Tribunal Superior Eleitoral

# ELECTRONIC VOTING SYSTEM

## | Frequently asked questions |

3rd edition

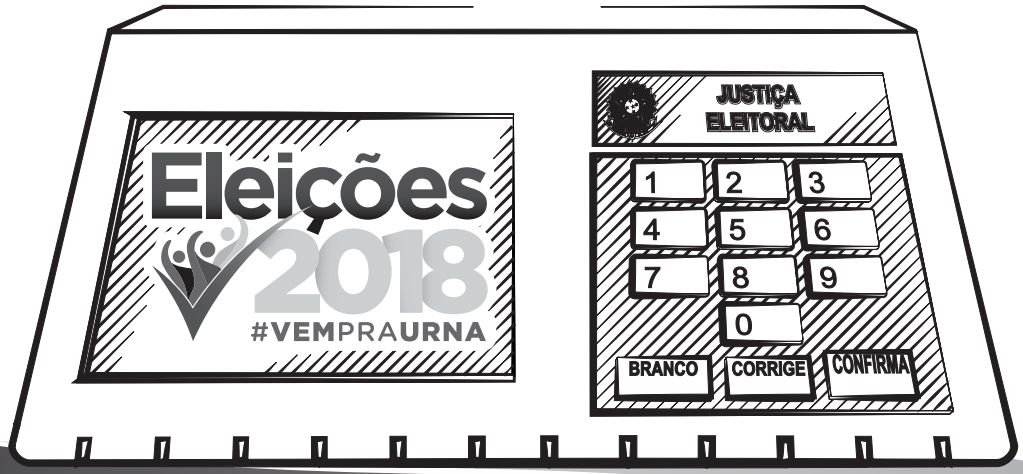

Brasília – 2018

Tribunal Superior Eleitoral

# ELECTRONIC VOTING SYSTEM

## | Frequently asked questions |

3rd edition




Brasília – 2018

Office of Information Management
SAFS, Quadra 7, Lotes 1/2, 1º andar
Brasília/DF – 70070-600
Telephone: +55 (61) 3030-9225

**Secretary-General of the Presidency**
Estêvão Waterloo

**Director-General of the Office of Information Management**
Rodrigo Curado Fleury

**Information Management Officer**
Janeth Aparecida Dias de Melo

**Coordinator of Publishing and Publications**
Renata Leite Motta Paes Medeiros

**Responsible for the content**
Secretary of Technology Information

**Publishing and editorial services**
Subdivision of Publishing and Graphic Design (Seprov/Cedip/SGI)

**Cover and graphic design**
Verônica Estácio

**Editorial services – copyediting**
Subdivision of Proofreading and Copyediting Services (Seprev/Cedip/SGI)

**Printing and print finishing**
Subdivision of Graphic Services (Segraf/Cedip/SGI)

Dados Internacionais de Catalogação na Publicação (CIP)
(Tribunal Superior Eleitoral – Biblioteca Professor Alysson Darowish Mitraud)

Brasil. Tribunal Superior Eleitoral.
Electronic voting system : frequently asked questions / Tribunal Superior Eleitoral. – 3rd ed. – Brasília : Tribunal Superior Eleitoral, 2018.
35 p. ; 21 cm.

Unidade responsável pelo conteúdo: Secretaria de Tecnologia da Informação.

1. Segurança do voto na urna eletrônica – Brasil. 2. Voto eletrônico – Brasil. 3. Urna eletrônica – Brasil. 4. Registro digital do voto – Brasil. I. Título.

CDD 342.810 75
CDU 342.843.5(81)

**SUPERIOR ELECTORAL COURT**

**President**

Justice Rosa Weber

**Vice President**

Justice Luís Roberto Barroso

**Court Justices**

Justice Edson Fachin

Justice Jorge Mussi

Justice Og Fernandes

Justice Admar Gonzaga

Justice Tarcisio Viera de Carvalho Neto

**Federal Electoral Prosecutor**

Raquel Dodge

# Introduction

With the aim to address the many different questions and theories regarding the security of Brazilian elections that have been disseminated by the media, which often lack both technical and legal grounds, the Superior Electoral Court (TSE) has compiled frequently asked questions on the issue in an effort to provide citizens with an enhanced knowledge of the mechanisms adopted by the Brazilian Electoral Court System to ensure the security and reliability of computerized elections in Brazil.

