E-voting in Latin America.
Political reflections about its establishment

Juan Rial

E-voting definition

A broad meaning of the concept of e-voting includes referring to every feasible electoral activity that can be carried out by information technology means. The latter includes citizen registry, mapping of voting districts, management, administration and voting logistics, voting, the counting of the votes, dissemination of voting results and their official certification. In a more restricted sense, it only refers to the act of casting a vote. In this paper, the same expression is used both ways, contexts allows us to infer which one is being referred to. The restricted sense of e-voting refers to digital voting, the possibility of voting using the Internet or electronic voting, which is cast through machines and programs which are not connected to the World Wide Web.

Casting a vote via the Internet is becoming more popular, even though it does not ensure privacy (secrecy) and we cannot be sure that the person casting the vote is the citizen that is using the voting instrument (computer terminal, cellular phone, etc.). Not even PINs (Personal Identification Numbers), cryptography or digital signatures can guarantee total security.

* Juan Rial, Uruguayan political scientist who has worked for ten years with Louis Goodman as a co-coordinator of Civil-Military Relations in the Latin American Project with the collaboration of the American University and Peitho. He has worked as a consultant for international organizations such as the United Nations, OSCE and International IDEA. In 1998, Mr. Rial organized a seminar in Burundi and Rwanda which analyzed the resolution of past violent conflicts. That same year he worked with Héctor R. Osada and evaluated the situation of Guatemalan armed forces after the implementation of peace agreements. In 1999, Mr. Rial took part in a world conference against corruption sponsored by the Vice-president of the US, Al Gore; in which he presented some works on defense and security forces in Latin America, as well as its challenges. He also prepared an assessment for Columbia University on the situation in East Timor after the referendum. Author’s e-mail: rial43@yahoo.com
in internet voting; even though more and more everyday product-purchasing, bank and other kind of transactions are made by using these means. The generation gap also influences this topic; older people do not trust the use of IT in electoral activities. Also, most of the political class ignores IT and are reluctant to use it. Overall, the number of citizens willing to use advanced forms of voting, i.e. cell phone registry and PINs, is still very small. Even though IT diffusion in political processes was supposed to happen quickly, it has evidently had a slow progress around the world.

Establishing fully automated processed in Latin America

In 1989, the Tribunal Superior Eleitoral in Brasil eliminated the old voting card which contained a photo and fingerprint; transferring the voter’s ID onto a database and issuing a simple election card called “título de eleitor” which is used massively. Later on, in 1996, it started to experiment with voting machines in municipal elections, generating information technology associated with the electoral process. In 1998 the scope of this experience was broadened and in October 2000 100% of the voters in municipal elections were included, 109 million citizens and half a million voters in the early 21st century. 354,000 ballot boxes were distributed in 315,000 electoral sections all over the country. In the following presidential election, there was an 85% use of an electronic ballot box. In the 2010 elections in which Dilma Rouseff won, 135.8 million Brazilian cast their vote using 480 thousand electronic ballot boxes, which took them approximately between 40 and 60 seconds to do so. Fifteen minutes after the electoral circuits were closed; over 100 million votes were counted. And even though it does not print a voting receipt, the system is highly reliable for the electoral authorities, the political class and the citizenry. An important addition and advantage is the use of biometric authentication to activate the equipment, guaranteeing the premise that one voter equals one vote.

Venezuela changed its system in 2004, during the Recall Referendum organized to decide if President Hugo Chávez should or should not remain as such. Under the purchase method, the Electoral Council called a tender. Three consortiums competed, the second one backed by the Spanish company Indra and the third one was Diebold of the US. The winner provided the Smartmatic Automated Electoral System, sold by

1 Companies such as Scytl (<www.scytl.com>) state that their Pnyx 1.2 software creates a voting certificate and a digital envelope that attaches itself to the digital vote, which could guarantee the use of Internet; however, criticisms regarding its use remain.

2 I have been a consultant on this topic for more than 15 years and I am familiar with the electronic ballot boxes used in Brazil. In 2003 I wrote a consultancy report for the PNUD of Argentina in which I stated that in a few years electronic voting methods would be established. I was wrong. Resistance rates were and are currently high.
the Smartmatic consortium with registered offices in Boca Raton, Florida; formed by the CANTV telecommunication company in Venezuela, the Bizta software company—also in Boca Raton—and the Caribbean Government Consultants Caribbean Government Consultants a consultancy firm in Florida. Olivetti was subcontracted to provide almost 20,000 machines3 used on August 15th 2004, all of this cost 63 million dollars (plus software installation, maintenance, communication and other fees, similar to those of AFIS machines) and was planned to be used by 14 million citizens; however, less than 9 million people voted. The system was established amidst a highly radicalized political controversy and the results did not satisfy the opposition, which reported the occurrence of frauds. The latter could not be proven; however, bad publicity that results from an “obscure” management of previous processes does not favor the expansion of electronic vote technology.

