons has always been based on one of those authorized programs. Right now, as already stated, Switzerland launches the so-called second e-voting generation, which intends to improve verifiability.

However, this section is devoted to assessing how the sociopolitical context may impact e-voting projects and, regarding the Swiss case, it is worth highlighting that the use of internet voting is closely related to the previous acceptance of postal voting. It is used by an average of 69% of voters (90% in some cantons; see p. 177 in

[372]), which is an exceptional rate. Moreover, postal voting is very easy to use. Once the electoral materials have been delivered to the voter, s/he only has to drop the relevant envelope in any postbox. It is to note that there is a specific social background behind such a procedure. Only countries with a large and solid social consensus can use such voting channels without major complaints afterwards.

Internet voting was adopted taking into account such a positive context. A strong civic culture has been supporting this innovation. Some concerns arose and civic activists highlighted potential weaknesses, even before the court [308], but political influence remained one step behind technical aspects, which is a correct approach.

On the other hand, the next case will show how an improper political approach may have a negative impact.

In 2010 Barcelona held a local referendum focused on the urban reform of Diagonal Avenue, which is a strategic axis along which public transportation, namely tramway, is problematic. Several social and political discrepancies arose.

Although Spanish law is very restrictive in relation to local referendums, Barcelona enjoys a specific framework that, taking into account the needs of big cities, nuances the normal distribution of competences between central, regional and local authorities. This Carta Municipal entitles the City Council to "gather citizen opinions by means of popular consultations" (art. 35 Law 22/1998, de la Barcelona Municipal Act; translated from Spanish). The main advantage consists in excluding a previous authorization of the central government. Detailed rules (Normes Reguladores de la Participació Ciutadana) were approved on November 22, 2002, and finally, as a first implementation, the City Council called for a referendum to be held from May 10 to May 16, 2010 (see p. 1 in [191]). Specific legal guidelines (Document de Bases) were also adopted for this referendum.

Internet voting was available from controlled and uncontrolled environments. Such a flexible organization intended to achieve a high turnout, which is a key political parameter when there are sharp discrepancies, as was the case.

An independent commission was created as well. Among other competences, it monitored the proper implementation of the legal framework and validated final results (see p. 15 in [191]). The commission was composed by external experts coming from different bodies (e.g., Parliament, Catalan Technical University).

It is worth noting that the project was managed by Scytl and Indra conjointly. Both companies are Spanish and competitors in the electoral market worldwide. Therefore they do not usually launch initiatives together. Anyway, on this occasion, the City Council "finally offered the contract to Indra Sistemas, who subcontracts Scytl's e-voting platform" (see p. 21 in [191]; translated from Catalan).

Bitter political disputes accompanied the referendum and several complaints arose (e.g., ballot layout), but the next paragraphs will focus on two specific issues: ID management and the protocol for addressing negative events.

Regarding ID management, safeguards against impersonation proved to be too weak. Voters requested a password online and they had to provide a cellular phone number and personal such as birthdate or similar information. As such data are somehow available on the Internet, a journalist impersonated a politician, a member of the City Council (see p. 51 in [191]). When he tried to cast a ballot, he was informed that he was supposed to have already voted the day before and therefore he could not cast a ballot again. Given the scandal, operators removed the first vote, which is also a controversial measure, and allowed a second ballot from the same ID (see p. 62 in [191]). The impersonator was identified, brought before the court and declared innocent due to the lack of conclusive evidence [472].

Concluding, the City Council intended to raise turnout, which was politically reasonable, but critical procedural steps, like the ID management, were weakened.

This case also provides other elements that, going beyond the anecdote, represent important lessons for further e-voting projects. That is the case of the comic incident that happened when the mayor tried to vote (see video in [52]) and unfortunately the system did not work (see p. 31 in [191]). Once in front of the computer, the mayor detected some problems, asked a technical adviser for help and they agreed to dissimulate. They would say to the media that the mayor had properly cast his ballot. Actually it was not true and the lie was discovered just a few hours later when, reading the lips, one could realize that the adviser was telling to the mayor that it would be worth not fixing the problem at that time and lying to the media. Despite the scandal, the City Council did not change its information for two days, but finally the mayor was forced to admit his mistake. He informed that he had cast his ballot the same first day in the afternoon, but he had been refusing this explanation during two days. Once again, (bad) politics seemed more important than technical issues and good management. Politics may cause the failure of e-voting projects.

Finally, when talking about the interaction between politics and technical management, it is worth recalling that politicians, that is to say, representative institutions always (have to) retain the final decision. Democracy also matters.