# Contents

# 1. CAN VOTERS RELY ON THE SECURITY OFELECTRONIC VOTING MACHINES (EVMs)?

Electronic voting machines (EVMs) feature many different mechanisms that allow individual voters and civil society organizations to check the security and the proper functioning of the voting system. The Brazilian Electoral Court System makes use of state-of-the-art information security tools and expertise to ensure the integrity, authenticity, and secrecy – should that be deemed appropriate, of machine contents. These mechanisms were put to the test by means of Public Security Tests, in which they showed robustness and were improved with contributions from the specialized technical community. In addition to that, there are numerous mechanisms designed to perform the auditing and checking of voting results that can be tried by candidates and coalitions, the Brazilian Prosecution Service, the Brazilian Bar Association and individual voters.

The parallel vote is a security procedure that may be monitored by voters. On the day before elections, during a public hearing, voting machines are randomly chosen for testing. These machines, which had already been set up and configured in different polling places, are then brought back to the competent Regional Electoral Court, and substituted by similar machines, which had been set up and configured in compliance with the same protocols of the replaced ones. On Election Day, the selected machines are inspected during a public hearing, being used in a parallel vote under the same conditions of the original polling station, except for the fact that all votes cast on these e-voting machines

are registered on the side. Each vote is registered in a paper ballot and then cast on the voting machine, being everything recorded on video. By the end of the day, at the same time of the closing of the polls, the counting of paper ballots takes place and is then compared with the results of the machine bulletin [Boletim da Urna]. This is a procedure that can be easily understood, and it is rather simple to monitor its steps.

The verification of machine bulletin [Boletim de Urna] constitutes another rather simple mechanism. After polls close, machine bulletins featuring the counting of votes of each polling station become public documents.

The results of each machine bulletin may be easily compared with the total published on the website of the Superior Electoral Court by either checking the results of each polling station or checking the final result of the elections. This auditing procedure has been widely used by political parties and coalitions, and may also be used by individual voters.

The questions listed next address specific doubts related to the security of e-voting machines and the transparency of voting processes and systems.

# 2. ARE ELECTRONIC VOTING MACHINES (EVMs) SAFE? IS IT POSSIBLE TO RUN UNAUTHORIZED SOFTWARE PROGRAMS ON THEIR OPERATING SYSTEM?

The operating system loaded on e-voting machines does not run unauthorized software programs. Similarly, it is not possible to modify machine applications. Brazilian e-voting machines (EVMs) utilize top-notch cryptography, digital signature and hash technologies. Machine hardware and software use these technologies to create a chain of trust, making sure that e-voting machines certified by Electoral Courts run only software programs developed by IT experts from the Superior Electoral Court. Said software programs are loaded on each machine during the electoral system sealing ceremony. Any attempt to execute unauthorized software programs in e-voting machines results in operational blocking. Similarly, attempts to run official software programs in non-certified pieces of hardware lead to the cancelation of application processing. This whole technology has been put into practice on the Public Security Tests, allowing the Superior Electoral Court to make the equipment even safer.

The set of applications loaded on e-voting machines during the electoral system sealing ceremony features digital signatures hashes. In the event of suspicion regarding the authenticity of software programs loaded on e-voting machines, their matching digital signatures and

hashes may be checked and validated by either running applications developed by IT experts from the Superior Electoral Court or software programs developed by political parties, the Brazilian Prosecution Service, and the Brazilian Bar Association or by other entities.

Finally, e-voting machine contents and results are protected by digital signature. It is not possible to modify information on candidates or voters after such information has been recorded in the machine. Thanks to digital signature technology, it is not possible to change, inter alia, the following machine files: voting results recorded in machine bulletins, the history of operations executed by the voting software (log), and the Digital Record of the Vote (RDV).

# 3. ARE ELECTRONIC VOTING MACHINES (EVMs) VULNERABLE TO EXTERNAL SECURITY THREATS?

Electronic voting machines (EVMs) are not vulnerable to external security threats. These machines consist of pieces of equipment that operate in an isolated way, featuring no mechanism that provides for their connection to computer networks like the Internet. The hardware of Brazilian e-voting machines is not compatible to network connections of any form, irrespective of whether such connections are based on wired or wireless devices. It is worth noting that the Linux Operating System that is loaded on e-voting machines is treated by IT experts from Electoral Courts so that it does not feature any software mechanism that allows network connections or remote access.

