TRUST IN ICT FOR THE PUBLIC SECTOR: E-VOTING IN BRAZIL'S 2014 ELECTION

Luiz Fernando Abel[1]

Apart from the numerous works on ICT implementation in the public sector and its subsequent success or failure, there is a lack of specialised literature to address a case where technology has been successfully implemented by the government, but starts to face trust problems. This is the status of e-voting in Brazil, more specifically, during the 2014 presidential elections. This research looks at the conditions for trust in ICT in the public sector and provides an assessment of the Brazilian case, aiming at enhancing the debate on why e-voting should be trusted or not. To do so, a framework is proposed by the author, based on previous findings of the literature. The discussion includes points mentioned by Brazilian authorities and citizens' perceptions.

Keywords: election; Brazil; trust; electronic voting; technology; public sector.

CONFIANÇA EM TICS NO SETOR PÚBLICO: O VOTO ELETRÔNICO NAS ELEIÇÕES BRASILEIRAS DE 2014

Apesar do grande número de trabalhos sobre a implementação de tecnologias de informação e comunicação (TICs) no setor público, e seu subsequente sucesso ou falha, é escassa a literatura especializada que aborda o caso em que a tecnologia foi implementada com sucesso, mas passa por problemas de confiança. Este é o estado do voto eletrônico no Brasil, mais especificamente nas eleições presidenciais de 2014. Esta pesquisa aborda as condições para confiança em TICs no setor público e oferece uma avaliação do caso brasileiro, com o objetivo de engrandecer o debate sobre por que o voto eletrônico deve ser confiável ou não. Para isso, um quadro de análise é proposto pelo autor, baseado em contribuições anteriores da literatura. A argumentação inclui pontos mencionados pelas autoridades brasileiras responsáveis e percepções dos cidadãos sobre o tema.

Palavras-chave: eleição; Brasil; confiança; voto eletrônico; tecnologia; setor público.

CONFIANZA EN LAS TIC EN EL SECTOR PÚBLICO: EL VOTO ELECTRÓNICO EN LAS ELECCIONES BRASILEÑAS DE 2014

A pesar del gran número de estudios sobre la aplicación de las TIC en el sector público, y su posterior éxito o el fracaso, hay poca literatura que aborda el caso en que la tecnología se ha aplicado con éxito, pero pasa por problemas de confianza. Este es el estado del voto electrónico en Brasil, específicamente en las elecciones presidenciales de 2014. Esta investigación se ocupa de las condiciones para la confianza en las TIC en el sector público y proporciona una evaluación de Brasil, con el objetivo de potenciar el debate sobre por qué el voto electrónico debe ser de confianza o no. Para eso, un marco analítico es propuesto por el autor, basado en las contribuciones anteriores

1. Master of international management from Fundação Getulio Vargas – Escola de Administração de Empresas de São Paulo (FGV-EAESP). Double master's degree in management from the London School of Economics and Political Science (LSE) with Università Commerciale Luigi Bocconi. Bachelor of public administration from FGV-EAESP. E-mail: <luizfernandoabel@gmail.com>.

de la literatura. El argumento incluye puntos mencionados por las autoridades brasileñas y percepciones de ciudadanos del sujeto.

Palabras clave: elección; Brasil; confianza; voto electrónico; tecnología; sector público.

CONFIANCE DANS LES TIC AU SECTEUR PUBLIC: LE VOTE ÉLECTRONIQUE AU COURS DES ÉLECTIONS BRÉSILIENNES DE 2014

Outre les nombreux travaux sur la mise en œuvre des TIC dans le secteur public, et son succès ou l'échec, il y a un manque de littérature spécialisée pour traiter un cas où la technologie a été mis en œuvre avec succès par le gouvernement, mais commence à faire face à des problèmes de confiance. Ceci est le statut du vote électronique au Brésil, plus précisément au cours des 2014 élections présidentielles. Cette recherche porte sur les conditions de la confiance dans les TIC dans le secteur public et fournit une évaluation du cas du Brésil, visant à renforcer le débat sur la raison pour laquelle le vote électronique doit être digne de confiance ou non. Pour ce faire, un cadre analytique est proposé par l'auteur, sur la base des constatations antérieures de la littérature. La discussion inclut des points mentionnés par les autorités brésiliennes et les perceptions des citoyens.

Mots-clés: election; Brésil; confiance; vote électronique; technologie; secteur public.

JEL: O38; D72; D78; D83; H11.

1 INTRODUCTION

New technologies have been changing the way governments execute their policies around the globe. With the introduction of new, digital systems, the provision of services to citizens, as well as its internal organisation, have been performed in different ways than the traditional practice. As part of this transformation, new forms of conducting the electoral process have been created in some the world's democracies, with electronic voting systems replacing the paper ballots.

However, along with e-voting, a number of concerns have been raised as to whether the use of technology is reliable to execute democratic processes, such as general elections, plebiscites and referenda. A different set of ICT systems, voting machines, and even internet voting, were created and used in different countries in the five continents, with some nations opting back to manual procedures after hacking threats were identified in the electronic experience. Thus, the issue of trust in information systems for the public sector has been a big part in the continuing debate on e-voting.

Given that, this paper will discuss the concepts of trust in the light of e-voting for general elections in Brazil, one of the world's largest democracies. In particular, it will analyse the impact of this policy in the 2014 presidential elections, considering the citizens' perception of trust in digital voting systems used by the Brazilian government.

