DOI: 10.9732/P.0034-7191.2019V118P097

Aspectos jurídicos, políticos e técnicos sobre sistemas eletrônicos de votação e a urna eletrônica brasileira

Legal, political and technical considerations on electronic voting systems and the brazilian voting machine

Augusto Tavares Rosa Marcacini[1]
Irineu Francisco Barreto Junior[2]

Resumo: Sistemas eletrônicos de votação demonstraram ser muito rápidos em proporcionar resultados finais, mas questões muito sensíveis são levantadas acerca de sua segurança e transparência. Este artigo discute o que é esperado de uma eleição política, comentando sobre princípios democráticos a serem

1 Livre-Docente em Direito pela Faculdade de Direito Universidade de São Paulo. Doutor em Direito Processual pela Faculdade de Direito Universidade de São Paulo. Vice-Presidente da Comissão de Direito Processual Civil, Membro da Comissão de Ciência e Tecnologia e Membro Consultor da Comissão de Informática Jurídica da Ordem dos Advogados do Brasil – OAB-SP. Advogado. São Paulo, SP, Brasil. *E-mail*: amarcacini@gmail.com

2 Pós Doutorando em Sociologia pela Faculdade de Filosofia, Letras e Ciências Humanas (FFLCH), da Universidade de São Paulo - USP. Doutor em Ciências Sociais pela Pontifícia Universidade Católica de São Paulo – PUC-SP. Docente do Programa de Mestrado em Direito da Sociedade da Informação e do Curso de Graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas (FMU-SP). São Paulo – SP, Brasil. Analista de Pesquisas da Fundação Seade - SP. *E-mail*: neubarreto@hotmail.com

seguidos, discutindo questões relacionadas à segurança da informação e a experiência internacional, e apresentando um breve relatório acerca dos métodos de auditoria que foram definidos e executados pelo Tribunal Superior Eleitoral brasileiro. Como conclusão, não há meio de conduzir uma eleição que simultaneamente atenda a estes três requisitos: a) votos anônimos; b) seja publicamente auditável; c) 100% digital. O artigo conclui que a chave para obtenção de segurança, segredo e transparência reside na aplicação de modelos que anulem a vulnerabilidade de sistemas de votação integralmente eletrônicos, tais como a adoção de máquinas de votação independentes do software e trilhas de auditoria em papel verificáveis pelo próprio eleitor.

Palavras-chave: eleições políticas; urnas eletrônicas; auditoria de eleições eletrônicas; voto secreto; princípio da publicidade; trilhas de papel; democracia; sociedade da informação.

Abstract: E-voting systems proved to be very fast to provide final results but very sensible issues arise on its security and transparency. This paper discuss what is expected from an political election, arguing about democratic principles to be followed, discussing issues related to information security and international experience, and presenting a brief report on some of auditing methods that were defined and executed by Brazilian High Electoral Court. As a conclusion, there is no way to hold an election that simultaneously meets these three requirements: a) anonymous votes; b) publicly auditable; c) 100% digital. The key for achieve security, secrecy and transparency is to abandon the use of 100% electronic voting systems, and adopt software-independent voting machines and paper auditing trails.

Keywords: political elections; voting machines; e-voting auditing; anonymous votes; publicity principle; paper trail; democracy; information society.

Sumário: Introdução. 1 - Informática e eleições. 2 - Duas importantes características de uma eleição democrática. 3 - Breve histórico do emprego de meios eletrônicos no sistema eleitoral brasileiro. 4 - Críticas ao uso de máquinas de votação exclusivamente eletrônicas, no Brasil e no mundo. 5 - Algumas experiências internacionais. 6 - A pouca auditabilidade das urnas eletrônicas brasileiras e seus riscos para a democracia. 6.1 - Métodos de auditoria empregados no Brasil. 6.2 - Votação paralela. 6.3 - Auditoria do código de programação. 6.4 - Testes públicos de segurança. Conclusões.