Other countries like the Philippines have made great progress; the establishment of this system allows them to know the results of the election the same day it takes place. In the 2010 election, 80 thousand electronic ballot boxes were used; to know the results of previous elections weeks had to go by. India which has the biggest electorate in the world still uses very simple machines, a calculator, in a peculiar election system that takes place successively in each state for more than a month.

In Estonia, ever since 2007 citizens can vote via Internet and since 2011 voting via cell phones has been tested; however, the use of this system has been limited. In the 2011 elections, in which cell phones were used, only 9% of the voters used this system. Estonia and Switzerland have tested voting via Internet.

Belgium and Switzerland have also used the system of electronic vote ballots that include a chip and are aided by a computer and a printer. A similar system that uses a computer as a voting ballot printer was established in the Argentinian province of Salta in 2011 and in municipal elections in Chaco. Estonia and Bulgaria also have similar systems to elect their presidents.

The US has a very decentralized voting system. Some counties have electronic voting machines; others use electronic ballot boxes and also systems that use ballots with chips to “scan” them. Voting via Internet has been used by civilian and military personnel deployed abroad; however, this practice has been discontinued.

Many Latin American countries have carried out pilot testing processes and have even gone beyond. In 2001, some Brazilian states neighboring

---

3 You can see the versatility of the machines if you consider it was a modified design of machines used in casinos as “slots”.

Juan Rial  E-voting in Latin America 173

DR © 2012. Instituto Nacional de Administración Pública, A. C.
Paraguay loaned the latter machines to pilot test 1% of the voters in Asunción; in 2003, 45.83% of the voters used this system in the national elections. They still used this system in 2006 for internal party and municipal elections; however, they did not continue to use it because political problems involving context. There were rumors of fraud and this was —wrongly— attributed to the use of electronic ballot boxes.

Argentina’s 2003 mayoral election in the city of Ushuaia in Tierra del Fuego had a digital voting system. They tried other ways and some pilot tests were made; however, no progress was made. Finally, a different system was used in April 2011 in the Salta province; elections with the widest scope of electronic systems in Argentina were held. They took place in 79 schools and 725 tables, a third of the registered voters, 244,702 out of 812,881 citizens.

The system which was used in Salta tried to overcome the idea of its possible manipulation. They tried to prevent it by using Electronic Voting Ballots (Boletas de Voto Electrónico (BVE)). The computers that were used did not constitute an electronic ballot box; they were only a way to select votes on the screen, print ballots and count them when the process was over and make a report. The voters receive a ballot with a chip to get printed. To avoid “chain voting” the ballot has a verification ticket. The voter introduces the ballot in a printing slot, selects his vote in the screen and prints it once he is sure of it; goes back to the table, hands in the verification ticket and the already folded ballot to ensure secrecy and introduces it in the ballot box. After the voting has ended, the counting is done using the same machine. The chip ensures it cannot be used after the printing, in the screen, the ballots are checked with the printed ones and a report is also printed. To consolidate these results, an encrypted file is sent to a data center so as to have a final result. The advantage posed by said process is that there is no data stored in an electronic ballot box, but in papers, which can be eventually audited manually. In this province, this system will be 66% established in the course of two years and 100% by 2015. Meanwhile, it is sought to expand the system in other municipal or provincial elections. Although this system and the one in Venezuela are similar, it is in fact a more advanced system that the latter because the voting does not require an electronic ballot box.

The Constitutional Court in Germany prohibited the use of voting machines, arguing about the reliability of the casted votes. Currently, on a national level and with the use of different systems, only Brazil, the Philippines, India and Venezuela have achieved 100%.

