Urna eletrônica de terceira geração: Um protótipo para eleições auditáveis

Fernando Teodoro de Lima[1], **Mario A. Gazziro**[1], **Antonio de Abreu Batista Jr** [2]
Paulo Matias[3], **João V. C. Costa**[1]

[1]Universidade Federal do ABC (UFABC)
Santo André – São Paulo – Brasil

[2]Departamento de Informática – Universidade Federal do Maranhão (UFMA)
São Luís – Maranhão – Brasil

[3]Departamento de Computação – Universidade Federal de São Carlos (UFSCar)
São Carlos – São Paulo – Brasil

{fernando.lima,mario.gazziro}@ufabc.edu.br, antonio.batista@ufma.br

matias@ufscar.br, custodiovjoao@gmail.com

Abstract. *In this work, we developed a third generation electronic voting machine prototype that meets several proposed functional requirements by the international scientific community, which established – over the last decades – the guidelines for the latest generation of electronic voting machines. In addition to the voting module, we implemented the various modules needed to run an election, such as setup and verification modules. Finally, we report the use of this prototype in a real election occurred in a Brazilian university.*

Resumo. *Nesse trabalho foi desenvolvido um protótipo de urna eletrônica de terceira geração, atendendo a vários dos requisitos funcionais propostos pela comunidade científica internacional, a qual estabeleceu – ao longo das últimas décadas – as diretrizes para a última geração de urnas eletrônicas. Foram implementados, além do módulo de votação, os diversos módulos necessários à execução de uma eleição, como módulos de cadastro e apuração. Por fim, relatamos o uso desse protótipo em uma eleição oficial, ocorrida dentro de uma universidade brasileira.*

1. Introdução

Muitos sistemas de votação eletrônica, entre eles o atual sistema brasileiro, funcionam como uma caixa preta [van de Graaf 2017]. Eles não permitem que o eleitor verifique que o seu voto foi incluído na contagem nem testemunhe uma correta apuração deles, obrigando o eleitor a confiar na boa fé das pessoas. Se tais sistemas algum dia cair sob o controle de pessoas desonestas, elas poderão eleger quem desejarem. Entretanto, o que se espera de um bom sistema eleitoral é que ele permita – dentre outras funcionalidades – que qualquer pessoa possa acompanhar e conferir uma apuração, independentemente de possuir algum conhecimento técnico em informática, obtendo acesso ao conteúdo do voto, e ainda assim, garantindo resguardado o seu sigilo.

Ao longo dos últimos anos diversas máquinas de votação eletrônica foram propostas [Karima et al. 2014, Culnane et al. 2015, Puri et al. 2017]. Todas elas buscando

aprimorar e/ou facilitar os procedimentos de auditoria, tanto do registro do voto como de sua apuração e totalização. A última geração delas, as urnas eletrônicas de terceira geração, são caracterizadas por unir de forma tecnológica os dois tipos de registro do voto: o físico e o digital [Brunazo Filho and Gazziro 2014]. Entre as várias formas de se fazer isso, duas delas se destacam:

1. O uso de códigos de barras *QR* – que nada mais são do que registros digitais impressos em meio físico e que podem ser lidos (escaneados) pela maior parte dos celulares que possuem câmeras fotográficas; e
2. O uso de *tags* de RFID embutidas na cédula de votação. Tal solução foi utilizada nas urnas de terceira geração da Argentina. Nelas o voto era gravado em chips de rádio frequência embutidos nas cédulas de votação e impresso por fora delas. É importante ressaltar que os chips RFID adotados na cédula argentina foram responsáveis por várias das vulnerabilidades descobertas naquele sistema [Oro 2015], sendo a impressão em papel suficiente para mitigar vários ataques, como leitura à distância e gravação com celular.

Entretanto, no Brasil, o uso de urnas de terceira geração ainda está distante de aplicações sérias, sendo que os principais desafios são prover uma solução segura e ganhar a confiança dos eleitores em usá-la [Wang et al. 2017]. Atualmente, o Brasil é o único país do mundo a usar urnas de 1^a geração, em que os votos são gravados apenas digitalmente, não oferecendo possibilidade de auditoria por outros meios [Filho et al. 2015]. Deste modo, a confiabilidade do resultado publicado fica totalmente dependente da confiança no software instalado no equipamento.

Neste artigo, nós apresentamos as soluções técnicas elaboradas para um protótipo de urna eleitoral eletrônica de terceira geração que atende a vários dos requisitos funcionais propostos pela comunidade científica internacional [Adida and Rivest 2006, Ali and Murray 2016]. Apesar da versão atual de nosso protótipo não prover a propriedade de verificação fim-a-fim do voto, eleitores e fiscais podem acompanhar cada parte do processo, que é de fácil compreensão mesmo para um cidadão não-técnico.

2. O protótipo desenvolvido

O protótipo de urna desenvolvido é constituído de diversos módulos, estando o código fonte de todos eles disponível no endereço: `https://github.com/mariogazziro/UrnaEletronica3G`. O projeto foi desenvolvido em linguagem *Python* e faz uso de bibliotecas livres como *PySide* para controle de janelas e *SQL Alchemy* para a base de dados de cadastros. O compilador utilizado foi o GCC da GNU, gratuito e de código aberto, usado e desenvolvido por muitos usuários no mundo inteiro. A seguir, na Tabela 1, apresentamos um comparativo entre o protótipo desenvolvido e a urna eletrônica em uso nas eleições brasileiras, com relação aos requisitos funcionais propostos por [Brunazo Filho and Gazziro 2014].

2.1. Módulos construídos

Os módulos devem ser executados na ordem estabelecida abaixo, seguindo o fluxo natural de uma eleição.

1. Ajuste de Urna: Gera um par de chaves de encriptação para cada seção eleitoral. Uma das chaves do par, a chave pública, é distribuída entre as máquinas de votação

de uma seção eleitoral e usada por elas para encriptar cada voto. A outra chave do par, a chave privada, é distribuída entre as máquinas de verificação de votos e de apuração que a utiliza para verificação de integridade do voto, impedindo que cédulas geradas em outras seções eleitorais sejam apuradas na seção atual.