Introdução

O Brasil começou a usar dispositivos eletrônicos de votação em 1996, inicialmente apenas nas maiores cidades, e, após somente mais uma experiência parcial nas eleições de 1998, desde a eleição de 2000 o voto do eleitor brasileiro é coletado exclusivamente por meio digital. No entanto, é de se notar a pouca quantidade de estudos e publicações nacionais de maior densidade a respeito do uso das modernas tecnologias de informação em eleições políticas, em comparação com o que se observa nos meios internacionais.

É certo que nenhuma tecnologia causou tanto impacto nas sociedades humanas como a informática. O emprego de computadores se tornou um fato praticamente uníssono em quase todos os ramos de atividade, desde os de cunho produtivo, como também os de lazer. Computadores dominam a cena nos ambientes de trabalho e doméstico. Nesse contexto, é relevante considerar o uso do computador para

intermediar relações humanas, de modo que sua aplicação prática ou os meandros de seu funcionamento deixem de frequentar apenas o currículo tecnológico, fazendo-o adentrar também o das ciências humanas e, entre elas, o Direito.

O estudo acerca da aplicação e impacto da informática sobre as relações jurídicas e sociais é essencialmente um estudo multidisciplinar. Não é possível compreender o Direito sem compreender o fato sobre o qual ele se aplica. Se esse fato é de alguma maneira intermediado por sistemas informáticos, o que podemos chamar de *fato informático*, para bem aplicar o Direito a tais situações deve-se ter alguma noção a respeito do funcionamento dos computadores. Em especial, quando a questão se relaciona com a confiabilidade das informações representadas em formato digital, ao estudioso se faz necessário um entendimento mínimo sobre aspectos relacionados à segurança da informação. Nesse sentido, temas como o estudo das provas informáticas e o da votação eletrônica guardam elementos em comum, pois em ambos os cenários a compreensão do fato pressupõe um conhecimento mínimo acerca da segurança da informação e de como o dado digital é produzido, armazenado, transmitido, ou também alterado, de modo que se possa fazer um juízo valorativo mais preciso acerca da credibilidade de tais informações.

E talvez nenhum uso de computadores seja tão dependente de uma ampla visão holística de todos os aspectos envolvidos quanto o uso de computadores nas eleições políticas. Tal aplicação não é uma questão meramente técnico-informática, como não é exclusivamente jurídica, nem apenas afeta à ciência política, mas, sim, uma questão que exige a mais perfeita compreensão e sinergia do conhecimento abrangido por pelo menos essas três áreas do conhecimento.

Visões tecnológicas por demais estreitas, sem a compreensão do significado político de uma eleição, ou dos

princípios jurídicos que a regem, tendem a uma simplificação grosseira das dificuldades de se informatizar a colheita do voto, comparando-a com outras muitas tarefas que são razoavelmente bem realizadas pelo computador ou pela Internet, como, por exemplo, os serviços de *internet banking* ou a informatização dos processos judiciais. De outro lado, a visão estritamente jurídica tende a abordar o tema sob a ótica da normatização que o regulamenta e das decisões judiciais proferidas a seu respeito, descuidando-se da compreensão mais profunda acerca do funcionamento de sistemas informáticos, suas peculiaridades e seus limites, isto é, do *fato informático*.

É esta segunda visão que tende a dominar a literatura em Direito Eleitoral produzida no país, em que raramente a votação eletrônica brasileira é referida ou tratada com alguma profundidade; ou, quando algumas linhas são escritas sobre o tema, estas se resumem a repetir formalmente e de modo acrítico as leis e regulamentos que orientam as eleições, ou os julgamentos proferidos pela Justiça Eleitoral nas eventuais impugnações apresentadas por candidatos ou partidos, em questões que envolvam a tecnologia empregada. A experiência estrangeira também é muito pouco mencionada nesses estudos. Ainda enquanto estas linhas são escritas, o sítio informático do Tribunal Superior Eleitoral assevera que "*o sistema eletrônico de votação adotado no Brasil é referência mundial*"[3] mas, tal afirmação, não parece se confirmar em pesquisas feitas na literatura internacional sobre *e-voting*. De fato, são poucos os trabalhos internacionais que meramente citem a experiência brasileira, menos ainda que a considerem um paradigma a ser seguido.