In order to carry this research, a review of other authors' work on the topic of trust related to information systems in the public sector will be included, as to summarise previous contributions to the discussion and clarify concepts that will be used in the analysis. To this extent, authors engaged in the debate of this topic and e-voting will be prioritised as to other publications addressing a more general of the topic or focused on other means of e-government.

Finally, extensive secondary data from public databases in Brazil, such as the Federal institution in charge of the electoral policies and procedures (TSE, in the Portuguese acronym), academic journals and specialised literature, as well as the press, will be used in the case study.

It should be pointed that this research will also discuss the limitations involved when looking at this issue. However, these limitations should not be an obstacle to the expected conclusion of this work, which aims at contributing to the debate on the issue of trust in the Brazilian e-voting system in 2014.

2 LITERATURE REVIEW

The general literature on e-government tends to focus on disruptive technologies and its effects on government bodies, mentioning the expected transformation brought by them. More specifically, in terms of e-voting, a significant amount of research gives attention to the economic factors behind it, the ideal stage of democratic development to use it, the implementation procedures and safety requirements to introduce e-voting technologies, as well as the scandals involving its usage.

This research, however, will focus on one of the "after-implementation" matters related to e-voting, the issue of trust. After all, even after being successfully implemented in the public sector, ICTs could not to be trusted by the citizens – even after years of use –, and that would still be a failure. In the light of elections, this matter is undoubtedly crucial, given that "citizen trust and participation in the political system are necessary for the stability of democratic regimes, as distrust and disengagement can lead to civil violence and regime change" (Marx, Pons and Suri, 2015).

Esteve, Goldsmith and Turner (2012) introduce trust as representing a rational decision on the part of the trustor to trust the trustee. More than that, the authors point out that it comes with a possibility that the trustor may not achieve anticipated outcomes when placing trust in the trustee, entailing "an unavoidable element of risk and potential doubt" (Lewis and Weigert, 1985).

In addition, it is possible to say that "trust entails vulnerabilities and the possibility of an exploitation of the relationship between the trustor and trustee,

but the trustor must believe that this exposure will not be exploited in a manner detrimental to their interests" (Corritore, Kracher and Wiedenbeck, 2003).

Thus, according to professor Sandra Jovchelovitch, from the London School of Economics and Political Science, "trust cannot be understood outside the cultural and social contexts in which it takes shape and in which it is exercised as social practice" (Jovchelovitch, 2008).

The willingness of citizens to rely on a service will depend on "their judgment of the overall social and political context that sustains them and is shaped on the basis of more general beliefs and political predispositions" (Avgerou *et al.*, 2009).

The Sans Institute (2004) mentions that in order for a democratic system to function voters must believe the entire election process from start to finish is fair. It is said that even in the most contested elections, "the system works because the electorate is confident that each vote is counted and every ballot possesses an intrinsic value" (*op. cit.*).

So, when it comes to voting systems,

> trust may be conceived as the certainty, held by all electoral stakeholders, that the whole process takes place observing the desired assumptions, specifically with regard to the requirements that voting systems must meet, thus attesting the quality of the system and ensuring compliance with security parameters (Nogueira and Sá, 2012).

More than that, "trust in elections entails judgment of the trustworthiness of a larger range of activities than voting, including candidates' political manifestos and campaigns" (Moisés, 2006).

In that sense, professor Chrisanthi Avgerou (2013) explains that "trust in e-voting emerges from and relies on government agents' and citizens' democratic engagement. A country's confidence in its democratic polity affects trust in the introduction and subsequent practice of electoral innovation such as e-voting".

Therefore, in this work it will be first analysed the defining elements proposed by the literature to assess if an e-voting technology is to be trusted or not, and then, through the analysis of the Brazilian 2014 presidential elections, these elements will be tested, in addition with a better understanding of the other dimensions (citizens' beliefs and perceptions) to enhance the debate why e-voting in Brazil should be trusted or not.

3 ANALYTICAL FRAMEWORK

There are different aspects to be covered in order to better understand the impact of trust on e-voting. Some authors explain that a set of requirements is needed, by listing them, and others provide a more schematic approach to address this matter.

The aim of this research is to explore, with the models proposed by the literature on trust and e-voting, under which circumstances the governmental use of ICT (via electronic voting system) is to be trusted, as to guide the analysis of the case of the 2014 presidential elections in Brazil.

Given that "the production of trust in ICT-mediated government services relies on citizens' perceptions of their trustworthiness" (Avgerou *et al.*, 2009), and the perception of trustworthiness relies on the indicators used to describe the aspects of trustworthiness related to the technology, it is crucial to know what are these indicators, that is, the factors impacting trust in e-voting.

It is worth noting that these indicators may be given a different perception when informed by the media, for example, or others, and by the citizens' own experience of the service. This is better explained by prof. Avgerou's adaptation of the Kee and Knox's model to trust in e-voting (figure 1).

The model "depicts the composite entity of the electoral authority and the e-voting technology as the object of trust" (Avgerou, 2013), and includes the citizens' disposition to trust in political institutions, influenced by their previous experiences as a component to this perception of trustworthiness in the e-voting system and electoral authorities.