Norway is a very good example. It started using internet voting in September 2011, for local elections, but it was the final step of a long implementation during which the EMB proved to be aware of common e-voting challenges. As stated above, procurement procedures based on a competitive dialogue, transparency of the overall project or in-house expertise are hardly difficult to find in other countries. However, the Norwegian parliament had always expressed great concern. Secrecy, for instance, was a big issue for politicians [534]. The composition of the parliament guaranteed political support to the use of internet voting, but, after the 2013 parliamentary elections, the new government decided not to maintain the program.

Similar outcomes may be found when a country adopts EMB's transformations. Ongoing e-voting projects can be discontinued due to a new institutional framework,

new intergovernmental relationships and new legal responsibilities. That happened in Mexico after expanding the powers of the federal EMB and thus lessening local leaderships. Despite being a federal state, Mexico had launched different local e-voting initiatives. Coahuila, which was the pioneer, Jalisco or the capital itself had used voting machines and even internet voting for citizens living abroad. Each case faced particular problems, but the new centralized federal EMB, created in 2014, makes more difficult such a variety of initiatives. In June 2015 theăInstituto Nacional Electoral (INE) trialled its own voting machines, with non-binding effects [421], but only a single e-voting project is foreseen nationwide.

3.7 Voters Matter

E-voting platforms should comply with a number of specifications that normally range from IT requirements to legal and even social preconditions, but any e-voting solution should always have only one main target, which is the voter. If the elector fails to cast his/her ballot, any other potential e-voting advantages will become meaningless. And that has happened in some countries.

Usability and accessibility are important components therefore. Traditional paper ballots also face some constraints that may prevent them from being user-focused and fully accessible. Beyond the legal framework that imposes some layouts, "the ballot paper form and content needs to be easily understandable. Simplicity aids speed of voter flow, and assists all voters — not only those less literate — to vote with confidence that they have not made a mistake."[17] The Brennan Center for Justice compiled up to 13 bad practices, like splitting candidates for the same office onto different pages or columns, placing response options on both sides of candidate names, not writing short, simple instructions or placing instructions far from related actions [419]. For instance, the so-called butterfly ballot, already mentioned, did not comply with basic usability standards.

Regarding e-voting, Brazil and India represent countries that accepted such a technology provided a very easy way to operate with the computer was implemented. Venezuela also accepted DRE machines with the same premise. Second, some failures have a direct link with usability issues. The Finnish project was quite small, actually only three municipalities, but it illustrates fairly well what usability weaknesses may entail. Finally, accessibility is a key parameter for e-voting development. Voting technologies open new opportunities for those citizens who cannot use ordinary electoral procedures.

As for the first group of countries, Brazil started using e-counting machines in 1982, just after the dictatorship, but the final outcome was not satisfactory. A parallel counting proved that the official results were inconsistent (see p. 69 in [118]). It was the so-called Proconsult case, in relation to the company that managed the system.

[17] ACE Project / Ballot Paper Design: `http://aceproject.org/ace-en/topics/vo/voc/voc02/voc02a`

Such a bad precedent has somehow impacted the subsequent implementation of e-voting technologies in Brazil.

Later on, in 1996 the first voting machines started being deployed on a gradual basis. Initially, only towns over 200,000 inhabitants were entitled to introduce voting machines, but they spread very quickly and in 2000, with only two in-between elections, voting machines were used nationwide.

Having identified the weaknesses of the traditional Brazilian electoral system, e-voting machines were supposed to face local *caciques*, that is to say, leaders that used to tamper with electoral results. E-enabled tools would prevent such manipulations and therefore improve the integrity of the process. But Brazilian authorities were also aware that digital illiteracy might become an important barrier for an efficient implementation of voting machines. The final decision intended to address both problems (*caciques* and illiteracy) with user-friendly voting machines.

Such devices simulate a traditional telephone. There is a numerical keyboard and the voter only types his/her national ID code and the number of his/her political choice. Each candidature has a given number that is intensively advertised during the electoral campaign. Afterwards, the screen displays the chosen option and the voter only has to press a button confirming it. The vote is already cast. Obviously, the system could be improved, but it is worth highlighting its simplicity.

As a positive feature, simulating a traditional telephone eases the cultural change entailed in the lack of a physical paper ballot. Such a transition should always draw the attention of e-voting experts due to its important consequences. The principle of equality, a legal cornerstone, may be damaged if the e-voting systems do not take into account those citizens who are less familiar with new technologies [391]. And that is especially important when the paper based procedure totally disappears, as in Brazil.