3 TSE, página com informações sobre "Biometria e urna eletrônica", disponível em <http://www.tse.jus.br/eleitor-e-eleicoes/eleicoes/urna-eletronica/biometria-e-urna-eletronica> [acesso em 05/12/2017].

O presente artigo se propõe, então, a apresentar uma visão multidisciplinar da questão, abordando tanto os seus aspectos jurídico-político quanto tecnológicos. Como método de estudo, a pesquisa adentra tanto a experiência internacional quanto nacional, analisando os ângulos jurídicos, políticos e tecnológicos da aplicação da informática nas eleições políticas, especificamente quanto ao momento de coleta do voto, pois este pode ser considerado o ponto mais sensível na informatização de uma eleição, como será melhor desenvolvido no correr deste texto.

1 Informática e eleições

Como toda atividade que lida com grandes volumes de dados, as eleições políticas podem amplamente se beneficiar da utilização das novas tecnologias da informação e comunicação. Há várias tarefas que podem ser melhor desempenhadas mediante o uso de sistemas informáticos, o que será brevemente apresentado a seguir, para distingui-las do ponto central do presente estudo, que recai especialmente sobre o momento da coleta do voto. Antes e depois desse momento, muitas tarefas relacionadas a uma eleição podem ser informatizadas e suas dificuldades não destoam dos percalços gerais que acompanham a introdução das novas tecnologias da informação em outros ramos de atividade.

A organização de uma eleição depende do trato de um imenso volume de dados: cadastramento de eleitores, sua distribuição pelo território e a manutenção dessa base de dados ao longo do tempo; organização partidária e controle dos candidatos aos vários cargos eletivos em disputa; ou, para darmos mais um exemplo, a gestão de recursos materiais e humanos que serão utilizados na votação. Ainda durante o período que antecede o voto, o uso de meios informáticos,

em especial da Internet, pode servir para proporcionar um controle eficiente, público e transparente acerca dos orçamentos de campanha. Após o pleito os computadores são muitíssimo eficientes para realizar rapidamente a totalização de um grande número de votos, podendo igualmente valer-se das comunicações em rede para divulgação pública dos resultados finais. Em todos esses momentos, facilmente observáveis, a informática pode, como em qualquer outro ambiente, apresentar problemas e dificuldades de implantação, mas o trato e solução dessas questões não é algo diverso do que seria em outro cenário como, por exemplo, os já citados sistemas bancário ou judicial. O momento da coleta do voto, entretanto, configura um fato com peculiaridades únicas e, por isso, sua informatização é uma tarefa um tanto mais delicada.

2 Breve descrição do emprego de meios eletrônicos no sistema eleitoral brasileiro

Desde 1996, o Brasil começou a utilizar máquinas eletrônicas de votação que se tornaram conhecidas pelo impreciso nome de "urna eletrônica", eis que "urna", efetivamente, o equipamento não é. O vocábulo "urna" significa uma caixa ou repositório lacrado ou fechado e, no caso da "urna" eletrônica, não é disso que se trata. As expressões inglesas para designar tais apetrechos, *voting machines* – máquinas de votação – ou *e-voting machines* – máquinas eletrônicas de votação – neste segundo caso a excluir os aparelhos mecânicos ou eletromecânicos, teriam sido mais precisas. Trata-se, afinal, de um *computador*, controlado por um *software* como qualquer outro dispositivo eletrônico de propósito geral, cabendo a tal software definir todas as funções que serão executadas pela máquina. O aparelho nacional de votação

apresenta um mecanismo de entrada de dados via teclado, por meio do qual é coletada a vontade do eleitor que confere o seu voto em uma tela de vídeo para, em seguida, registrar as escolhas feitas em uma mídia interna de armazenamento exclusivamente digital e, ao final da votação, emitir um resultado tanto na forma de um boletim impresso, como na de arquivos digitais que serão transmitidos para uma central de totalização.