Furthermore, the applications loaded by Electoral Courts on e-voting machines, and the recording of voting results are both protected by modern digital signature technologies. Hackers inevitably fail when attempting to change any application file.

# 4. HOW DOES THE TSE CONTROL/ IDENTIFY THREATS PERPETRATED BY EMPLOYEES OF ELECTORAL COURTS?

Electoral Courts make use of modern tools designed to control the source code of electoral systems. Indeed, these tools provide for the monitoring of any modification of the source code, revealing what has been modified and by whom. Only a selected group of employees and limited-term commissioned staff hired by the Superior Electoral Court has access to the source code, being such professionals also authorized to carry out software adjustments. As a consequence, e-voting machines used in Brazilian elections are loaded with the same voting software, which is under the strict control of the Superior Electoral Court.

On the other hand, the knowledge on electoral systems is fragmented among different departments of the Superior Electoral Court. That means that the team responsible for the development of machine software is different than the one that is responsible for the system that tabulates election results. Such access control precautions can also be found in the system that controls software updates. The number of electoral systems involved in the organization of any given election is so large that it is literally impossible for an insider to have sufficient knowledge to carry out any type of attack. In addition to that, both the Superior Electoral Court and regional electoral courts perform many different tests during the period that the electoral systems are being developed with the aim to check the proper functioning of the entire set of voting

applications. Political parties, the Brazilian Prosecution Service and the Brazilian Bar Association are entitled to monitor the development of such voting software, being authorized to inspect the source code in the same environment where voting apps that will be used in elections are created.

In addition to their tenured employees, Electoral Courts hire limited-term commissioned staff during election years to render support to activities related to the transportation, preparation and maintenance of e-voting machines. Millions of poll workers are also summoned to work on Election Day. Neither the commissioned staff nor poll workers are granted access to the source code of electoral systems. Although these professionals have access to e-voting machines, they are not capable of violating machine hardware or software thanks to the many different security mechanisms in place. Such mechanisms are based on digital signature and cryptography technologies that create a chain of trust between hardware and software, preventing any form of machine violation.

# 5. HOW MANY SUSPECTED FRAUD CASES HAVE BEEN IDENTIFIED BY THE TSE AS OF THE ADOPTION OF ELECTRONIC VOTING MACHINES (EVMs)?

Electronic voting machines (EVMs) were adopted in Brazil during the elections of 1996. After 22 years, alleged frauds have been reported, but so far none has been confirmed. The TSE and other agencies invested in the constitutional right to investigate Brazilian elections, including the Brazilian Prosecution Service and the Federal Police, have come to that conclusion after carrying out independent audits of e-voting machines.

The party defeated at the 2014 presidential elections conducted an extensive auditing of the elections. The results of all the country's voting machines were made available, and the party's team had direct access to voting machines and other materials. After six months of work, its conclusion was that the official results corresponded faithfully to the votes registered in every voting machine, i.e., that there was no fraud in the vote count.

Indeed, the computerization of Brazilian elections led to the elimination of numerous unlawful maneuvers and deviations that resulted in a high number of electoral fraud cases. As of the single computerized registration of voters in 1985 until the adoption of the biometric identification of voters, Electoral Courts have adopted countless anti-fraud mechanisms.

# 6. WHY HAVEN´T OTHER COUNTRIES ADOPTED THE VOTING MACHINE MODEL USED IN BRAZIL?

Brazil has not chosen an e-voting machine model based on the products that were already manufactured and commercialized in the market. Brazilian e-voting machines feature a unique design, and were developed to meet the needs of the domestic market, and not to be traded abroad.

Since the adoption of e-voting machines in 1996, many different countries have addressed the Superior Electoral Court with the aim of learning more about the Brazilian EVM and eventually adopting this innovative Brazilian technology. Partnerships were established in some cases with the aim of sharing knowledge among different nations. Since then, electronic voting has been adopted by many countries and, obviously, each country has performed the technological adjustments that they deemed appropriate to introduce such technology to their respective legislation, culture and economy.

Past partnerships established with other countries included the lending of Brazilian EVMs and the necessary software adjustments to comply with the legislation of each partner country. In practice, the Superior Electoral Court was responsible for providing software and hardware support during the organization of elections in these countries, being then duly monitored and inspected by local authorities. Unfortunately, budgetary and personnel limitations led the Superior Electoral Court to shut these partnership program. After that, many

countries have failed in developing their own e-voting technology, and ended up abandoning the electronic vote.