2. Ajuste de Eleição: Realiza o cadastro dos partidos (ou chapas, no caso de eleições não políticas), dos cargos e dos candidatos. O sistema permite cadastrar mais de um voto possível por cargo, o que permite a um eleitor, por exemplo, votar em 2 candidatos a senador.
3. Votação: O módulo de votação propriamente dito, no qual o eleitor deve necessariamente votar utilizando-se de um número pré-definido para identificação dos candidatos. É permitido ao eleitor, ainda, escolher a ordem de votação desejada, assim, este primeiro escolhe o(s) cargo(s) para o qual deseja votar. Caso o número de candidatos seja pequeno, recomendamos manter uma listagem com os códigos dos candidatos impressa e colada dentro da cabine de votação. No caso de um número muito grande de candidatos, como em eleições nacionais, o eleitor necessita adentrar à seção já sabendo o número de seu candidato, similar às eleições brasileiras.
4. Verificação: Módulo de verificação do voto, a ser usado pelo eleitor para conferir se o conteúdo do código de barras *QR* impresso é igual ao conteúdo escrito por extenso em sua cédula de votação. Idealmente deve ser executado em outra máquina na seção eleitoral, para garantir que não haja comunicação entre a máquina que gerou o voto e a máquina de verificação.
5. Apuração: O módulo de apuração totaliza cada voto apenas uma vez, com o auxílio de um número aleatório de até 10 casas decimais embutido no código *QR*, junto ao conteúdo do voto. O voto é encriptado. Com isso, garante-se que votos de outras eleições ou outras seções eleitorais gerem alertas e não sejam contabilizados. Caso seja constatada divergência entre o registro textual (legível por um humano) e o registro digital (código *QR*) presentes em uma mesma cédula, deve-se considerar o registro digital errôneo e proceder à contagem manual dos votos.

3. Protocolo aplicado ao voto

Com relação ao processo completo adotado em um sistema de eleição utilizando preceitos de terceira geração, listamos nessa seção, em detalhes, todas as fases envolvidas no processo.

Fase de inicialização

A comissão eleitoral executa os procedimentos listados abaixo.

1. Criação de chaves:

   1.1 execute o módulo de Ajuste de Urna. O módulo retornará um par de chaves de encriptação - pública k_{pub} e privada k_{pri}.

   1.2 insira uma cópia da chave pública k_{pub} em cada uma das máquinas de votação e uma cópia da chave privada k_{pri} nas máquinas de verificação e apuração.
2. Cadastros:

   1.1 São cadastrados os Partidos (ou Chapas) pela comissão eleitoral, atribuindo um número decimal de dois dígitos.

Tabela 1. Tabela comparativa, extraída e adaptada de [Brunazo Filho and Gazziro 2014]

Princípio da Publicidade	Urna brasileira	Urna 3G UFABC
Gera voto impresso conferível pelo eleitor	NÃO	SIM
Eleitor pode conferir o conteúdo da gravação digital do voto antes de sair do local de votação	NÃO	SIM
Fiscal externo pode verificar a igualdade entre os diversos registros do voto	NÃO	SIM
Fiscal externo pode acompanhar e verificar a contagem dos votos de cada seção eleitoral	NÃO	SIM
Princípio da Independência do Software		
Uma modificação ou erro não detectado no software pode causar um erro indetectável no resultado da apuração	SIM	NÃO
Outros Conceitos Desejáveis		
Tempo para publicação na Internet dos resultados por Seção, para fiscalização da Totalização	72h (2012)	1,5 hora por seção com 400 votos
Conferência da assinatura digital do software feita em equipamento sob controle do fiscal	NÃO	SIM
Distribuição matricial de urnas e mesas: o eleitor pode escolher uma urna livre para votar, sem ter que esperar que um eleitor anterior complete seu voto. Menores filas.	NÃO	SIM
Eleitor pode escolher a ordem dos cargos a votar	NÃO	SIM
Adaptação para plebiscitos e outras consultas - disponibilidade de opções “sim”, “não”, ou outras mais específicas	NÃO	SIM
Troca de equipamento defeituoso	LENTA	RÁPIDA
Necessidade de recuperação de dados	SIM	NÃO

1.3 Realização do cadastro dos cargos, com a possibilidade de definição do número de votos por cargo, a exemplo do caso do cargo a senador, no qual cada eleitor pode votar em até dois candidatos.

1.3 São cadastrados todos os candidatos e seus respectivos partidos (ou chapas)e cargos, com a possibilidade de inclusão de foto.

Fase de votação

Primeiramente, os eleitores se identificam aos mesários, que verificam se estes estão aptos a votar. E, caso estejam aptos, as suas assinaturas também são colhidas por eles. Uma vez que um eleitor entra na cabine, o procedimento é como segue:

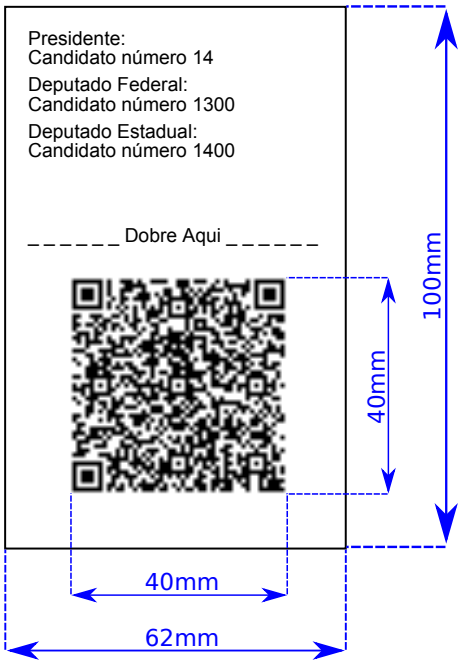

Figura 1. Cédula de votação gerada pela urna de terceira geração, com suas dimensões. Registro físico e digital unidos no mesmo tipo de mídia, o papel.

1. O eleitor entra com a sua escolha de candidatos na máquina de votação.
2. Em resposta às entradas do eleitor, a máquina imprime uma cédula como a da Figura 1. Nela há um código de barras *QR* contendo o registro digital do voto, além de um registro textual legível por um humano.
3. Após receber a cédula, o eleitor dirige-se a máquina de verificação (diferente da que votou) para conferência do voto. Caso detecte alguma divergência com relação à sua escolha de candidatos, o eleitor descarta a cédula e retorna ao primeiro passo.
4. O eleitor deposita a cédula em urna previamente lacrada para garantir o total sigilo do voto.

O registro digital do voto é um código de barras *QR* contendo a concatenação da strings $S_1 = RSA_{K_{pub}}(voto)$ e S_2. S_1 é o voto encriptado e S_2 um número pseudo aleatório gerado pela máquina de votação. RSA é o algoritmo de chave pública RSA [Rivest et al. 1978] e K_{pub} a chave de encriptação copiada para a máquina de votação.

Embaralhamento das cédulas

Cada eleitor vota em um cabine e deposita a sua cédula de votação em uma urna previamente lacrada. A urna deve ser sacudida sempre que uma nova cédula foi incluída nela, após o eleitor ter conferido o seu voto. Este procedimento operacional é importante para garantir ao eleitor o sigilo de seu voto, com relação a ordem de votação dos eleitores em suas seções eleitorais.

Fase de verificação da cédula

O eleitor dirige-se a máquina de verificação para conferência do voto. Ele, então, mostra a sua cédula de votação para ela.