Desde as eleições de 2000, como já assinalado, todos os votos dos eleitores brasileiros passaram a ser colhidos, registrados e totalizados de modo *exclusivamente* eletrônico. Trata-se de uma experiência de grandes proporções, eis que o Brasil realiza eleições sempre em escala nacional em uma mesma data – não há, como em outros países, eleições parciais que ocorram apenas localmente – atingindo recentemente um universo de 144.088.912 eleitores aptos a votar na eleição de 2016, dos quais 118.757.780 compareceram.[4]

Para um país de dimensões territoriais agigantadas, e diante de tal número expressivo de eleitores que comparecem simultaneamente em um mesmo dia, é inegável que o uso das tecnologias da informação pode aprimorar a eficiência das eleições políticas. As novas tecnologias podem ser aplicadas para enviar resultados locais a partir dos pontos mais distantes e inacessíveis do território nacional, ou para facilmente somar milhões de votos e apresentar ao público em geral os resultados finais, esmiuçados em seus mais precisos detalhes. E meios informáticos podem ser usados para receber os votos diretamente dos eleitores, como também tem sido feito, sendo esse o aspecto mais sensível da informatização de eleições políticas.

4 Informações divulgadas pelo Tribunal Superior Eleitoral, disponíveis em <http://www.tse.jus.br/imprensa/noticias-tse/2017/Julho/tse-realizou-maior-eleicao-municipal-da-historia-em-2016>.

A vantagem mais perceptível, quanto ao uso das tecnologias da informação em uma eleição, é que tais meios proporcionam uma apuração extremamente rápida, mesmo diante de um universo de dezenas ou centenas de milhões de votos. Não há dúvida de que o uso de máquinas eletrônicas de votação agiliza e torna muitíssimo mais eficientes as tarefas de coleta de votos, sua apuração e divulgação posterior do resultado. A grande questão, todavia, é saber o quanto seguras são, de fato, as eleições conduzidas por meios eletrônicos, especialmente quando os votos são exclusivamente registrados na forma digital, e também compreender quais são os riscos envolvidos em todo esse processo.

3 Duas importantes características de uma eleição democrática e suas relações com a informatização do voto

Democracia não é um conceito novo. Entretanto, se o termo não for interpretado de forma binária, isto é, como comportando apenas dois tipos de regime político, o democrático e o não-democrático, e sim analisada a existência de uma vasta gradação de direitos e garantias estabelecidos em cada país, ou mesmo de práticas, tradições e experiências socioculturais, com tonalidades que possam ser consideradas mais ou menos afeitas à democracia, pode-se pensar em estabelecer uma escala variável e gradual de padrões democráticos. Como bem assinalado por Ana Cláudia Santano:

> Embora já não exista mais a necessidade de antes de legitimar as eleições, agora os desafios são outros, e quase todos conectados à transparência. Vincula-se diretamente com a distinção que se deve ter da democracia como procedimento da democracia com qualidade. Não se pode pensar que, somente porque se realizam eleições periódicas, mas em condições precárias de liberdade,

> com uma deficitária organização e que terminam elegendo a líderes com pouca ou nula capacidade de transformação social, é que há um ambiente democrático. A democracia como procedimento – em sua versão minimalista e "schumpteriana" – não agrega legitimidade a um governo, nem fomenta o sentimento de cidadania. Somente a democracia material, dotada de integridade e qualidade, é capaz de fortalecer princípios sociais concretos.
>
> A qualidade da democracia é um conceito complexo, porém essencial ao tema aqui exposto. Reporta-se ao grau em que, dentro de um regime democrático, uma convivência política se aproxima das aspirações democráticas da sua cidadania.[5]

Assim, soa possível dizer que, embora ideia antiga, o nível de democracia alcançado pela experiência moderna é um fato muitíssimo recente na história da humanidade. Para destacarmos um dos aspectos que são indissociáveis de uma moderna visão democrática, e que diz respeito intimamente ao tema aqui abordado, o "*sufrágio universal e pelo voto direto e secreto*" assegurado no art. 14 da Constituição Federal brasileira é uma prática ainda não efetivada por muitos países do globo e, mesmo nos países considerados democráticos, é um padrão que somente se consagrou em torno do último século.