FIGURE 1
Trust conditions and relationship for e-voting
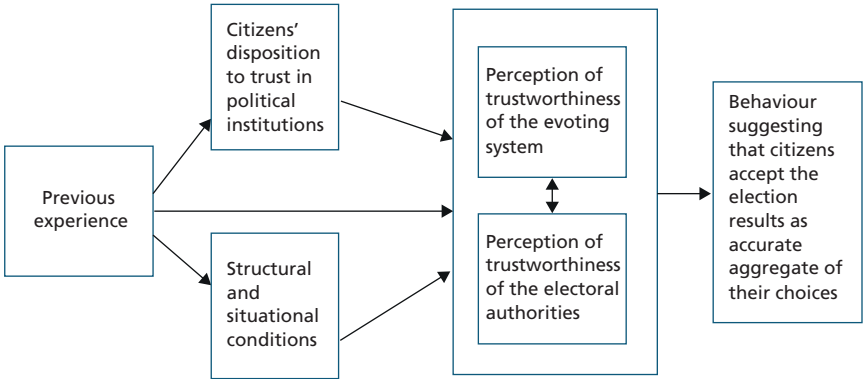
Source: Avgerou (2013).

Still, the structural and situational conditions are to be covered in this section, as "there must be trust in the process itself for the results to be trusted, otherwise even legitimate results may be rejected" (Esteve, Goldsmith and Turner, 2012). So, this analytical framework will address the indicators proposed by the literature to assess the e-voting system for now.

Rodrigues Filho (2010) presents two factors to be taken into consideration in the analysis of trust in e-voting: security and investment. As he mentions the electronic voting technologies are susceptible to failures and frauds, if you have a high level of investment and, by that, guarantee secure mechanisms (for example, for vote counting), then they should be trusted by its users.

Following this generalist view, Esteve, Goldsmith and Turner (2012) explain that the two challenges faced are to have an election which reflects the will of the voters, while, at the same time, is convincing to key electoral stakeholders that it has been able to do so. Among the factors to establish and maintaining trust cited by the authors, security is also emphasised to guarantee the integrity of the system, through transparency, testing, certification, evaluation – to name a few –, while the costs are seen (non-exclusively) as a disadvantage.

To this extent of analysis, prof. Avgerou goes further and points out that e-government technologies must be perceived to be "useful and easy to use, as well as secure" (Avgerou *et al.,* 2009). The usefulness is related to performance improvements (for example, efficiency, effectiveness, transparency) and security, as the need "for institutional mechanisms that safeguard integrity of transactions" (for example, certification) (*op. cit.*).

Neumann (2004), also included by the Sans Institute (2004), cite the aspects of distrust that have made fully electronic voting systems controversial, such as the weakness of the certifications (by vendor-commissioned evaluations) and the inability of black-box testing (on top of the general secrecy of evaluations). To this point, he lists a basic set of standards by which an electronic voting system could be judged, because many electronic voting systems, even when certified, "raise serious questions about security, accuracy, and reliability" (Sans Institute, 2004).

The first criteria is system integrity, if "each vote is recorded accurately and tamper proof" (Neumann, 2004). As the vote is recorded, the system should also ensure data confidentiality and voter anonymity. Other criteria to guarantee security are operator authentication, disclosability – a process open for inspection –, as well as system reliability, in terms of shielding against possible attacks, when the system is made available. Also, "the user interface presented to voters and election officials must be easy to use and be designed to prevent accidental and intentional misuse or improper configuration" (Sans Institute, 2004).

These points are further developed in Schneier's article, with four requirements named. The first two, already mentioned, refer to the accuracy of the process, or "how well the process translates voter intent into appropriately counted votes" (Scheneier, 2004), and anonymity of voters, the secrecy of votes. Inside the former, security is included as it "should be impossible to change someone else's vote, stuff ballots, destroy votes, or otherwise affect the accuracy of the final tally" (Schneier, 2004).

In addition, the author suggests that voting systems should be scalable, as to handle large elections (for example, Brazil, India and the United States), and the feature of speed, that is, to produce fast results. Both senses are set to be improved by the efficiency brought by electronic voting machines.

Finally, Nogueira and Sá (2012) explain that several are the requirements "in order to maintain the security levels of the paper ballot method and the degree of trust people place in the voting process", and point out that for "a completely trustworthy e-voting system – one that does not lose, add, alter, disregard, or disclose ballots – there is also the need to ensure that voting stakeholders also trust the system" (*op. cit.*).

A set of twelve requirements is first presented, in order to analyse and evaluate the adequacy of e-voting systems, but then are grouped into five core requirements by the authors: Authenticity, singularity, anonymity, integrity, uncoercibility. In another words, these are the items already seen in the literature previously mentioned, if authenticity is considered as security, like in Neumann's research, as well as the concepts of anonymity and integrity (or accuracy).

But as interviews were also carried with people of interest for the topic (engineers and experts in electronics, IS and technologies), the authors confirmed those and were informed of two other dimensions: usability, as well as accessibility and convenience.

As a conclusion, the factors identified by these last three works (table 1) provide a clear set of concepts that would be a close fit to the outcome of a trusted e-voting election. Given that, if the items identified and highlighted by these authors are combined and applied, it would be possible to oversee the areas of trust or distrust in Brazil's e-voting system.

TABLE 1
Comparison of core requirements for e-voting extracted from the literature

	Neumann (2004)	Schneier (2004)	Nogueira and Sá (2012)
Accuracy[1]	X	X	X
Anonymity	X		X
Easy to use[2]	X		X
Scalable		X	
Security[3]	X	X	X
Speed		X	

Author's elaboration.
[1] Also included by Esteve, Goldsmith and Turner (2012). Referred as "system integrity" by Neumann (2004) and Nogueira and Sá (2012).
[2] Also included by Avgerou (*et al.,* 2009). Referred as "usability; acessibility and convenience" by Nogueira and Soares (2012).
[3] Included by all authors.

In such matter, to depict the complexity of the case, an analytical framework was created (table 2), based on these findings of the literature, that will assist in the comprehension of trust, or lack of it, in the use of e-voting in Brazil for the 2014 presidential elections.