**Other systems linked to voting machines**

To transmit the results, different types of Internet connections are used: traditional landlines, cellular or satellite, as well as other traditional
systems to transport data directly. Their processing requires ad hoc counting programs which will carry out the corresponding operations to assign positions according to legal standards and instructions given by the corresponding program. New systems are trying to be developed to identify the voter. Issuing documents which contain barcodes or magnetic codes does not improve the levels of identification when compared with a purely visual observation of a person and their document which has a photograph. A “safe” system would include in situ verification of biometric data, for example, fingerprint verification by scanning them and comparing them to the ones saved in the electoral roll or iris inspection of the person that wants to vote. However, these systems are still very expensive and slow to identify a great number of people because it involves contrasting data from each person in the roll with all of the registered voters, so as to prevent someone from voting more than once. In 2004, Venezuela tried using the Automated Finger Print System (AFIS) provided by the Taiwanese-American company Cogent Systems which supplied 12,000 machines; meanwhile the Israeli company GILAT provided satellite communication to effectively implement the system; however, it could not operate correctly.

To count the votes, scanners, or machines that recognize certain marks can be used. These marks are usually circles, ovals, rectangles or squares that have been filled with ink or graphite, indicating the voter’s choice. Once the machine recognizes it, it stores the data. Various control tests conducted in universities or institutes usually use this same mechanism. The machine “reads” the marks and when the electoral activity is over, it transmits the results. The scanned ballots are not discarded, so a backup exists; the electronic count can be checked so as to prove if both results are the same. This can also be done with voting machines that issue a paper ticket.

Every electoral body has to fulfill certain basic requirements to ensure the integrity of the electoral process. Being a highly political activity, the basic rights of the citizens have to be protected. Equality means, one person one vote. Accessibility means that every citizen should be able to vote and to be candidates according to existing constitutional and legal norms. Also, votes have to be secret. The process has to ensure transparency; it must be open to citizen’s observation, it should not favor any political force or candidate and should ensure neutrality. Simplicity is necessary so that the voters receive very little instructions and avoid mistakes. Flexibility and mobility are required; the system should offer alternatives for those who travel and for those who have physical problems so that no one’s right to vote is denied. The process should meet the verifiability principle and should be auditable in each of its operational stages. Finally, the system should yield reliable results in the shortest time possible to avoid creating political uncertainty; also, every system that wants to be established should avoid becoming obsolete, ensuring durability and reasonable cost.
An elections means zero mistakes

An election is not a study based on the principles of probability sampling, the report of a precisely defined universe, all of the citizens authorized to vote that have voted, so there cannot be any margin of error. The result has to be accurate, reflecting the expressed will of the citizenry, without mistakes. This will ensure the integrity of the process. Electronic systems eliminate questionable options that are usually present in manual systems (double votes, votes marked in erroneous places, defective or spoiled ballots, etc.) and help overcome these problems. However, security problems that electronic systems have are important.

The main security problem in electronic voting processes is the possibility of an operator, programmer or “root/administrator” accessing the content of votes through computer manipulation programs before or during electoral activities to know the voter’s identity and preferences or change the voter’s decisions. The constitutional principle of secret vote and the need to have “clean” processes has to prevent all of the above, if this does not happen the system’s reliability disappears. Manual processes do not have to worry about this “administrator”, this is the main argument against the use of modern technologies in electoral activities.

Security in e-voting processes

The main “suspicion” in an electronic process is its security when compared to a manual one. Therefore, an e-voting system has to pay attention to every wrongful intervention possible in process, whether it is inside or outside said system.

The points listed below describe the security requirements a voting system should have.

First. Integrity of the system. Equipment, hardware, programs and software should be designed to be fraud proof. Ideally, there should not be changes once the electoral process has started. Once the equipment, source code, initial parameters, configuration information and basic programs and routines have been certified; everything has to remain static until the end of the process. Only data can be entered and processed according to what was previously established.

Second. The source code has to be properly owned by the appropriate electoral authority not a company that provides materials. The hardware and software’s system, including the source code, have to be available for inspection at all times; including backup documents (technical and operation manuals). There cannot be confidentiality claims made by private providers. However, “confidence” or “secrecy” is needed to ensure
the systems. Free access to the source code, just to take a look at it, verify its content and suitability, without having the possibility of modifying it, means that only those who have the appropriate authorizations (electoral employees, party delegates or monitoring organizations) will be able to do it. Those in charge of these tasks must go through security controls that ensure their personal integrity.