1. A máquina:
   1 lê S_1 a partir do código de barras *QR*;
   2 computa $voto' = RSA_{K_{pri}}(S_1)$; e
   3 imprime $voto'$.
2. O eleitor, então, confere se o conteúdo do código de barras *QR* impresso é igual ao conteúdo escrito por extenso em sua cédula de votação $voto' = voto$; e
3. Caso detecte alguma divergência com relação à sua escolha de candidatos $voto' \neq voto$, o eleitor descarta a cédula e vota novamente.

Fase de transporte das cédulas

A comissão eleitoral lacra as urnas e as leva para área de apuração de votos.

Fase de contagem de votos

O presidente da seção eleitoral deve proceder como segue:

1. Para cada urna lacrada deve-se romper o lacre e retirar as cédulas, uma a uma, enquanto existirem cédulas de votação nela. Cada cédula deve ser processada pelo módulo de apuração.

   A máquina de apuração procede como segue para cada cédula:

1. caso, a *String* aleatória, S_2 lida a partir do código QR, já tenha sido processada antes; uma mensagem de alerta é exibida, indicando que aquela cédula em questão ja foi computada, e nada mais é feito.
2. caso contrário, o conteúdo do voto é decriptado $voto' = RSA_{K_{pri}}(S_1)$ e;
3. o voto é contabilizado para o candidato, e exibido na tela do equipamento, a qual pode ser ligada a um projetor para facilitar a auditoria dos fiscais presentes.

Conforme cada cédula vai sendo lida, o resultado da totalização apresentado na tela vai se atualizando, exibindo sempre a contagem atual de votos para cada candidato. Quando todas as cédulas tiverem sido lidas, o presidente da seção eleitoral aciona o botão *GERAR BOLETIM*. A máquina de votação, então, emite o resultado final da apuração, de forma impressa. Finalmente, o presidente da seção verifica se o número de assinaturas colhidas corresponde ao total de votos contabilizados pela máquina.

4. Probabilidade de colisão de números aleatórios em um seção eleitoral

Cada cédula contém um número aleatório para garantir que, quando escaneado eletronicamente, um voto nunca seja contabilizado mais de uma vez em uma seção.

Porém, caso a máquina acidentalmente escolha para uma cédula um número que já tenha sido sorteado antes e já tenha sido atribuído a um outro eleitor da mesma seção eleitoral, o voto de um deles não seria contabilizado. No entanto, a probabilidade desse evento acontecer é muito pequena. No caso de uma auditoria, poderia-se verificar se a frequência com que essa situação ocorre condiz com a probabilidade esperada teoricamente.

Essa probabilidade é estimada por meio do paradoxo de aniversário. Seja X o número de colisões, k o número de eleitores de uma seção eleitoral e $[1, n]$ o intervalo dentro do qual a máquina sorteia os números aleatórios. Abaixo, calculamos $P\{X = 0\}$, a probabilidade de que não haja nenhuma colisão, e $P\{X \geq 1\}$, a probabilidade de que haja uma ou mais delas.

$$P\{X = 0\} = \prod_{i=0}^{k}(1 - \tfrac{i}{n}) \tag{1}$$

$$P\{X \geq 1\} = 1 - P\{X = 0\} \tag{2}$$

A máquina gera números pseudo aleatórios de até 10 casas decimais. Impor esse comprimento máximo permite que câmeras de baixo custo, em função de suas limitações óticas e baixas resoluções (em geral, em torno de 640×480 pixels) leiam os códigos *QR*. O gráfico da Figura 2 mostra a probabilidade de colisão de números aleatórios em seções eleitorais com diferentes números de eleitores. Nós estamos considerando que a máquina sorteia números em um espaço com $n = 2^{30}$ elementos.

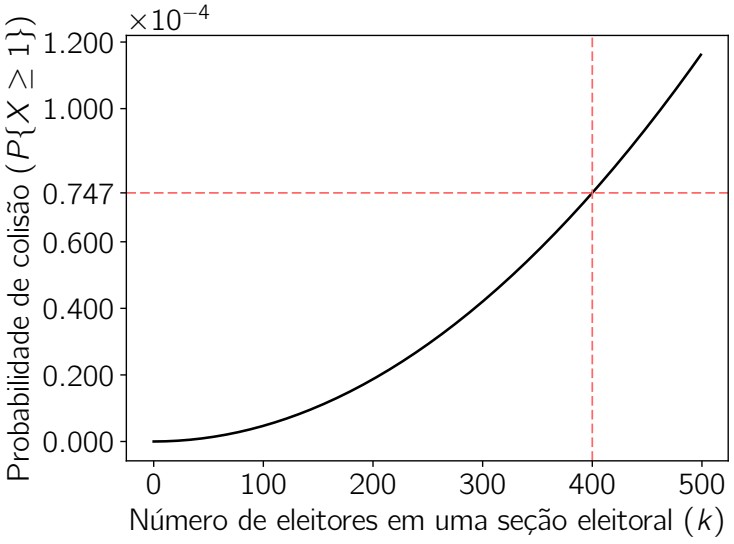

Figura 2. Probabilidade de colisão de números aleatórios em uma seção eleitoral.

5. A eleição realizada

O protótipo da urna foi testado em ambiente real, em uma votação referente à portaria n° 25 de 23 de junho de 2016 do CMCC, da instituição de ensino UFABC. A votação ocorreu dia 20 de julho de 2016 no período das 10h00 às 13h00 e das 15h00 às 19h00, nos *campi* de Santo André e São Bernardo da instituição. A eleição disponibilizou 12 vagas no total, 2 para representantes discentes de graduação, 2 para representantes da pós-graduação e 2 para representantes dos servidores técnico-administrativos, bem como os respectivos suplentes em ambas as categorias para composição do Conselho do CMCC, um dos centros da mesma universidade. A apuração da eleição aconteceu dia 21 de julho de 2016 das 13h20 às 13h47 (tal como à ata n° 02/2016 da Comissão Eleitoral para Conselho de Centro do CMCC). Nela, foram constatados 64 eleitores votantes com um total de 63 assinaturas – devido a uma falha dos mesários em colher uma assinatura de um dos eleitores. Tal discrepância foi desconsiderada pelo então presidente da comissão, uma vez que a diferença entre um eleitor e uma assinatura não alteraria o resultado final da eleição. **No dia 22 de julho de 2016 o seu resultado foi divulgado e a eleição foi dada como conclusiva**. Este foi o primeiro uso de uma urna de terceira geração em uma instituição pública brasileira.