O detalhe relevante dessa garantia do art. 14 da CF, que torna o cenário de uma eleição política significativamente diverso do de outros fatos cotidianos, é a exigência do voto secreto, uma prática relativamente nova na história do pensamento democrático. Como relatam Alvarez e Hall,[6] durante os primeiros 120 anos da história dos Estados Unidos, os votos eram apresentados pelo eleitor de forma pública e oral, até que cédulas de votação e as primeiras máquinas mecâ-

5 SANTANO, Ana Cláudia; **Voto impresso: por que tanta resistência? Resposta ao artigo 'O voto impresso e a falsa sensação de segurança' de Fernando Neisser**.

6 ALVAREZ, R. Michael; Hall, Thad E., **Electronic Elections**.

nicas de votação começaram a ser introduzidas. No Brasil, a ênfase ao voto secreto só seria dada pelo Código Eleitoral de 1932, que também consagrou o voto feminino.[7] Antes disso, ao final da monarquia, a chamada Lei Saraiva - Decreto nº 3.029, de 1881[8] – havia introduzido o voto secreto, mas o voto aberto seria restaurado durante a Primeira República.[9]

O sigilo do voto tem por objetivo assegurar a liberdade do eleitor de votar segundo a sua consciência. Essa parece ser a melhor forma encontrada para garantir que os eleitores – cada um deles – serão livres para expressar nada diverso do que a sua vontade íntima. O sigilo do voto busca proteger o eleitor de todos os tipos de pressão: daqueles vindos de seu círculo privado ou profissional (família, amigos, ou o seu patrão) ou dos que possam ser exercidos por autoridades, ou por aqueles que detenham quaisquer outras formas de poder capazes de influenciá-lo ou intimidá-lo.

Mas mesmo a característica de *secreto* que se atribui ao voto difere de outros tipos de segredo havidos como socialmente relevantes e, portanto, protegidos pelo Direito. É que os sigilos, em geral, destinam-se a proteger uma dada informação dos olhares de *outros* sujeitos, que não sejam partícipes daquela relação. Esse é o caso, por exemplo, do sigilo bancário, que convém ser aqui mencionado, uma vez que a altíssima informatização do sistema financeiro é por vezes apontada como exemplo de sucesso a justificar a viabilidade

7 Decreto nº 21.076, de 24 de fevereiro de 1932, disponível em: <http://www2.camara.leg.br/legin/fed/decret/1930-1939/decreto-21076-24-fevereiro-1932-507583-publicacaooriginal-1-pe.html>.

8 Disponível em <http://www2.camara.leg.br/legin/fed/decret/1824-1899/decreto-3029-9-janeiro-1881-546079-publicacaooriginal-59786-pl.html>. Dizia esse decreto, em seu art. 15, § 19, que: "O voto será escrito em papel branco ou anilado, não devendo ser transparente, nem ter marca, sinal ou numeração. A cédula será fechada de todos os lados, tendo rotulo conforme a eleição a que se proceder".

9 MACIEL, Ana Rosa Reis, **Brasil: do voto de cabresto ao voto eletrônico**.

da informatização de eleições. Afinal, se largas somas de dinheiro trafegam por canais de comunicação eletrônicos, por que não realizar eleições *online*, ou, como se faz no Brasil, por meio das chamadas urnas eletrônicas?[10] Mas o sigilo das transações bancárias é algo diverso daquele aplicado nas eleições. As operações não são sigilosas para o próprio banco, para o correntista, ou para aquele em cujo favor o pagamento ou a transferência são realizados. O mesmo se pode dizer do sigilo das comunicações, do sigilo profissional, ou do segredo de justiça. Não há sigilo, nesses casos todos, que atinja os partícipes dessas relações. Em uma eleição, o sigilo deve ser completo, atingindo todas as pessoas, mesmo as envolvidas no ato de votar. Os organizadores da eleição não podem saber "quem votou em quem" e sequer o próprio eleitor pode contar com alguma forma de identificar o seu próprio voto, pois isso poderia ser usado de maneira indesejável para obrigá-lo a demonstrar quem sufragou, tornando-o, pois, vulnerável tanto à coação como à prática de corrupção, isto é, a negociação de seu voto em troca de vantagens para si. Um eleitor submetido a alguma forma de pressão, da qual não consiga ou não possa se esquivar, poderia ser constrangido a provar para quem direcionou o seu sufrágio.