After exchanging experiences with the Superior Electoral Court, some countries either succeeded in developing their own computerized systems or came to the conclusion that the cost associated with the implementation of e-voting was too high – it may be extremely expensive to adopt e-voting practices in places where the number of electoral fraud cases is very low or with a reduced number of registered voters. Whereas many countries currently use e-vote on a regular basis; other countries are still testing and developing their own electoral solutions.

# 7. WHAT IS THE DIGITAL RECORD OF THE VOTE (RDV)?

The Digital Record of the Vote (RDV) is the file this file, a report called "zerésima" – a report that indicates that no vote has been cast yet in the e-voting machine – is generated. The machine bulletin [Boletim de urna] – a report that features the vote count of the polling station where the EVM has been place – also uses RDV data.

The RDV file has two distinct features:

- the vote is recorded exactly as it was typed by the voter: the RDV fi le solely records the information typed by voters in e-voting machines, and that is all, there is no additional processing or information (it is not possible to identify voters based on vote information recorded in a RDV fi le). The RDV fi le is only used after polls close in order to generate a machine bulletin and thus tabulate the votes cast for each candidate or party and the total of void and blank votes. Given that the RDV file records exactly what voters type, it constitutes a relevant tool for auditing and verification purposes of the total votes of a given polling station; and
- the record of the vote ensures its secrecy: similarly to those old ballot boxes made of canvas, inside which paper ballots would be all scrambled, making it impossible to link paper ballots to the voters who had cast them, the RDV file randomly records the votes cast. The votes for each elective office are stored in a different position, rendering it impossible to make any association of the

votes cast or to associate such votes with the sequence of voters that show up to vote.

Political parties and coalitions are entitled to have copies of the RDV file of any e-voting machine they choose. After being given copies of RDV files and based on the specifications of their format, which is determined by Electoral Courts, political parties and coalitions may develop their own apps to compare the official vote count of selected EVMs with the one generated by their own software programs.

# 8. WHY ARE VOTES NOT PRINTED? IS THE ELECTORAL JUSTICE BREACHING THE LAW?

The printed vote was instituted by Law n. 13.165/2015, its implementation originally intended to take place starting at the 2018 Elections. However, the Supreme Federal Court decided to suspend the Law's efficacy until a decision on its constitutionality was made. The Electoral Justice is thus prevented from implementing the printed vote.

The purposes of printed vote are as follows:

- to enhance the auditing capacity and provide for election recounts; and
- to allow voters to verify if their intentions match the votes forwarded to the TSE for subsequent tabulation.

With regard to audits, based on Brazilian Electronic Voting Machines (EVMs) samples, paper ballots would be counted and compared with the results delivered by EVMs. The applicable principle is that printed votes are more likely to be trusted than EVM results, for they could have been checked by the voters.

On the other hand, direct manipulation of paper ballots facilitates the occurrence of fraud, which would lead to conflicting results that are less reliable than those delivered by EVMs. In practice, attacks against the integrity of elections would be targeted at the paper audit trail instead of the electronic vote, resulting in the undue annulment of votes,

or even calls for new elections, while the will of the electors is perfectly kept undamaged on the electronic records.

Just as voting practices have evolved over time – from paper ballots to e-voting – it is also necessary that auditing procedures evolve. There are other forms of audits, which are cheaper and safer than printed vote. Brazilian Electoral Courts already make use of some innovative auditing procedures, including the parallel vote and the inspection of the source code of its voting system six months before the selection of the voting software to be used during elections. The RDV file itself constitutes a significant auditing tool, being already used by political parties and coalitions that seek to check the integrity of EVMs tabulation of votes cast.

With regard to the issuance of printed receipts that detail in full the votes cast by voters, such possibility violates the principle of vote secrecy, a civil right set forth in the Federal Constitution, for voters could then disclose their votes to third parties. Even with a printed record, in an auditing procedure the individual voter does not have an unquestionable guarantee that his vote was effectively counted.

Since the passing of Law nº 13.165/2015, the Superior Electoral Court made all necessary efforts to implement the printed vote in time for the 2018 Elections: regulations were drafted, discussed and approved; software modifications were developed for the voting machine; and a company was contracted through public procurement as the provider of vote printers.