5.1. Tempo de apuração

A apuração eletrônica levou 15 minutos, com mais alguns minutos despendidos na elaboração da ata. Ao todo, foram apurados 64 votos, de forma digital, a uma taxa de $\approx$15 segundos por voto, sendo esse o tempo utilizado em retirar a cédula de votação da urna, apresentá-la ao sistema de apuração eletrônico – constituído de um dos módulos de nossa urna eletrônica – e apresentação da tabela de resultados atualizada a uma comissão de fiscais presente, utilizando um *datashow*. Os fiscais também puderam examinar o conteúdo impresso em cada cédula de votação.

Para apurar uma seção eleitoral típica, com 400 eleitores, o tempo estimado é de uma hora e meia.

6. Considerações Finais

Neste trabalho, apresentou-se um protótipo de urna eletrônica de 3^a geração em que se descreveu as suas soluções técnicas. Além disso, mostrou-se também que o protótipo atende a várias das recomendações estabelecidas pela comunidade acadêmica para esta nova geração de urnas eletrônicas.

Dentre as melhorias previstas no desenvolvimento futuro dessa urna eletrônica está incluir em seu projeto o fato de que o voto deve ser incondicionalmente seguro [van de Graaf 2017] além de utilizar encriptação homomórfica com o objetivo de prover mecanismos para verificação fim-a-fim do voto [Rivest 2002].

Referências

Adida, B. and Rivest, R. L. (2006). Scratch & vote: Self-contained paper-based cryptographic voting. In *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, WPES '06, pages 29–40, New York, NY, USA. ACM.

Ali, S. T. and Murray, J. (2016). An overview of end-to-end verifiable voting systems. *CoRR*, abs/1605.08554.

Brunazo Filho, A. and Gazziro, M. A. (2014). Critérios para avaliação de sistemas eleitorais digitais. *XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Ed. por GRAAF, Jeroen van de, NOGUEIRA, José Marcos*, pages 599–610.

Culnane, C., Ryan, P. Y. A., Schneider, S., and Teague, V. (2015). vvote: A verifiable voting system. *ACM Trans. Inf. Syst. Secur.*, 18(1):3:1–3:30.

Filho, A. B., Carvalho, M. A. M., Teixeira, M. C., Jr, M. A. S., and Fernandes, C. T. (2015). Auditoria especial no sistema eleitoral 2014. *XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 511–522.

Karima, D., Victor, T., and Faycal, R. (2014). An improved electronic voting machine using a microcontroller and a smart card. In *IDT*, pages 219–224. IEEE.

Oro, I. A. B. (2015). `https://ivan.barreraoro.com.ar/vot-ar-una-mala-eleccion`. Acessado em 9 de Outubro, 2017.

Puri, T., Singh, J., and Kaushal, H. (2017). Prototyping of Indian electronic voting machine. *International Journal of Engineering Research and Development*, 13(5):44–51.

Rivest, R. (2002). Voting, homomorphic encryption. `http://web.mit.edu/6.857/OldStuff/Fall02/handouts/L15-voting.pdf`. Acessado em 9 de Setembro, 2017.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126.

van de Graaf, J. (2017). Long-term threats to ballot privacy. *IEEE Security & Privacy*, 15(3):40–47.

Wang, K.-H., Mondal, S. K., Chan, K., and Xie, X. (2017). A review of contemporary e-voting: Requirements, technology, systems and usability. *Data Science and Pattern Recognition*, 1(1):31–47.

Critérios para Avaliação de Sistemas Eleitorais Digitais

Amilcar Brunazo Filho[1], Mario A. Gazziro[2]

[1]CMIND – Comitê Multidisciplinar Independente

[2]UFABC – Universidade Federal do ABC

amilcar@brunazo.eng.br, mario.gazziro@ufabc.edu.br

Abstract. *Since the first applications with electronic voting machines in the 90s models and standards have been developed but little is discussed what should be the criteria for classification and comparison of such models. This paper proposes a set of basic concepts necessary and their comparison criteria that can be applied in the design and evaluation of digital electoral systems. A table of compliance is also presented for some models in use in several countries in Latin America.*

Resumo. *Desde as primeiras aplicações com máquinas eletrônicas de votação nos anos 90, alguns modelos e padrões já foram desenvolvidos, mas é pouco discutido quais deveriam ser os critérios de classificação e de comparação de tais modelos. Neste trabalho é proposto um conjunto de conceitos básicos necessários e de critérios de comparação que possam ser aplicados no projeto e na avaliação de sistemas eleitorais digitais. Também é apresentada uma tabela de conformidade para alguns modelos em uso em diversos países da América Latina.*

1. Introdução

Já em 1993, quando se iniciava o uso de equipamentos eletrônicos de votação em eleições oficiais de alguns países, Peter G. Neumann apresentou uma proposta de critérios de segurança para ser aplicada na avaliação de sistemas de eleição eletrônica [Neumann 1993] que envolvia uma longa lista de itens sobre confidencialidade, integridade, disponibilidade, confiabilidade, segurança e muitos outros.

Desde então, foram desenvolvidos novos recursos de hardware e de software e novas infraestruturas de comunicação tiveram grande crescimento. Simultaneamente, vários países passaram a testar e adotar sistemas eleitorais digitais isolados ou conectados pela Internet. Esse crescimento de recursos e de sistemas ocorreu de forma independente e sem coordenação, gerando uma grande variedade de modelos com características bem diferenciadas quanto ao atendimento dos critérios de segurança e de confiabilidade.

Na área do voto digital, critérios de confiabilidade que parecem essenciais para uns, são simplesmente ignorados por outros e os esforços de padronização ainda são modestos e insipientes, tendo se encontrado obstáculos e resistências inesperados, que acabam retardando a produção de normas locais e internacionais.

O presente trabalho apresenta um pequeno conjunto de conceitos fundamentais e critérios para classificação e avaliação de confiabilidade de sistemas eleitorais digitais e foi desenvolvido a partir da experiência dos autores no estudo e acompanhamento dos sistemas usados em países da América Latina, com destaque dos sistemas usados no Brasil, na Venezuela e na Argentina.

Em nenhum desses três casos se usa o voto pela Internet porque a legislação dos três países, em respeito ao Princípio da Inviolabilidade do Voto, exige que o ato de votar ocorra em um local isolado e protegido contra acesso de terceiros, nas chamadas cabines indevassáveis. Apenas a transmissão dos resultados parciais, resultantes das contagens dos votos digitais dados em máquinas isoladas, pode ocorrer pela Internet. Assim, a descrição de modelos e as tabelas de conformidade apresentadas no final do trabalho consideram apenas os modelos de equipamentos de gravação do voto sem conexão com a Internet durante o ato de votação.

Ainda com relação à votação pela Internet, há fortes restrições nos meios acadêmicos quanto à sua confiabilidade técnica. Em 2008, por solicitação da ONG americana *Verified Voting*, uma comissão de mais de trinta especialistas em TI elaborou um estudo [CT 2012] contrário aos modelos de votação pela Internet existentes por causa dos enormes desafios que ainda não foram tecnologicamente resolvidos para justificar a confiabilidade técnica de tais sistemas.