TABLE 2
Framework for assessing trust in e-voting systems

Trust factor	Definition[1]	Found	Not found
Accuracy	Votes should not be able to be modified or destroyed.		
Anonymity	It should not be possible to associate a vote to a voter.		
Easy to use	E-voting system should be accessible without requiring specific abilities or equipment (incl. people with special needs).		
Scalable	E-voting system should be able to handle large elections.		
Security	E-voting system should have operator authentication (incl. authenticity and singularity), disclosability (transparency), system reliability when made available (testing, certification, evaluation).		
Speed	E-voting system should be able to produce fast results.		

Author's elaboration.
[1] As summarised by Neumann (2004), Schneier (2004) and Nogueira and Sá (2012).

This framework covers the six core trust factors, as defined by the literature review, which will be an important tool for the analysis proposed. Each of the trust factors should be checked against the e-voting system and then signalised if found or not found accordingly.

Thus, having already introduced the issue of trust in information systems of the public sector and its connection with the e-voting policy, this paper will next review the main aspects of the Brazilian case, pertinent to the issue of trust in e-voting, and then analyse it through the lens of the framework presented.

4 THE CASE STUDY

As a result of a project financed by the World Bank and developed by the Supreme Electoral Court of Brazil (TSE, in the Portuguese acronym), electronic voting was introduced in the Brazilian municipal elections of 1996, aiming at extinguishing fraud and improving political participation, which used to be low due to the country's share of illiterate population (Esteve, Goldsmith and Turner, 2012).

The TSE, as the federal institution in charge of the electoral policies and procedures, wrote the terms of reference for the system, which was at first used in the 26 state capitals and a small number of secondary cities, mainly in the states of Sao Paulo, Rio de Janeiro and Minas Gerais (Brazil, 1996). Following the success of the procedure, the e-voting machines started, from the year 2000, to be used nationwide on all general and municipal elections held in Brazil, plus in a referendum held in 2005.

Electronic voting became a source of national pride, as Brazil became the first country in the world to deploy a fully computerized balloting countrywide. After that, a number of democratic nations adopted e-voting, such as France, Argentina, Japan and India, with some countries later discontinuing its use, like Italy, Australia and Norway (Esteve, Goldsmith and Turner, 2012).

Elections in Brazil have been considered to be "trouble-free", in comparison to other Latin American countries, "such as Mexico, where the legitimacy of elections results are often disputed creating political instability" (Avgerou *et al.*, 2009). However, after a fraud was found in the Brazilian Senate's internal electronic system, in 2001, suspicion also affected the e-voting ballot boxes. Paper trail was adopted by law and system provider "Diebold-Procomp" partnered with Microsoft in 2002 to have Windows CE installed – changing to Linux in 2004. The Brazilian electoral law was revised every second year, in order to enact in law the electronic ballot box evolution and changing specifications. Formal complaints were also filed in the 2002 elections by three parties, including the largest in Brazil (Partido do Movimento Democrático Brasileiro – PMDB), against the e-voting system, but the TSE, which decides on legal challenges against ballots' results as well, rejected all of them.
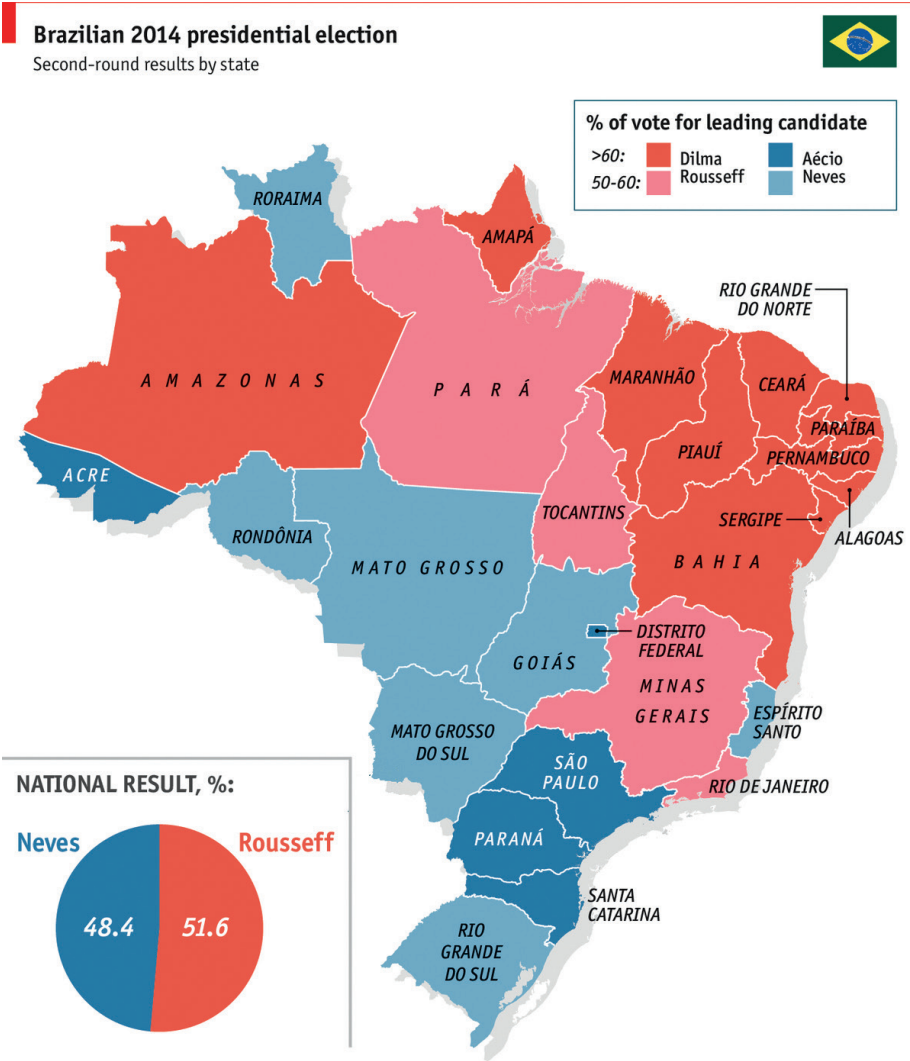
Still, in 2014, after the closest polling results in a Brazilian presidential election since 1989 (see figure 2), and as victory came for same party that had been in power for twelve years (Partido dos Trabalhadores – PT), fraud suspicion became part of a nationwide discussion over the e-voting machines used.