Em artigo que traz como referências outros estudos internacionais sobre a compra de votos, Steingraber, Signor e Silva desenvolvem, com emprego de modelos matemáticos, interessante estudo acerca do potencial impacto do suborno ao eleitor durante uma eleição.[11] Parece evidente, entretan-

10 V., a respeito dessa frequente comparação, SCHNEIER, Bruce. **Internet Voting vs. Large-Value e-Commerce**, disponível em: <https://www.schneier.com/crypto-gram-0102.html#10>.

11 STEINGRABER, Ronivaldo; SIGNOR, Diogo; SILVA, Elder Mauricio. **What is needed to change the result of an election: an analysis with agent-based models**.

to, que a certeza de que a "contrapartida" ao suborno será entregue pelo eleitor é fator determinante para o sucesso desse tipo de fraude. Assim, para ser eficaz na proteção do eleitor contra quaisquer constrangimentos, o voto deve ser secreto para todos, incluindo-se os votantes acerca de seu próprio voto. O sigilo do voto significa que nem mesmo o eleitor pode ser capaz de identificar o voto que manifestou, ou distingui-lo do conjunto de votos.

Assim, pode-se dizer que o voto dito *secreto* deve ser sobretudo um voto *anônimo,* não identificado e não identificável.

Entretanto, é necessário, ao mesmo tempo, que o resultado final possa ser demonstrado. E, mais do que isso, que possa ser *publicamente* demonstrado. Nas democracias, o povo é a fonte do poder, portanto, uma eleição popular é a gênese de todo o poder político. O objetivo mais óbvio de um processo eleitoral é proporcionar um resultado final que corresponda à vontade dos eleitores. Mas esses mesmos eleitores são sujeitos da eleição e devem ter o direito de controlar a lisura do pleito e a fidelidade do seu resultado. Assim, a *transparência* de todo o certame, o que implica a sua *auditabilidade pública,* é também um primado essencial para a democracia.

O cenário de uma eleição política, portanto, é bastante peculiar e não pode ser simploriamente comparado com outros ambientes que, com lustroso sucesso, foram completamente informatizados. Em um pleito todo o processo deve ser transparente, público, feito às claras e sob as vistas de toda a sociedade, mas cada voto deve ser completamente anônimo, zelando-se pela impossibilidade de sua identificação e, simultaneamente, conter elementos que permitam demonstrar sua autenticidade, impedindo fraudes.

Em síntese, uma eleição é um fato com características singulares, pois tem como premissas importantes dois re-

quisitos potencialmente conflitantes, sob o ângulo de sua efetivação prática: transparência (de todo o processo eleitoral) e sigilo (do voto).

É oportuno notar que, ao se reintroduzir o voto secreto no país, o legislador de então preocupou-se em descrever em detalhes *como* se faria para se obter tal sigilo, assegurando que as cédulas de votação pudessem ser, ao mesmo tempo, anônimas e confiáveis. Dizia o art. 57, do Código Eleitoral de 1932:

> Art. 57. Resguarda o sigilo do voto um dos processos mencionados abaixo.
>
> I - Consta o primeiro das seguintes providências:
>
> 1) uso de sobrecartas oficiais, uniformes, opacas, numeradas de 1 a 9 em séries, pelo presidente, à medida que são entregues aos eleitores;
>
> 2) isolamento do eleitor em gabinete indevassável, para o só efeito de introduzir a cédula de sua escolha na sobrecarta e, em seguida, fechá-la;
>
> 3) verificação da identidade da sobrecarta, a vista do número e rubricas;
>
> 4) emprego de urna suficientemente ampla para que se não acumulem as sobrecartas na ordem em que são recebidas.
>
> II - Consta o segundo das seguintes providências:
>
> 1) registro obrigatório dos candidatos, até 5 dias antes da eleição;
>
> 2) uso das máquinas de votar, regulado oportunamente pelo Tribunal Superior, de acordo com o regime deste Código.