Por estes motivos, o presente estudo não abrange o que genericamente é chamado de "sistemas eleitorais pela Internet".

Experiências e observações com voto digital em eleições oficiais sempre estarão inseridas em ambientes e situações influenciadas pelas peculiaridades culturais e políticas locais e até mesmo pelas fortes cargas emocionais que eleições oficiais acendem. Dessa forma, o presente trabalho destacará conceitos fundamentais e critérios básicos que os autores entendem ser necessários ser aplicados nas realidades sociais e políticas de onde derivam suas observações.

2. Conceitos Fundamentais e Critérios Básicos para o Voto Digital

2.1. Confiabilidade de Sistemas Eleitorais

O conceito de confiabilidade de sistemas eleitorais envolve duas faces distintas de igual importância:

Confiança técnica: determinada por avaliações e medidas objetivas;

Confiança subjetiva: baseada no sentimento pessoal.

Em um processo eleitoral, pode-se tentar conquistar a confiança subjetiva dos atores, transferindo a confiança que depositam nas autoridades eleitorais para a confiança no processo que as autoridades administram.

Mas, em processos eleitorais eletrônicos, onde pequenas falhas podem passar despercebidas provocando grandes desvios no resultado, e ainda, onde os interesses das partes envolvidas são crescentes e podem ser divergentes, cada vez mais se torna necessário conquistar a confiança subjetiva dos eleitores e dos candidatos por meio da demonstração objetiva da confiabilidade técnica do processo.

Em 2010, Wolter Pieters [Pieters 2010] propôs que as palavras inglesas "*confidence*" e "*trust*", quando usadas em referências a processos eleitorais, tivessem significados similares aos de confiança subjetiva e de confiança técnica, respectivamente, e apresentou o quadro a seguir, atribuído a Niklas Luhmann:

Tabela 1. Modelos de auto-confiança subjetiva e técnica proposto por Luhmann

	"Confidence" **(Confiança subjetiva)**	**"Trust"** **(Confiança técnica)**
Tipo de confiança	Inconsciente	Consciente
Interpretação	Alternativas não percebidas	Comparação de alternativas
Ação	Sem decisão	Decisão / Escolha
O que os cientistas desejam	Minimizar	Maximizar

A proposta é que, em processos eleitorais eletrônicos, deve-se procurar minimizar a necessidade de confiança subjetiva dos eleitores e maximizar a confiança tecnicamente demonstrada.

Também é comum o entendimento que a melhor via para avaliar e demonstrar a confiabilidade técnica em um processamento eletrônico de votos é a TRANSPARÊNCIA de todos os atos de votação, de registro dos votos (gravação digital) e de contagem dos votos digitais.

2.2. Soberania dos Eleitores e dos Candidatos

Em eleições, os direitos soberanos e prioritários pertencem aos eleitores (direito de votar) e aos candidatos (direito de ser votado). Tais direitos devem prevalecer e não podem ser restringidos pelos direitos dos demais participantes do processo eleitoral, como os administradores, juízes, auditores, fornecedores, programadores e demais operadores, os quais têm por DEVER garantir os direitos eleitorais do cidadão.

Para exercer seu direito de forma soberana, ELEITOR e CANDIDATO devem poder FISCALIZAR COM RECURSOS PROPRIOS e EFETIVOS todos os procedimentos eleitorais, como votação, registro de voto, apuração, etc., como bem explanado pelo Procurador da República Celso Antônio Três [Três 2002], durante o Seminário do Voto Eletrônico promovido pela Câmara dos Deputados em maio de 2002, quando expôs:

"Contudo, mesmo fosse cientificamente possível garantir a segurança técnica, isso não seria suficiente. Impõe-se disponibilizar ao cidadão, através de suas faculdades normais, motu próprio, a possibilidade de sindicar a devida observância à sua vontade eleitoral.

A Constituição da República, de forma lapidar e definitiva, estabelece a pedra fundamental do Estado Brasileiro, após certificar que "... todo o poder emana do povo..." (art. 1º,§ único, da C.F.), diz que "a soberania popular é exercida pelo sufrágio universal e pelo voto direto e secreto ..."(art. 14, "caput", da C.F.).

De sua parte, um dos sustentáculos do Direito Constitucional, vital a conferir efetividade aos preceitos fundamentais, é a conhecida teoria/doutrina dos poderes implícitos, traduzida pelo extraordinário Mestre Paulo Bonavides, ao dizer que "... na interpretação de um poder, todos os meios ordinários e apropriados a executá-lo são considerados sempre parte do próprio poder..."(Curso de Direito Constitucional, Malheiros, 10ª edição, p. 432).

De que vale um poder, uma prerrogativa, desprovido dos instrumentos necessários à sua efetivação?!?!?

Soberania pressupõe poder supremo. Onde está a supremacia do povo em um processo cuja apuração não é instrumentado por mecanismos que permitam-lhe certificar-se da soberania de sua vontade?!?!?. Pior. Sequer os agentes operadores, Membros da Justiça Eleitoral, do Ministério Público, dos Partidos Políticos, Candidatos, são, diretamente, dele dotados. Apenas assistidos por técnicos.

Soberano que não é instrumentado a fiscalizar o exercício de sua soberania não é soberano.

É inerente, "ratio essendi" da soberania popular, que todo o processo eleitoral, alistamento, registro de candidaturas, propaganda política, votação, apuração, diplomação, etc., sejam aferíveis pelo titular dessa soberania, o povo. Aferíveis, diga-se, por todo o eleitorado, desde o mais rutilante PhD até o excluído analfabeto"

O mesmo conceito foi acatado pelo Tribunal Constitucional da Alemanha, ao julgar um processo em 2009, onde se analisava a constitucionalidade de sistemas de voto puramente digital. Num longo acórdão [TCFA 2009], a corte suprema alemã criou jurisprudência, demarcando princípios e fundamentos sobre o uso de máquinas de votar, dos quais se destaca o seguinte, conforme tradução para o português realizada pelo CMind [CMind 2010]:

"Princípios

2. Na utilização de máquinas eletrônicas de votar, é necessário que o cidadão, que não possui experiência especial sobre o assunto, possa controlar de forma confiável os passos essenciais da ação de votar e da aferição dos resultados.

Fundamento 156

As principais etapas no processamento dos dados pelas máquinas de votar não poderiam ser entendidas pelo público. Como a apuração é processada apenas dentro das máquinas, nem os oficiais eleitorais, nem os cidadãos interessados no resultado podiam conferir se os votos dados foram contados para o candidato correto ou se os totais atribuídos a cada candidato eram válidos. Com base num resumo impresso ou num painel eletrônico, não era suficiente conferir o resultado da apuração dos votos na central eleitoral. Assim, foi excluída qualquer conferência pública da apuração que os próprios cidadãos pudessem compreender e confiar sem precisar de conhecimento técnico especializado."