# 9. DOES THE BRAZILIAN E-VOTING MACHINE (EVM) SYSTEM KEEP A RECORD OF ITS OPERATIONS?

Brazilian e-voting machines (EVMs) are loaded with a file that keeps chronological record of main software operations – the log file. The log file records, inter alia, the following operations: the beginning and closing of voting hours, the issuance of reports, the execution of different apps, the adjustments on date and time, the implementation of contingency procedures and records that support the assessment of voting dynamics.

The log file constitutes an auditing and transparency mechanism that is made available by Electoral Courts. Indeed, log files provide for the analysis of EVM history, from the moment that apps are loaded in it until the closing of the polls during an occasional runoff. Just like RDV files, log files are also disclosed to political parties and coalitions so that they can make their own assessments of EVM events.

Based on the log files of the EVMs that were used during an election, the Superior Electoral Court gets to organize a powerful database, extracting valuable information on voting dynamics. Such information contribute to the improvement of many different procedures related to the operation of EVMs, including the loading of software programs in them, the identification of damaged components, the speed with which a vote is cast and recorded, and the dynamics of biometric apps. These procedures are aimed at ensuring enhanced assistance to voters on Election Day and at promoting faster EVM loading and inspection activities.

# 10. WHY IS THE TIME OF VOTING RECORDED BY THE BRAZILIAN EVOTING MACHINE (EVM) SYSTEM?

Brazilian EVMs record the time registered voters cast their vote without identifying said citizens. This is a valuable information for the calculation of managerial indicators like the average amount of time spent by each registered voter to cast their vote. To illustrate the aforementioned example, it is worth noting that such information provides the grounds for an analysis of the number of voters per polling station, which enables Electoral Courts to adjust this figure and thus reduce the formation of waiting lines, ensuring that voters get to vote undisturbed.

# 11. WHAT ARE PUBLIC SECURITY TESTS?

Public security tests are aimed at increasing the reliability, transparency and security of the casting and counting of votes in addition to promoting improvements in the electoral process as a whole. In that sense, it is worth noting that, in 2015, the TSE has published Resolution n. 23,444, which establishes that public security tests integrate Brazilian elections and are to be organized before every election, preferably during the second term of the year before the one in which an election is held.

When opening voting systems to ensure the inspection of source codes and the conduction of different testing programs, Electoral Courts seek to identify opportunities to improve the existing software security mechanisms, relying on the vision and experience of other public agencies, experts and concerned citizens.

The TSE uses public security tests as a supporting tool to promote the continuous improvement of electoral systems. Electoral Courts do not seek to encourage any form of competition nor market any single attribute of public testing participants.

# 12. DOES THE ISSUE WITH VOTE SHUFFLING, IDENTIFIED IN 2012, COMPROMISE THE INTEGRITY OF THE RESULTS? HAS IT BEEN CORRECTED?

A failure identified in the Public Security Test that took place in 2012 was related to RDV's vote shuffling algorithm, that is, the order in which each vote cast is recorded. In any way is vote count affected by the functioning of that mechanism, so vote total is to be trusted.

After the problem was identified, the said algorithm was immediately fixed and improved to correct its abnormal functioning. Numerous tests were exhaustively performed according to international standards in order to certify the quality of the newly improved algorithm. The certification tools included the DieHard suite, a randomness technique that tests the effectiveness of the shuffling of sequences. The tests also complied with the rules set forth by the National Institute of Standards and Technology (NIST).

The adjustment was open to broad scrutiny, including during the 2016 and 2017 editions of the Public Security Test. The current version of the software has proven to be robust and has no longer been criticized.

# 13. HAVE THE ISSUES IDENTIFIED IN 2017 BEEN CORRECTED?

The issues identified during the 2017 Public Security Test have already been corrected. The Superior Electoral Court gave full transparency to the findings of the researchers, publishing a detailed report at http://www.tse.jus.br/hotsites/teste-publico-seguranca-2017/arquivos/tps2017-relatoriotecnico.pdf. In May 2018, researchers were invited to verify the effectiveness of the adjustments to the software, concluding that everything had been corrected. The technical team of the Superior Electoral Court also afforded full transparency to the new adjustments by publishing a report at http://www.justicaeleitoral.jus.br/arquivos/relatorio-tecnico-tps-2017-1527192798117.