The winning candidate Dilma Rousseff has not been entirely accepted by the Brazilian population, and as the main opposition party (Partido da Social Democracia Brasileira – PSDB) requested an audit of the election results, the number of citizen's questioning the trust of this policy were increased.

Up to this point, e-voting in Brazil has been fairly accepted by the population. According to a survey published in 2009 by the TSE (Brazil, 2009), 97% of the users approved the e-voting ballot box. The Electoral Court itself also appeared to be a trustworthy guarantor of the election process as another survey by NGOs Instituto Nexus and TV Cultura in 2004 showed 81.5% of respondents to have full or partial confidence in the institution, with 89.5% also judging positively the services it provides.

However, it could be argued that a general positive attitude towards ICT in Brazil, partially because of familiarized citizens with ICT being as a trusted facilitator of services during the hyperinflation period of the 1980s, helped the perception of trustworthiness enjoyed by the electronic voting system so far (Avgerou *et al.*, 2009).

FIGURE 2
2014 election results for Brazilian presidency

Brazilian 2014 presidential election
Second-round results by state

% of vote for leading candidate

>60:	Dilma	Aécio
50-60:	Rousseff	Neves

RORAIMA

AMAPÁ

RIO GRANDE DO NORTE

AMAZONAS

PARÁ

MARANHÃO   CEARÁ

PARAÍBA

ACRE

PIAUÍ   PERNAMBUCO

RONDÔNIA

TOCANTINS

SERGIPE   ALAGOAS

MATO GROSSO

BAHIA

DISTRITO FEDERAL

GOIÁS

MINAS GERAIS

ESPÍRITO SANTO

MATO GROSSO DO SUL

SÃO PAULO

RIO DE JANEIRO

PARANÁ

SANTA CATARINA

RIO GRANDE DO SUL

NATIONAL RESULT, %:

Neves   **Rousseff**

48.4   51.6

Source: A riven... (2014).
Publisher's note: image whose layout and texts could not be formatted and proofread due to the technical characteristics of the original files provided by the authors for publication.

Some Brazilian academics and scientists say, basing their arguments on the security and risks of this kind of system in the United States (Rodrigues Filho, 2010), that the security of electronic voting is susceptible to failures and frauds.

In addition, "some Brazilian experts have questioned the current e-voting system and its security through internet sites, forums, articles and books" (Maneschy, 2000; Brunazo Filho and Cortiz, 2006), accusing the TSE of "opening the doors for new and sophisticated frauds much more serious than the traditional ones" (Maneschy, 2000).

On the other hand, the Brazilian e-voting system still has several qualities that make it, and consequently the elections, perceived to be trustworthy. In fact, it does have voter identification mechanisms, apart from system testing and certifications mechanisms, as well as transparency mechanisms (Esteve, Goldsmith and Turner, 2012).

More than that, Brazilian elections have been considered of high integrity level by The Electoral Integrity Project, developed by the University of Harvard in partnership with the University of Sydney in 2015. Brazil's mark of 74.1, out of 100, was higher than the average in the Americas, ranking higher than Italy, Japan and the United States.

Therefore, a deeper analysis is to be executed in order to enhance the debate on whether the results of the Brazilian 2014 presidential elections are to be trusted or not. Firstly, it will be examined if the trust factors introduced in the previous item are found or not in this case study, including the arguments for perceiving the e-voting system trustworthy or not. It will be also discussed other conditions that may have influenced the trustworthiness of the system, that is, whether people's beliefs about the trustworthiness of the government that enacts the ICT-mediated service could have impacted the citizens' predisposition of trust in the electronic voting policy.

5 ANALYSIS

Despite the general status of trust in the Brazilian election process and authorities, including the e-voting ballot box, after 2014 there is an on-going debate on whether e-voting should be maintained or not, and a considerable controversy if the machines, as well the entire policy, are reliable enough for the process.

This goes is line with the argument of civil society pressure groups, such as the "Open Rights Group" in the United Kingdom, the word of specialists, reported in Brazil and in "strong democratic traditions, such as the United States and Canada" (Rodrigues Filho, Alexander and Batista, 2006), the cases of recount and flawed trials published in the international media, as well as word of mouth from government oppositionists.

Yet, it goes against the arguments for the use of e-voting in Brazil, which include the benefits brought the use of ICT in the elections, studies' reports,

such as The Electoral Integrity Project, civil pressure groups, such as "WebRoots Democracy" in the United Kingdom, the word of specialists that consider it to be "safe enough" (Kobie, 2015), and the press covering the use of Brazilian e-voting ballot boxes and digital democracy, as well as the official audits and mechanisms explained by the official authorities, the TSE.