Como consequência direta da extensão desse conceito, deve ser destacado que a participação de técnicos e da academia na validação de um processo eleitoral digital, embora seja prática desejável, não pode ser imposta como substituta válida ao direito do

eleitor comum compreender e auditar o registro e o destino do seu voto usando seus próprios conhecimentos e recursos.

A experiência com o processo eleitoral brasileiro serve como exemplo da necessidade de prevalência do direito do eleitor fiscalizar *motu-próprio,* sobre possíveis auditorias desenvolvidas por especialistas e acadêmicos, como o caso das fragilidades no software das urnas eletrônicas encontradas em 2012 pela equipe do professor Dr. Diego Aranha [Aranha 2012] depois do mesmo software das urnas eletrônicas ter passado por análise e escrutínios por várias equipes de auditores e especialistas contratados pela autoridade eleitoral desde 2002.

E tais tipos de fragilidades ainda persistem, como um dos autores do presente trabalho pôde constatar *in-loco* na Cerimônia de Apresentação dos Sistemas, no TSE em 2014.

A tentativa de substituir uma forma de auditoria contábil simples, feita pelos eleitores e candidatos, por uma validação e certificação exaustiva do software usado em mais de 400 mil equipamentos no dia da eleição, é complexa e financeiramente proibitiva para os agentes autorizados (Ministério Público, OAB e partidos políticos), como mais uma vez ficou comprovado nessa última Cerimônia de Apresentação dos Sistemas, onde tais agentes tradicionalmente não participam por alegada falta de recursos.

O Princípio da Soberania dos Eleitores e Candidatos tem forte influência na avaliação de sistemas eleitorais existentes, pois é muito frequente que auditorias feitas por especialistas sejam impostas como substitutas da possibilidade de auditoria pelo eleitor comum e pelos candidatos, sendo apresentadas como importante marco de confiabilidade quando, na realidade, estão desatendendo um direito fundamental de cidadania.

2.3. Tripartição de Poderes

O conceito de tripartição dos poderes, que surgiu na antiga Grécia e agora é adotado em todas as repúblicas modernas (pós Revolução Francesa), foi formalizado por Montesquieu no final do Sec. XVIII, e divide as funções de governo em três poderes independentes, harmônicos e autorreguladores: Legislativo, Executivo e Judiciário

Seu objetivo é evitar o abuso de poder, o autoritarismo, o absolutismo e o corporativismo, dando transparência aos atos de governo.

No Brasil, a tripartição dos poderes é estabelecida pelo Art. 2º da Constituição Federal de 1988, mas não vigora no processo eleitoral, onde uma mesma entidade, apesar de chamada de Justiça Eleitoral, detém as funções normativas, administrativas, fiscalizatórias e judiciais, decorrentes do art. 1º e Parag. Único do Código Eleitoral (Lei 4.737/65).

No 1º Relatório CMind [CMind 2010] é analisado e apresentado detalhes de como não há controle jurisdicional externo sobre as autoridades eleitorais brasileiras, resultando em abuso de poder, falta de transparência administrativa e quebra da imparcialidade judicial que, no seu exercício, acabam por restringir diretamente a efetividade dos direitos do eleitor e do candidato, acima citados.

2.4. Princípio de Inviolabilidade Absoluta do Voto

Há mais de cem anos foram criados os conceitos de inviolabilidade do voto e o de votação em cabines indevassáveis, para impedir a coação de eleitores, pois esta é uma modalidade de fraude eleitoral muito insidiosa, com grande potencial de modificação da verdade eleitoral. Assim, o sistema eleitoral deve impedir que terceiros possam identificar o autor de um voto. Também, ao eleitor não deve ser possível provar, para terceiros, em quem votou.

Entre os procedimentos criados para defender esse princípio, se insere o conceito de cabines indevassáveis para a votação e, é de entendimento comum que sistemas eleitorais que não façam uso de cabines indevassáveis, não dão garantia de inviolabilidade do voto e nem impedem a coação de eleitores.

A garantia do sigilo do autor do voto também tem que ser absoluta, pois basta existir uma mínima possibilidade teórica de violação do voto de um eleitor, que a coação de eleitores se implanta e produz seus efeitos deletérios sobre o resultado eleitoral, mesmo que os agentes coatores não consigam, de fato, identificar o autor de cada voto.

Diferente do sigilo telefônico e bancário, o conceito de sigilo absoluto do autor do voto impõe que nem mesmo juízes possam ordenar a sua quebra.

Entre as consequências do princípio da inviolabilidade absoluta do voto, se tem:

- *A identificação do eleitor não deveria ser feita no mesmo equipamento eletrônico no qual o eleitor vota, para evitar que algum software malicioso possa vincular de forma sistemática o conteúdo do voto com a identidade do seu autor;*
- *O registro e o processamento digital do voto não deveriam incluir ou reter dados de rastreamento que remetam à origem do voto, tais como, identificação da máquina de origem, o momento exato da votação, a identificação de quem estava "logado" no equipamento, etc.*

A necessidade de manter total irrastreabilidade do voto digital (inviolabilidade absoluta) associada ao direito do cidadão comum de poder entender o processamento do seu voto (soberania do cidadão), são características que tornam o processamento digital do voto uma atividade com peculiaridades únicas que, por exemplo, resultam ser muito mais difícil processar de forma segura e transparente um voto digital do que transferir uma enorme quantia de dinheiro por computadores.

2.5. Princípio da Publicidade e o Voto Digital

Como já dito acima, em 2009, a Corte Constitucional da Alemanha estabeleceu jusrisprudência sobre a transparência e a confiabilidade de sistemas eleitorais informatizados ao decidir que tais sistemas devem atender ao Princípio da Publicidade, de maneira que o eleitor comum (sem conhecimentos especiais de informática) tenha o direito de poder ver, compreender e conferir o registro e o destino do seu voto, e os candidatos tenham o direito de poder conferir, também com recursos próprios, a contagem eletrônica dos votos.

E, nessa toada, declarou inconstitucionais Sistemas Eleitorais de 1ª Geração – aqueles com gravação digital direta do voto, como ocorre nas urnas eletrônicas brasileiras – que não permitem ao eleitor ver para quem foi registrado e será contado o seu voto, e nem aos candidatos conferir ou auditar a apuração voto a voto, como se pode ver neste outro trecho da tradução apresentada pelo CMind [CMind 2010]:

"Decisão

2. A utilização de máquinas de votar Nedap ESD1 e ESD2 (máquinas DRE sem voto impresso conferível pelo eleitor) na eleição do 16º Parlamento Alemão não estava de acordo com o PRINCÍPIO DE PUBLICIDADE no processo eleitoral implícito no artigo 38, conjugado ao artigo 20, parágrafos 1 e 2 da Constituição.