Third. Some experts consider it could be more convenient to use open source software, because it would allow greater studies regarding security breaches, instead of a proprietor code that is by definition, secret. Nonetheless, different levels at which the system operates have to be taken into account, so that the people authorized to do so can access every programming level and not only programs that run “superficially”. Those who access the system to operate or audit constitute the weak link in the system’s security chain. Being guardians themselves, the old adage can be used: “Qui custodies ipsos custodies?”, that is, who will guard the guardians? The use of redundancy programs that repeat the same process on alternate ways seems a good idea at first to discover flaws, but it can also increase them. A virus can be introduced at the same time in more than one verification program. The use of special algorithms that are tolerant to “n” number of flawed components is recommended, although it is well known that this can fail when it gets to “n+1”.

Fourth. All of the manuals and documents concerning the system have to be written in a clear way. They must not be inconsistent or have ambiguous phrases that raise doubts, or lack information regarding every aspect of the process. The computer industry standard regarding writing of manuals that chooses obscurity to compete in the market cannot be accepted. Documents have to be very precise, especially in security topics, warning about problems that may eventually arise.

Fifth. The system’s design, establishment and maintenance have to guarantee that there there is no possible way bugs (malfunction) can arise in the system, as well as the introduction of viruses during its operation. Computer jargon speaks of malware, a way to refer to malicious software that includes Trojan viruses, logic bombs, bugs and other codes that intend to produce unwanted changes. Hence the need to not change anything after it has been audited and certified as appropriate to be included in the election.

Sixth. Strongly centralized systems can lead the “administrators” to be tempted to manipulate them and facilitate attempts to subvert the system through a central operation and jeopardize the whole process. Systems that have divided management or decentralized operations require greater design control to avoid compatibility problems among them and a greater
amount of time and staff to verify the system’s operation. Usually it means having systems that function in a coordinated, but decentralized way.

Seventh. It is suggested to have a voters’ registry and identity verification system, another system to vote (included in the counting process or not) and one to transmit results, each one of them independent from one another. If DRE (Direct Recording Electronic) voting machines are used, these will leave physical evidence of the votes to re-count an electoral process and respond to possible complaints and suspicions. Most DRE machines on the market do not leave this kind of evidence. Some companies now offer the possibility of producing magnetic cards that record votes to allow a subsequent audit of votes cast. It is true that the introduction of a printed vote will make the system more expensive and eliminate what was saved by the disappearance of paper. Nonetheless, any suspicions the system initially generates can be overcome by pointing out this redundancy. It would be highly recommended, for a period of time, to use these cards (“paper”).

Eighth. There are some machines that can produce a piece of paper that includes the results instead of chips or memory cards. Printed paper reels can be “easily” replaced, the use of these machines represents a source of vulnerability. Their use is not recommended. Data entered into the system has to be adequately verified so that only the correct information that comes from fraud proof sources can be entered.

Ninth. The secrecy of the votes has to be guaranteed, this way no one can know the voter’s will inside or outside the system. Voter’s identification systems and voting processes cannot be associated, so nobody can know who voted for whom. There should be coordinated, parallel systems of voters and vote identification which should not be integrated. There are those who defend integrated systems that hide the voter’s identity and that does not allow data to be reversed to associate them with the voter. But, to achieve this, the possibility of subsequently auditing the system has to disappear.

Tenth. Internal system operators have to make sure that it cannot be accessed through the “backdoor” using simple alphanumeric codes (passwords) that allow maintenance staff to access it and possibly carry out fraud operations. The operator’s entry authentication should be the same as the one used by security and intelligence agencies. The staff that works with this equipment should be subject to precise biometric identification mechanisms and possibly to more than one system (iris identification or fingerprints to work with the equipment and its programs and specific passes with alphanumeric codes to access restricted places). Every time

---

4 Nowadays there are portable machines that can print tickets in triplicate when using credit cards. Something similar could be used in voting machines.
someone who operates the system accesses it, it should be registered; this should not be able to be erased without affecting its functioning, to be able to allocate responsibilities. A real-time inventory must be kept regarding the distribution system’s situation of peripheral equipment, as well as faulty material and its subsequent replacement. The latter does not require specialized technology, but adequate management systems. Security also includes that of the place equipment is installed in; for both people that are entering and for the facilities themselves.

Eleventh. It is well known that every system is vulnerable and that there is always the possibility of cracking it by introducing a “Trojan horse virus” that does not need to modify the source code. It is also well known that “bugs” can be installed to get around cryptographic verification numbers. Systems based on personal computers are vulnerable to the appearance of false parallel systems, impersonators, and that the existence of “root” administrators can lead to corruptness. However, this needs an opportunity and an administrator’s lax attitude. Constant audits and checks have to be made to the system. Mexican electoral employees that had to fight against the idea that an election equaled fraud in the late ’90 stated the following, which helped change this idea: “we should have locks and padlocks and locks for these padlocks”. This idea made the system notoriously more expensive due to a high degree of redundancy controls and introduction of other problems, nonetheless, it was effective. Nowadays, the Mexican Electoral Institute is an institution with an acceptable degree of reliability despite the problems of 2006.