As a consequence, the analytical framework proposed by the literature review is to be applied, in order to resume the trust factors *vis-à-vis* the official information available on the case. As it already presents a clear divide, in terms of opinions relating to e-voting, and, thus, a clear issue of trust in the 2014 presidential elections in Brazil, the outcome of this analysis aims to clarify the points of trust and distrust, why it should be maintained or not.

The first trust factor is "accuracy", that is, the guarantee that votes will not be subject to change – not modified or destroyed –, and will reflect the citizens' preferences. In that sense, the TSE clarifies that one of the functions of the e-voting machines is vote recording, via digital vote registration (RDV), which produces a file where all votes are registered, after the "zero vote" trail is issued – before the first voter comes in. All the votes are then "registered exactly as typed by the voter" (Brazil, 2015). No processing or additional information is executed. The RDV will only be used after the time to vote is finished and a trail is issued with the sum of votes to each candidate, plus blanks and nulls. This file is a proof of accurate vote counting in that section.

To this extent, representatives of political parties, political scientists, and NGOs valued the system for reducing the percentage of spoilt votes due to unreadable handwriting, hence reducing fraud and enfranchising illiterate voters. "While the rate of invalid votes averaged 40% before electronic voting, it dropped to 7.6% in 2002" (Esteve, Goldsmith and Turner, 2012).

Secondly, the e-voting system should not make it possible to have a vote associated to a voter, proving anonymity to its users. Related to this matter, the TSE informs that a log file of the operations is indeed kept by the machine's software, however the register via RDV guarantees the secrecy of the vote, because each vote is recorded in a random position inside the file – "comparable to the shuffled cells in a traditional ballot box" (Brazil, 2015). This measure does not allow any kind association within votes, or between votes and the sequence of voters in that location.

More than that, knowledge on the software itself is strictly restricted to TSE's personnel, and even people responsible for the voting stations (*mesários*) cannot access it. The staff in charge of totalising the votes is not the same in charge of the software itself, and any attempt to access it could be monitored.

Next, it is important to check that the e-voting equipment is easy to use, as no specific abilities or further devices should be needed to cast a vote. This seems to be the case in Brazil, where the e-voting machine is equipped with a numerical keyboard, resembling a phone keyboard, which illiterate people can also be familiar with. This is the case of both the terminal used by the voter, as the other used for authentication purposes (see figure 3).

FIGURE 3
E-voting machine used in Brazil, with authentication terminal on top

Source: Bom... (2014).

Likewise, the "voting machine has a very simple interface, comprising an unambiguous presentation of voting options, confirmation and cancellation procedures, pictures of candidates and Braille coding on the buttons to secure universal access including illiterate and blind people" (Avgerou *et al.,* 2009). This has made a difference in the number of null votes, as complicated ballot papers were no longer used, and meant that all could use it, rich an poor, facilitating the democratic procedure.

Moving on to the scalability of the e-voting system, it seems not to be a problem for Brazilian case, as the country is the fourth largest democracy in the world (OECD, 2016). More than 140 million voters had to vote in 2014 (Brazil, 2014), or justify the absence, as voting is compulsory in Brazil.

The complexity of the elections is another key point, as voting sections are held as far as the Amazon region, and the machine can be transported to work on its internal battery or a car battery, aside from the standard electrical plug. It was even mentioned by the international media with astonishment that "the days of transporting paper election ballots through the Amazon by canoe were over" (Hamilton, 2002).

All in all, the elections appear to be run peacefully. As described by Avgerou *et al.* (2009), "the fast and uncrowded voting experience created a relaxed

and almost celebratory atmosphere at the voting stations. Many parents took their young children with them to the voting booth to show them how they used the machine".

In terms of security, operator authenticity in Brazil is made by the *mesários* checking the voter's ID and electoral card. This procedure was considered not to be satisfactory in terms of guaranteeing authenticity and singularity of the voter, which resulted in the implementation of biometric technology, as seen on figure 3. Nevertheless, only 15% of the voters were entitled to vote using the new procedure (Brazil, 2014), given that it demands prior relisting in the voting section. The states of Alagoas, Amapá, Sergipe and the Federal District were the sole members of the Brazilian Federation to have fully conducted it for the 2014 presidential elections.

The TSE claims it is not vulnerable to external attacks as it has no connection to external networks, such as internet, nor does it have wifi connection. Also, it is not possible to install unauthorised apps in the machine (Brazil, 2015). The system uses encryption techniques and physical security measures (for example, sealing of machines), plus universities audit the system, even though reports are not public.

The source code of the e-voting software in Brazil is available to a number of stakeholders (including the Prosecutor's Office, the Brazilian Bar Association – OAB, political parties, and technical representatives), in order to guarantee transparency on that matter and have more people to verify the system (Brazil, 2015).

One year prior to election day, public tests are held, and since TSE's resolution 23,444 edited in 2015, it became integral part of the Brazilian electoral system. However, it is important to note that for the 2014 elections, public tests were not conducted.

Then, 180 days before election day, the stakeholders are invited to analyse the software in a TSE-controlled environment, to digitally sign the software together with the TSE (Esteve, Goldsmith and Turner, 2012). A self-certification is performed as well, to ensure the correctness of the software, but highly criticised because it is not done by third parties (*op. cit.*).

On the eve of election day, State authorities randomly select 3% of the machines, by draws, and the selected machines conduct a filmed parallel election on election day, by the local TSE authorities (the TREs) with members of political parties and the media, and it must match the expected results.