Fundamento 111

O PRINCÍPIO DA PUBLICIDADE exige que todos os passos essenciais da eleição estejam sujeitos à comprovação pública. A contagem dos votos é de particular importância no controle das eleições.

Fundamento 155

Os votos foram registrados somente em memória eletrônica. Nem os eleitores, nem a junta eleitoral ou os representantes dos partidos poderiam verificar se os votos foram registrados corretamente pelas máquinas de votar. Com base no indicador no painel de controle, o mesário só pode detectar se a máquina de votar registrou um voto, mas não se os votos foram registrados sem alteração. As máquinas de votar não previam a possibilidade de um registro do voto independente da memória eletrônica, que permitisse aos eleitores uma conferência dos seus votos"

Mas, destaque-se que o Princípio da Inviolabilidade Absoluta do Voto não conflita com o Princípio da Publicidade no processo eleitoral, pois é o CONTEÚDO DO VOTO que deve ser PÚBLICO e conferível pelo eleitor (no ato de votação) e pelo fiscal (no ato de apuração), enquanto é o AUTOR DO VOTO que deve ser SECRETO a todo instante.

A adoção da transparência em todos os procedimentos no processo eleitoral eletrônico, incluindo a abertura do software para validação e certificação prévias, é chamado de Modelo de Segurança por Transparência.

Em oposição a esse modelo aberto, há o Modelo de Segurança por Ofuscamento, onde os procedimentos de registro dos votos e o software usado são fechados e ficam sob controle absoluto da equipe de desenvolvedores e operadores do sistema. Nesse modelo fechado, que protege a segurança do administrador, em detrimento do direito do eleitor e do candidato ao Princípio da Publicidade, se pretende que a eventual confiança subjetiva dada aos administradores seja aceita como garantia indireta da confiança técnica sem, no entanto, permitir a determinação efetiva desta.

2.6. Princípio da Independência do Software

O Princípio da Independência do Software em Sistemas Eleitorais estabelece que:

"Um sistema eleitoral é independente do software se um erro não-detectado no software não puder causar um erro indetectável no resultado da apuração ou na inviolabilidade do voto"

Foi criado, e se tornou necessário, a partir da constatação prática de que é muito mais difícil e caro se determinar que um software eleitoral complexo está livre de erros que afetem o seu desempenho, do que desenvolver esse próprio software.

Sobre a dificuldade e quase impossibilidade de se estabelecer confiabilidade técnica do software de sistemas eleitorais destacamos os seguintes pareceres de destacados autores internacionais na área de segurança em TI, conforme tradução nossa:

- Ph.D. Ronald R. Rivest (MIT - criador da técnica de criptografia assimétrica RSA e da Assinatura Digital) e Jonh Wack (NIST) [Rivest 2006]

"A tarefa de encontrar todos os erros num grande sistema é geralmente considerada impossível ou extremamente cara. Nossa habilidade para desenvolver software, de longe supera nossa habilidade de provar seu funcionamento correto ou de testá-lo satisfatoriamente dentro de restrições econômicas razoáveis (um teste completo de confiabilidade num software eleitoral certamente terá custo proibitivo).

Um sistema eleitoral no qual a integridade do resultado depende do funcionamento correto do seu software sempre será, de alguma forma, suspeito e irá requerer verificações sistemáticas do software, mesmo depois de uma completa (e cara) certificação por normas federais."

- Ph.D. Richard M. Stalmann (MIT - criador do projeto do software livre) [Stallman 2008]

"Votar com computadores é uma grande porta aberta para a fraude. O computador executa um software, e o software pode ser alterado ou substituído. Ele pode ser substituído apenas temporariamente por outro, durante a eleição, projetado para dar falsos totais. Nenhum estudo do software que deveria ser executado pode assegurar que o programa efetivamente executado não age mal.

O voto eletrônico é um evento especial, porque, normalmente, o eleitor não consegue estar atento a todas as partes envolvidas e descobrir se o seu voto foi corretamente contado. Não podemos assumir que o fabricante é honesto, ou que a autoridade eleitoral é honesta ou que os dois não conspiram juntos. Um sistema eleitoral deve ser a prova de tudo isso, mas isso é impossível num sistema puramente computacional."

O que há de comum nos pareceres desses dois autores é que determinar a confiabilidade técnica de sistemas eleitorais eletrônicos por meio da validação e certificação do software de fato utilizado é tarefa muito complexa que exige muitos procedimentos de alto grau tecnológico antes e durante a votação e apuração, proibitivamente cara e, na prática, impossível dentro de condições razoáveis de tempo e de orçamento.

Conforme as Diretrizes Voluntary Voting System Guidelines (VVSG) [Nist 2009], sistemas eleitorais devem oferecer total verificabilidade do resultado por via independente do software usado, estabelecendo as seguintes recomendações, assim traduzidas e adaptadas:

- *Ao menos dois registros do voto devem ser produzidos e um deles deve ser guardado em meio que não possa ser modificado pelo sistema (eletrônico) de votação, de forma que ambos registros não estejam sob controle de um único processo digital;*

- *O eleitor deve estar capacitado para verificar a igualdade dos dois registros do seu voto antes de deixar o local de votação;*
- *O processo de verificação dos registros do voto devem ser independentes e ao menos um deles deve ser conferível diretamente pelo eleitor;*
- *Os dois registros de um voto poderão ter sua consistência verificada posteriormente por meio de identificadores únicos que permitam a correlação dos registros.*

2.7. Disponibilidade Absoluta

Uma eleição não pode ser parcialmente adiada por indisponibilidade do sistema computacional. Deve ocorrer na data e hora marcadas em todo o território, não podendo ser postergada, nem mesmo parcialmente, por falha de qualquer origem, inclusive por ataque externo.

Assim, torna-se necessária forte resistência a ataques do tipo DoS (Denail of Service).

2.8. Outros Conceitos Desejáveis

Além dos conceitos essenciais e necessários acima descritos, interessa que outros conceitos também sejam atendidos por um sistema eleitoral digital como:

- Usabilidade - sistema amigável ao eleitor
- Direito de Refutação (dentro do local de votação)
- Celeridade – na votação e na apuração
- Recuperação de erros e retomada desburocratizada
- Portabilidade e logística econômicas
- Treinamento sempre disponível para eleitor e mesário
- Distribuição matricial de equipamentos e mesas eleitorais

3. Tabela de Conformidade

A tabela seguinte descreve a conformidade de três modelos de máquinas de votação com relação a conceitos derivados dos requisitos apresentados acima.