Other countries also adopt similar strategies in order to address such a digital gap. India, for instance, is using voting machines that are far away from cutting-edge computers. Again, there is a voting board, where the candidatures are displayed, and the voter only has to press one physical button, check the screen and confirm his/her option by pressing another button. Venezuela is another interesting case because it acknowledged the digital gap problem and intended to face it with a sensitive board that replicates the previous paper-based ballot. Again, voters interoperate with a user-friendly device, in this case fairly similar to what they used before, and confirm later the option that is displayed on the screen, which is a supplementary device.

On the other hand, in Finland, usability pitfalls led to interrupting the internet voting project. In 2008, Finland trialled internet voting from controlled environments thanks to a temporary authorization included in Law 880/2006. Scytl, a Catalan company, and TietoEnator, a local partner, were in charge. The project was initially limited to local elections and internet voting was only used in three municipalities — Karkkila, Kauniainen and Vihti. Moreover, voters could choose between two voting channels, the internet one and the traditional.

If a citizen wanted to use the internet voting channel, a smart card was given to him/her and, once the preferred option was selected, "the voter had to confirm her choice by pressing the visible OK button on the screen ... the system gave a message that the voting had successfully been finished and asked the voter to remove the voting card from the card reader and to return it to the election official" (see p. 174 in [38]). Finally, the system transmitted the relevant data to a central server.

After election day, some inconsistencies were discovered. In some polling stations, the total number of citizens who had been identified as actual voters was higher than the total number of votes that had been recorded and transmitted by the relevant computers. It was established that some voters had left the polling station before confirming their option by pressing the final voting button. The computer did not save their options as actual votes therefore. TietoEnator identified a "total of 232 cases ... it seemed that in these cases the voter, for one reason or another, had removed the voting card from the card reader before confirming the choice by pressing the OK button" (see p. 175 in [38]; 232 cases or up to 12,234 of internet votes, that is to say, 1.89%).

The first appeal filed against this system was refused by a local court, but the Supreme Administrative Court accepted the complaint and required by-elections in those three municipalities. The Finnish internet voting project stopped here.

Usability performance as well as the information provided to the voter raised as key factors for understanding what had happened. A deficient interface layout did not indicate that the voting session was not yet ended. Such a weakness had been detected during previous tests, but it was not fixed (see p. 178 in [38]). Written (not graphics) information also included other mistakes since it explained that the single action of choosing, without pressing the confirmation button, was enough.

Undervoting cases are a common concern when using voting machines. The Sarasota one, for instance, during a Florida congressional district race in 2006, was very similar. It "violates many of the basic usability principles ... The instructions are not clear and simple; they use the passive rather than the active voice; single instructions sprawl over many lines, while two different instructions share the same line; and the instructions are center-aligned rather than left-aligned on the page" (see p. 56 in [419]).

Finally, citizens also need accessible voting means. We use accessibility as "a set of measurable characteristics that indicate the degree to which a system is available to, and usable by, individuals with disabilities" (see p. 7 in [417]). The targeted group is therefore the key difference between usability and accessibility.

Traditional paper-based electoral procedures include several accessibility drawbacks that could be overcome with e-enabled tools. Internet voting, for instance, may help people with reduced mobility. And voting machines in general may include multilanguage support, which is especially appreciated in some countries, or advanced accessibility measures for impaired people. However, new technologies also raise new concerns. Remote electronic voting, for instance, may inherit, "all the accessibility and usability issues ... [and] it adds new issues related to the technologies

that enable remote electronic voting. accessibility and usability of remote electronic voting systems present complex challenges that must be resolved to ensure voter efficiency, effectiveness, satisfaction, privacy and independence when voting remotely" (see p. 38 in [417] NIST).

3.8 Conclusions

Through examination of several case studies concerning various facets of e-voting technology and implementation, we have shown that e-voting is much more complex than what could be initially expected.

Proper computer design and maintenance is obviously needed, but there are other factors that cannot be neglected, as often happens unfortunately. Moreover, such factors use different perspectives and thus an interdisciplinary approach, which would be based on a permanent dialogue between technical, legal and social practitioners, is highly desirable.

Among other elements, legal aspects will highlight that the public nature of elections prevents implementing certain technical solutions. Democratic awareness will also recall that elections pursue public interests and thus private companies have to adapt their role to such a specific market. Civic activism as well as an advanced in-house expertise will facilitate a correct management approach and finally usability issues will underline that the voter has to be recognized as the key electoral player.

E-voting is being used, or at least considered, almost worldwide. And right now there are already good and bad experiences. The chapter aims at giving certain clues that have influenced e-voting implementations so far.

Acknowledgment

Barrat is supported by the Public Administration School of Catalonia (R+D Projects 2014) and the Spanish R+D Ministry (DER2015-68706-P).