Twelfth. Besides initial tests and adequate certification, the system should be audited once the process has been completed to bring about an operations evaluation. Auditing is a task that follows accounting principles even more than information technology ones; therefore, all of its operations can be checked. The best way to audit is to issue printed vouchers. Taking into account that the number of registered voters in the machine has to be the same as the ones who were manually or electronically verified as being present at the polls. The results of each table, perfectly capable of being identified, have to match the ones in the central tab for that table. The results derived from printed votes have to be the same as the electronic ones. Audits based on random samples can only show random mistakes, this is not the best way to prove if there has been a fraud or not. This audit includes more than just looking for tables or ad hoc places to prove there have been some manipulations. Books that record every incident or problem are very important for the audit. If some mistakes are discovered, the audit’s scope must be broadened.

Thirteenth. The system has to allow operations to be printed in paper so as to check results, in various stages of the operation.
Fourteenth. Current electoral laws are usually very careful regarding manual processes and require in many cases to approve them, special majorities; thus, every operation of e-voting should be established in precise legislations and not be left in the hands of regulations issued by electoral authorities or operational staff of these bodies. In a lot of cases, these authorities are not the ones who proposed the current norms, but employees of the companies that are in charge of turnkey operations through end to end contracts. The essentials have to be foreseen, this way those who work at an operational technical level, such as state or private company employees, will not be the ones making the important decisions regarding this process.

As it can be seen, the most relevant aspect of security is the staff that develops, monitors and manages e-voting. The latter should have certified levels of security and must be well paid. Voting requires high-security criteria which are not present in commercial operation systems. It’s staff requires maturity and discipline to manage the system; the cost of operating high-security systems is for times greater than running conventional ones and problems can still arise.

The 2004 process in Venezuela was relatively simple (there were only two options: YES or NO), and even though printed vouchers were given out, it did not yield the expected results. It is true that the use of machines to take fingerprints notoriously hindered the process; however, some points are not very clear. The National Electoral Council took a week to disclose 100% of the results; furthermore, estimated abstention levels constantly went up, which cannot be easily explained. The contender’s lack of trust and the ineffectiveness of the organizations observing the election (OEA and Carter Center) which lacked technical experts on the subject did not help the process.

In the 2004 municipal election in Brazil, 3% of the machines, 12,000 out of 400,000 had a device to print the vote; the voter then had to deposit the ballot in the ballot box. The electronic result had to be the same as the manual one yielded by the vouchers; giving greater security to the process.

In the US, in November 2004, 29.3% of the citizens used electronic machines to register votes; in 2002 only 12.6% did the same. Although the system had been previously criticized, no immediate complaints were received. The topic has never been relevant because of the election’s political impact.

Conclusion. Requirements of a e-voting system.

The most important aspect of adopting an e-voting system is security which means the system’s reliability. There are notorious incentives for those who work inside the system to resort to bribes; we have to distinguish between
attempted frauds and “accidents” that happen in computer processes. E-voting security norms that have been aforementioned have to be taken into account to certify the adoption of a system. The success of a system lies in the electoral body and the political class’ acceptance of it and their ability of transmitting these feelings to the citizenry and the media.

A voting system is more than mere technology. It is essentially the result of a social consensus that has been expressed in laws and other legal rules according to the socio political situation in which political quarrels are settled. The actors’ of this basic consensus are bodies and institutions; formally and informally regulated practices that are part of the country’s political culture. Legal dispositions are the result of consensus; electoral activities are regulated by constitutional laws and principles. The establishment of elections involves the use of legally accepted technologies. That is why we have to take into account the historical, cultural and political nature of electoral processes to choose which technology to use. The same technology used in two different societies or in the same society in different times can yield different results. Changing technology and implementing modern solutions does not always mean the system will improve. It is not advisable, as seen in the Venezuelan case, to make big changes that involve the use of new machines and fingerprint detection systems in a confrontational political context which means zero consensuses between the contenders. That is why we need to evaluate first the impact of new technologies on the political culture and if they answer society’s needs. Necessary modernizing progresses should not become mere businesses that only offer opportunities and temptations which are not always welcome.