The periodic Public Security Tests have proven successful, and the specialized technical community has effectively helped the technical team of the Superior Electoral Court develop election systems that are even safer.

# 14. IS THE SOURCE CODE OF THE VOTING SOFTWARE OPEN TO THE COMMUNITY?

Experts representing political parties, along with the Brazilian Prosecution Service, the Brazilian Bar Association, the Federal Police and other entities, are currently allowed to access the source code of the Voting Software and the entire set of apps that are loaded in Brazilian e-voting machines (EVMs). Thus, one cannot question about transparency regarding the source code. Yet, the Superior Electoral Court examines the possibility of ensuring greater access to the source code, enabling more citizens and institutions to check the correctness and integrity of the voting software.

# 15. ARE BRAZILIAN E-VOTING MACHINES (EVMs) 1ST GENERATION DEVICES? ARE 2ND AND 3RD GENERATION DEVICES SAFER?

Brazilian e-voting machines (EVMs) are innovative pieces of equipment that were first employed in the elections of 1996. EVMs hardware and software design was developed and keeps on being improved by the Superior Electoral Court, which has counted on the support of academics since the first conceptual drafts of EVMs were prepared until their most recent updates. EVMs constitute a project that was entirely developed in Brazil and remain being continuously enhanced. The TSE adjudicated the manufacturing of these machines to a company hired after winning a public bidding organized by the Court.

The denomination "generations" of e-voting machines, which is often used as a market strategy to promote sales of newer devices, is commonly associated with the way the system operates – direct recording electronic voting system, like the one used by Brazilian EVMs; document-based ballot voting system which scans votes cast (e.g. a paper ballot that gets to be scanned); or voter-verified paper audit trail (the voting machine may print a receipt that is either retained by the voter or stored within the machine). It is worth noting that the last two systems are associated with the "secondgeneration" of voting devices. These different operating systems were employed by different countries at different moments, requiring different technologies, being it impossible to establish correlations in the way they evolved or to state

that a certain system is safer than the other. Furthermore, be it a paper ballot or a voting receipt, the materialization of the vote in a piece of paper may have its effectiveness as an auditing tool questioned just like it happened prior to the introduction of e-voting practices. The “third generation” is said to provide voters with a verification mechanism regarding the inclusion of their vote in the tabulation system.

In case the mechanism fails to protect the secrecy of the vote, which is extensive to the voter him/herself, this voter may be forced to vote and to hand in the voting receipt to a third party. In addition to that, if voters are solely allowed to check whether their votes were tabulated in a computerized system, the issue regarding the blind trust that voters were required to have in the voting software, which was vastly criticized for “first generation” devices, is once again a problem to be tackled.

Brazilian EVMs were designed to prioritize hardware and software security, featuring many different auditing mechanisms. They constitute a modern product and are continuously improved, following their own evolvement path. Biometric readers, storage media, more powerful and reliable processors, and cryptographic hardware are just some of the updates implemented over the past few years. Indeed, these technological developments significantly increase the reliability and security of e-vote.

# 16. WHAT IS THE ADH SOFTWARE PROGRAM? IS IT POSSIBLE TO USE IT TO CHANGE THE VOTES CAST IN AN E-VOTING MACHINE (EVM)?

The Date and Time Adjustment app (ADH) is loaded in Brazilian EVMs and is used to perform adjustments in the clock of said machines. The ADH app is used in cases here the operator has set incorrect date and time when loading an EVM that will be later used in elections. It is also used in case an EVM clock features a battery problem and displays incorrect time. It is not possible to use the ADH app to alter the votes cast in an EVM.

An EVM clock must be precise and accurate as some operations depend on it to be appropriately executed. Such operations include the following:

- authorization to issue a report called *"zerésima"* as of 7 a.m. on Election Day;
- authorization to enable registered voters to cast their vote as of 8 a.m. on Election Day; and
- authorization to close the vote as of 5 p.m. on Election Day.