Also, during the election procedures, a "zero vote" trail is issued to prove the machine's memory is clean and a paper trail is issued after the time to cast a vote is over, following a 2009 electoral law, to be manually counted and proven to be accurate.

Last but not least, the speed to count the votes. According to the literature, an e-voting system should be able to totalise votes quickly, in order to guarantee its credibility. In Brazil, citizens are used to having the results of election day before midnight. As it takes considerably less time with e-voting than it used to in the manual voting system, "96.7% judged positively the speed of the counting of votes" (Avgerou *et al.*, 2009).

During the second round of the 2014 presidential elections, results were 100% totalised by 15 minutes past midnight of the following day (Apuração..., 2014), that is, approximately seven hours after the election sections were closed. Furthermore, an official app was made available by the TSE (figure 4), allowing citizens to be updated in real time to the election results.

FIGURE 4
TSE's vote counting app in the Brazilian 2014 elections

As a matter of fact, it is possible to note that the Brazilian e-voting system has been able to incorporate most trust factors listed in the analytical framework (table 3). It has been found, according to official information, that five, out of the six core requirements, were evident from official data, while security was only partially covered in the Brazilian case.

TABLE 3
Assessment of trust in the Brazilian e-voting system (2014)

Trust factor	Definition[1]	Found	Not found
Accuracy	Votes should not be able to be modified or destroyed.	X	
Anonymity	It should not be possible to associate a vote to a voter.	X	
Easy to use	E-voting system should be accessible without requiring specific abilities or equipment (incl. people with special needs).	X	
Scalable	E-voting system should be able to handle large elections.	X	
Security	E-voting system should have operator authentication (incl. authenticity and singularity), disclosability (transparency), system reliability when made available (testing, certification, evaluation).	Partially	
Speed	E-voting system should be able to produce fast results.	X	

Author's elaboration.
[1] As summarised by Neumann (2004), Schneier (2004) and Nogueira and Sá (2012).

6 CONCLUSION

For the reasons presented, it would be conclusive that the Brazilian e-voting system could be trusted, including the 2014 election results it provided. The security factors affecting negatively the framework shown are related to authenticity and singularity – which is already being addressed by the new biometric policy –, the public tests – which were not held prior to the election in 2014, but as of 2015 are integral part of the election process –, and the issue of self-certification currently used, instead of third-party certification of security. If the Brazilian government, via TSE, implements changes to these points mentioned, as well as maintaining the others, it could have a complete list of trust factors and it would make less room for disputes over its voting results, as "the ability to demonstrate that it is trustworthy has a direct impact in the legitimacy and acceptance of the voting results" (Avgerou *et al.*, 2009)

Still, some academics, political parties and activists call for greater transparency of the system and refuse to accept the e-voting system as trustworthy. In this sense, it also needs to be considered that there were a number of concomitant negative events happening in Brazil during the election period that affected citizens' trust in the government. President Rousseff had failed to implement policies in the first turn and left room a for a resurgence of solved

problems, such as inflation and slow economic growth, bringing discredit to the government (Kawai, 2016). In a period of economic downturn, technology also came in the way, but it may not be exactly the motivation for the distrust scenario created in Brazil.

That is because, as mentioned by prof. Avgerou *et al.* (2009), the perception of trust does not rely solely on indicators used to describe aspects of trustworthiness, but rather, it depends on the cognitive and emotional capacity that individual citizens bring to bear on their experience of a service, or on informants, such as the Brazilian press. "All of these may misinterpret or misrepresent the resulting service, either towards misplaced trust, or towards excessive suspicion" (*op. cit.*).

Therefore, the context of the 2014 elections should also be better analysed, because there is a need to know how the government in power in 2014, and the situation of the country in that moment, influenced the discourse of trust in the e-voting technology. Lack of confidence in the government, in general, would mean suspicion over any of the features it uses, including technology and, hence, e-voting.

After all, none of the voting systems, electronic or not, is perfectly safe. In fact, the three points of possible distrust found in the Brazilian e-voting system, could also happen if the paper-based elections had been held in 2014. The fundamental factors of credibility, presented by the literature, seem to be met, including some of the security measures. So, it might have been safe enough to guarantee the conduction of the 2014 presidential elections.

REFERENCES

A RIVEN country. **The Economist**, Oct. 27, 2014. Available at: <https://goo.gl/TJh2YU>. Accessed: Feb. 10, 2016.

APURAÇÃO Eleições 2014: presidente 2º turno. **Folha de S. Paulo**, 2014. Available at: <https://goo.gl/FdkoL1>. Accessed: Mar. 12, 2016.

AVGEROU, C. Explaining trust in IT-mediated elections: a case study of e-voting in Brazil. **Journal of the Association for Information Systems**, v. 14, n. 8, p. 420-451, 2013.Available at: <https://goo.gl/iqV3fG>. Accessed: Mar. 16, 2016.

AVGEROU, C. *et al.* Interpreting the trustworthiness of government mediated by information and communication technology: lessons from electronic voting in Brazil. **Information Technology for Development**, v. 15, n. 2, p. 133-148, 2009.

BOM Dia MT: dicas sobre o processo de votação de urna eletrônica. **Rede Globo**, Aug. 8, 2014. Available at: <https://goo.gl/mGCYjq>. Accessed: Mar. 16, 2016.

BRAZIL. Tribunal Superior Eleitoral. **Municípios com votação eletrônica**. Brasília: TSE, 1996. Available at: <https://goo.gl/RzyNrF>. Accessed: Mar. 3, 2016.