Os equipamentos analisados são os seguintes:

- Urnas Eletrônicas brasileiras, desenvolvidas pelo TSE, em uso no Brasil desde 1996. Também foram usadas no Paraguai, na Argentina e no Equador em 2004/6 mas depois foram abandonadas nesses países. Classificadas como de 1ª geração segundo [Rezende 2010]
- Equipamentos de votação SAES 3000, fabricadas pela empresa Smartmatic e usadas desde 2004 na Venezuela e mais recentemente na Bélgica e no Equador. Classificadas como de 2ª geração segundo [Rezende 2010]

- Equipamentos Vot-AR, fabricadas pela empresa MSA e usadas em algumas províncias da Argentina desde 2010 e mais recentemente no Equador. Classificadas como de 3ª geração segundo [Rezende 2010]

Tabela 2. Tabela de Conformidade

	UE2009 Brasil	**SAES Venezuela**	**Vot-Ar Argentina**
Princípio da Publicidade			
Gera voto impresso conferível pelo eleitor	NÃO	SIM	SIM
Eleitor pode conferir o conteúdo da gravação digital do voto antes de sair do local de votação	NÃO	NÃO	SIM
Fiscal externo pode verificar a igualdade entre os diversos registros do voto	-	NÃO	SIM
Fiscal externo pode acompanhar e verificar a contagem dos votos de cada seção eleitoral	NÃO	SIM	SIM
Princípio da Inviolabilidade Absoluta do Voto			
Garantia contra a violação do voto causada por um erro não detectado no software	NÃO	SIM	SIM
Garantia contra a violação do voto causada por reordenação do arquivo dos votos	NÃO	NÃO	SIM
Princípio da Independência do Software			
Uma modificação ou erro não detectado no software pode causar um erro indetectável no resultado da apuração	SIM	NÃO	NÃO
Conformidade com a Norma Técnica: *Voluntary Voting System Guidelines* (Seção 7.8)	NÃO	SIM	SIM
Outros Conceitos Desejáveis			
Tempo para publicação na Internet dos resultados por Seção, para fiscalização da Totalização	72h (2012)	?	2h (2011)
Conferência da assinatura digital do software feita em equipamento sob controle do fiscal	NÃO	?	SIM
Solução simples de diferenças entre o registro no papel e o registro digital do voto	-	NÃO	SIM
Distribuição matricial de urnas e mesas: o eleitor pode escolher uma urna livre para votar, sem ter	NÃO	SIM	SIM

que esperar que um eleitor anterior complete seu voto. Menores filas.			
Eleitor pode escolher a ordem dos cargos a votar	NÃO	SIM	SIM
Adaptação para plebiscitos e outras consultas - disponibilidade de opções "sim", "não", ou outras mais específicas	NÃO	SIM	SIM
Preparação simplificada, sem introdução de dados diferentes para cada seção/máquina	NÃO	NÃO	SIM
Troca de equipamento defeituoso e necessidade de recuperação de dados	LENTA SIM	LENTA SIM	RÁPIDO NÃO

4. Conclusões

Para finalizar, excluído o requisito da Disponibilidade Total, o processo eleitoral eletrônico brasileiro, com o respectivo equipamento de votação (urnas eletrônicas), não consegue atender aos demais requisitos e conceitos estabelecidos no presente trabalho, tais como: Soberania dos Direitos dos Eleitores e dos Candidatos, Tripartição dos Poderes, Princípio da Publicidade, Princípio da Inviolabilidade Absoluta do Voto e Princípio da Independência do Software (ou da Verificabilidade do Resultado Independente do Software).

A substituição da auditoria simplificada, pelos eleitores e candidatos, por uma validação e certificação exaustiva do software por agentes do Ministério Público, da OAB e dos partidos políticos foi totalmente ineficaz.

Dessa forma, o processo eleitoral eletrônico brasileiro recai a um processo sem garantias concretas de inviolabilidade e de justa apuração, onde se torna muito difícil estabelecer a sua confiabilidade técnica.

E essa dificuldade prática para estabelecer a confiabilidade técnica do software efetivamente usado no dia da eleição no Brasil, acrescida da não previsão de uma auditoria contábil deveras independente (pelos candidatos), equivale à adoção do Modelo da Segurança por Ofuscamento, descrito acima, e pretende que a eventual confiança subjetiva dada aos administradores eleitorais seja tomada como garantia indireta da confiança técnica sem, no entanto, permitir a determinação efetiva desta.

Vale lembrar que a confiabilidade subjetiva não pode ser imposta. Deveria ser conquistada, e a melhor forma de conquistá-la seria permitindo que se possa determinar a confiabilidade técnica objetiva.

Referências

Neumann, P.G. - Security Criteria for Electronic Voting - 16th National Computer Security Conference Baltimore, Maryland, September 20-23, 1993. - http://www.csl.sri.com/users/neumann/ncs93.html. Acessado em 07/09/14.

CT, Computer Technologists' Statement on Internet Voting – disponível em: http://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf 2012

Pieters, W. - Verifiability of electronic voting: between confidence and trust. In: Data Protection in a Profiled World. Springer, Dordrecht, pp. 157-175. ISBN 9789048188642, 2010. - http://doc.utwente.nl/72498/

Três, C.A.- A Soberania do Povo na Fiscalização do Exercício de sua Soberania. In: Seminário do Voto Eletrônico, Câmara dos Deputados, 29 de maio de 2002. - http://www.brunazo.eng.br/voto-e/textos/tres2.htm

TCFA, Decisão original do Tribunal Constitucional Federal da Alemanha em 03/03/2009
http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html

CMind, Comitê Multidisciplinar Independente. Relatório sobre o Sistema Brasileiro de Votação Eletrônica. Brasília: Edição dos Autores, 2010. Os temas referidos se encontram nas Seções 4.1.1 e 4.1.2- http://www.votoseguro.org/textos/CMind-1-Brasil-2010.pdf

Aranha, D. et al. - Vulnerabilidades no software da urna eletrônica brasileira. UnB, 2012. 36 pp. - disponível em http://sites.google.com/site/dfaranha/projects/relatorio-urna.pdf, visitado em 24 de setembro de 2014

Rivest R.R. , Wack, J.P. - On the notion of "software independence" in voting systems : USA, NIST/MIT, 28/07/2006 - http://people.csail.mit.edu/rivest/pubs/RW06.pdf

Stallman – A Opinião de Richar Stallman - http://www.vialibre.org.ar/2008/11/12/voto-digital-la-opinion-de-richard-stallman/

NIST, Voluntary Voting System Guidelines - NIST/US-EAC (2009). - Definição de Independent Verification Systems na Seção 7.8 - http://www.eac.gov/assets/1/AssetManager/VVSG_Version_1-1_Volume_1_-_20090527.pdf

Rezende, P. D. - Votação Eletrônica, 3ª Geração. CMind, 2010 – apresentado em cerimônia pública no TSE - http://www.cic.unb.br/docentes/pedro/trabs/TSE3G.pdf