It is not possible to use the ADH app to hack data stored in EVMs. Nevertheless, rumor has it that an alleged fraud case would involve the use of the ADH app. The alleged attack would occur as follows:

- the hacker would be granted access to both an EVM loaded with voting apps before elections were held and a media designed to activate the ADH app;
- s/he would use the ADH app to forward the EVM clock to the date and time scheduled for the beginning of voting hours;
- s/he would promote the insertion of spurious votes in the EVM until the time scheduled for the closing of the polls;
- the hacker would remove the media containing the spurious total and would keep it safe until Election Day;
- s/he would use the ADH app once again to adjust the EVM clock, setting the accurate date and time, would insert an empty media in the EVM for vote recording purposes and would seal the machine;
- on Election Day, after being placed in the corresponding polling station, this EVM would normally record the votes cast in it, but by the end of the vote, instead of using the media that recorded the votes in the transmission of the total of that specific polling station, one would use the media that contained spurious results instead.

All things considered, the thesis detailed above indicates that the control used to record the votes cast in an EVM is based solely on actual date and time. As it turns out, that is not true.

The *Voting Software* holds the last executed operation. Such attribute means that after the vote is closed, the software is blocked in the EVM, preventing the recording of new votes until the EVM is configured for an occasional runoff , that is, until it is prepared to be used in a new election. Furthermore, under no circumstances does the Voting Software erase or reset the records stored in the RDV file, which contains every vote that

has been cast in the EVM. Indeed, the voting software makes use of the RDV to issue the report called “zerésima”, indicating that no vote has been cast yet in that EVM.

Finally, even in the event that the removable media were switched, leading to two different results, the result printed in the machine bulletin of the corresponding polling station would not match the tabulated one. Party inspectors – or any concerned citizen, for that matter – could easily compare the official vote count of a said EVM with the result published in the respective polling station, being the latter the actual and correct total.

# 17. IS IT TRUE THAT THERE IS A SINGLE KEY DESIGNED TO PROTECT ALL E-VOTING MACHINE (EVM) MEDIA? IF SOMEONE HAD ACCESS TO THIS ENCRYPTION KEY WOULD THEY BE ABLE TO ALTER DATA STORED IN SAID MEDIA?

Some media inserted in e-voting machines feature a general mechanism that conceals information, which constitutes file system cryptography. The aforementioned media refer to EVM memory cards (internal and external), containing both the operational system and EVM apps (internal card), and in which information on voters, candidates and vote total are recorded (internal and external cards).

The purpose of fi le system cryptography is to set an additional barrier to an external threat perpetrated by a hacker with little or no knowledge on the organization of EVM software. That would set up difficulties for a potential hacker willing to make an assessment of media contents.

The file system cryptography of all memory cards uses a single key. In case there was more than one key, it would be impossible to perform contingency procedures, that is, to replace a damaged EVM by another one in perfect condition, which would resume the vote from the point where it was when it got interrupted. Furthermore, if there was more than one key, EVM audits would be compromised. However, it is incorrect to

state that if someone was in possession of the key to the fi le system they would be capable of generating media featuring “different contents”.

It is worth noting that the fi le system cryptography is not the mechanism upon which the security of all EVM apps is based. As a matter of fact, all fi les that require integrity and authenticity are digitally signed. That is the case, for instance, of EVM apps and files containing information on voters and candidates, the machine bulletin and the digital record of the vote. In addition to that, files that require secrecy are encrypted. In all such cases, different keys are used. These signature and cryptography mechanisms are the tools that prevent any modification in EVM media contents.

# 18. DOES COMPANY SMARTMATIC PRODUCE THE BRAZILIAN VOTING MACHINES AND HANDLE THE ENTIRE ELECTORAL PROCESS?

The Brazilian electronic voting machine was never produced by company Smartmatic. At the conception of electronic voting in Brazil, between 1995 and 1996, the hardware and software projects were developed by a group of data processing, electronics and communication experts from the Electoral Justice, the Armed Forces, the Ministry of Science and Technology, the Airforce Institute of Technology (ITA), the National Institute of Airspace Research (INPE) and the Ministry of Communications.

Since then, the manufacturing of the electronic voting machines is made by companies contracted in public procurements that are completely transparent and auditable. Smartmatic never won any of these contracts.

Besides, all software used in the elections is developed directly by the Superior Electoral Court team. The operation of all systems, i.e., the management of the whole electoral process, is handled exclusively by members of the Superior Electoral Court and the Regional Electoral Courts at all cases, not delegated to any contractors.


Printed on coated paper Couché 150g/m² (cover) and Couché 90g/m² (internal pages). The font used was Source Sans Pro size 11, line spacing of 16 points.


Tribunal
Superior
Eleitoral