_____. _____. **Justiça Eleitoral registra aumento do número de eleitores em 2014**. Brasília: TSE, 2014. Available at: <https://goo.gl/oVTbhX>. Accessed: Mar. 12, 2016.

_____. _____. **Urna Eletrônica tem aprovação de 97% dos eleitores**. Brasília: TSE, 2009. Available at: <https://goo.gl/RCf13X>. Accessed: Mar. 12, 2016.

_____. _____. **Sistema eletrônico de votação**: perguntas mais frequentes. 2nd ed. Brasília: TSE, 2015. Available at: <https://goo.gl/h1fcGP>. Accessed: Mar. 12, 2016.

BRUNAZO FILHO, A.; CORTIZ, M. A. **Fraudes e defesas no voto eletrônico**. São Paulo: All-Print-Editora, 2006.

CORRITORE, C. L.; KRACHER, B.; WIEDENBECK, S. On-line trust: concepts, evolving themes, a model. **International Journal of Human-Computer Studies**, v. 58, p. 737-758, 2003.

ESTEVE, J. B.; GOLDSMITH, B.; TURNER, J. **International experience with e-voting**. Nepal: International Foundation for Electoral Systems, 2012.

HAMILTON, T. Will we, should we e-vote. **Toronto Star**, Nov. 4, 2002.

JOVCHELOVITCH, S. Understanding relations between self and other in the Brazilian public sphere. *In*: MARKOVA, I.; GILLESPIE, A. (Eds.). **Trust & Distrust**: sociocultural perspectives. Charlotte: Information Age Publishing, 2008.

KAWAI, S. **A new "order and progress" in the Brazilian economy**. 1st ed. [s.l.]: [s.n.], 2016. Available at: <https://goo.gl/8nWhea>. Accessed: Mar. 12, 2016.

KOBIE, N. Why electronic voting isn't secure – but may be safe enough. **The Guardian**, 2015. Available at: <https://goo.gl/7NDPGr>. Accessed: Mar. 12, 2016.

LEWIS, J. D.; WEIGERT, A. Trust as a social reality. **Social Forces**, v. 63, n. 4, p. 967-985, 1985.

MANESCHY, O. Fraude eletrônica nas eleições. **Jus Navigandi**, 2000. Available at: <https://goo.gl/xzxMfz>. Accessed: Feb. 12, 2016.

MARX, B.; PONS, V.; SURI, T. Improving electoral participation: evidence from randomised evaluations. *In:* AFRICA POLICY OUTREACH CONFERENCE, 2015, Ghana. **Annals...** Ghana: J-PAL, 2015. (J-PAL Governance Initiative). Available at: <https://goo.gl/yL9szp>. Accessed: Mar. 12, 2016.

MOISÉS, J. Á. Citizens' distrust in democratic institutions. **International Review of Sociology**, v. 16, n. 3, p. 593-616, 2006.

NEUMANN, G. Special issue: the problems and potentials of voting systems. **Communications of the ACM**, v. 47, n. 10, p. 29-30, 2004.

NOGUEIRA, J. P.; SÁ, F. S. Trust in e-voting systems: a case study. **Lecture Notes in Business Information Processing**, n. 129, p. 51-66, 2012.

OECD – ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Financing democracy**: funding of political parties and election campaigns and the risk of policy capture. Paris: OECD, 2016. (Public Governance Reviews). Available at: <https://goo.gl/pca4bB>. Accessed: Mar. 12, 2016.

RODRIGUES FILHO, J. E-voting and the creation of trust for the socially marginalized citizens in Brazil. **ResearchGate**, Sept. 2010. Available at: <https://goo.gl/gDnXMD>. Accessed: Feb. 26, 2016.

RODRIGUES FILHO, J.; ALEXANDER, C.; BATISTA, L. E-voting in Brazil: the risks to democracy. **ResearchGate**, 2006. Available at: <https://goo.gl/XnDQJp>. Accessed: Feb. 26, 2016.

SANS INSTITUTE. **Trusting the machine**: inherent problems with electronic voting systems. 1st ed. North Bethesda: Sans Institute, 2004. (Global Information Assurance Certification Paper). Available at: <https://goo.gl/oZoZjc>. Accessed: Feb. 12, 2016.

SCHNEIER, B. What's wrong with electronic voting machines? **openDemocracy**, 2004. Available at: <https://goo.gl/UF9fte>. Accessed: Feb. 26, 2016.

COMPLEMENTARY BIBLIOGRAPHY

BORGES, B. Urna eletrônica pode ser fraudada? Especialistas explicam. **UOL Eleições 2014**, Brasília, Aug. 29, 2014. Available at: <https://goo.gl/YLZkfM>. Accessed: Mar. 12, 2016.

CAMPAIGNING for online voting in UK elections. **WebRoots Democracy**, 2016. Available at: <https://goo.gl/7bNUkA>. Accessed: Mar. 12, 2016.

E-VOTING. **Open Rights Group**, 2016. Available at: <https://goo.gl/MGBM8R>. Accessed: Mar. 12, 2016.

NORRIS, P. *et al.* **The year in elections 2015**. 1st ed. Sydney: University of Sydney, 2016. Available at: <https://goo.gl/1J1dZ1>. Accessed: Mar. 12, 2016.

VOTAÇÃO começa; 15% dos eleitores utilizarão urnas biométricas. **UOL Eleições 2014**, São Paulo, Oct. 5, 2014. Available at: <https://goo.gl/5eSxzp>. Accessed: Mar. 12, 2016.