No Código Eleitoral de 1950,[12] as "máquinas de votar" mencionadas na lei anterior foram eliminadas do texto, ficando assim dispostas as providências tendentes a assegurar o segredo do voto:

> Art. 54. O sigilo do voto é assegurado mediante as seguintes

12 Lei nº 1.164, de 24 de julho de 1950, disponível em: <http://www.planalto.gov.br/ccivil_03/leis/1950-1969/L1164.htm>.

providências;

1 – uso de sobrecartas oficiais uniformes, opacas e rubricadas pelo presidente da mesa receptora à medida que forem entregues aos eleitores;

2 – isolamento do eleitor em gabinete indevassável para o só efeito de introduzir a cédula de sua escolha na sobrecarta e, em seguida, fechá-la;

3 – verificação de autenticidade da sobrecarta à vista da rubrica;

4 – emprego de urna que assegure a inviolabilidade do sufrágio e seja suficientemente ampla para que se não acumulem as sobrecartas na ordem em que forem introduzidas.

Finalmente, o Código Eleitoral de 1965, atualmente em vigor, afirma em seu art. 82 que "o sufrágio é universal e direto; o voto, obrigatório e secreto", não trazendo um dispositivo exclusivo para definir os métodos empregados para assegurar o sigilo. No art. 146,[13] voltado a definir todo o ato de votar, são encontradas algumas disposições tendentes a proporcionar sigilo e auditabilidade à cédula de votação:

Art. 146. Observar-se-á na votação o seguinte:

.....

V - achando-se em ordem o título e a folha individual e não havendo dúvida sobre a identidade do eleitor, o presidente da mesa o convidará a lançar sua assinatura no verso da folha individual de votação; em seguida entregar-lhe-á a cédula única rubricada no ato pelo presidente e mesários e numerada de acordo com as Instruções do Tribunal Superior instruindo-o sobre a forma de dobrá-la, fazendo-o passar a cabina indevassável, cuja porta ou cortina será encerrada em seguida;

.....

IX - na cabina indevassável, onde não poderá permanecer mais de um minuto, o eleitor indicará os candidatos de sua preferência e dobrará a cédula oficial, observadas as seguintes normas:

13 Embora formalmente em vigor, o procedimento previsto no art. 146 tornou-se superado, diante da implementação do sistema eletrônico de votação, definido no art. 59, da Lei nº 9.504/1997.

> a) assinalando com uma cruz, ou de modo que torne expressa a sua intenção, o quadrilátero correspondente ao candidato majoritário de sua preferência;
>
> b) escrevendo o nome, o prenome, ou o número do candidato de sua preferência nas eleições proporcionais;
>
> c) escrevendo apenas a sigla do partido de sua preferência, se pretender votar só na legenda.
>
> X - ao sair da cabina o eleitor depositará na urna a cédula;
>
> XI - ao depositar a cédula na urna o eleitor deverá fazê-lo de maneira a mostrar a parte rubricada à mesa e aos fiscais de partido, para que verifiquem sem nela tocar, se não foi substituída;
>
> XII - se a cédula oficial não for a mesma, será o eleitor convidado a voltar à cabina indevassável e a trazer seu voto na cédula que recebeu; senão quiser tornar à cabina ser-lhe-á recusado a ocorrência na ata e ficando o eleitor retido pela mesa, e à sua disposição, até o término da votação ou a devolução da cédula oficial já rubricada e numerada;
>
> .....

Todas essas disposições, novas e antigas, demonstram uma visível preocupação em regrar a novidade democrática que se introduzia no sistema: *como* assegurar que votos anônimos sejam, ao mesmo tempo, confiáveis (ou auditáveis)?

A possibilidade de verificação de cédulas em papel, pelo próprio eleitor, é um bom meio de atingir esses requisitos. Cédulas podem ser preenchidas de forma anônima e mesmo assim é possível conferir sua autenticidade, seja usando papéis especiais, seja conferindo assinaturas de terceiros, como mesários e fiscais presentes à seção de votação, ou mediante a pública, contínua e atenta vigilância sobre as urnas em que as cédulas são armazenadas.

Evidentemente, o emprego das cédulas anônimas em papel não é um modelo à prova de falhas. Muito se sabe, especialmente pelas experiências passadas, acerca das possibilidades de fraude em uma eleição baseada no uso de cédulas de papel. Urnas podem ser violadas, cédulas podem

ser trocadas, ou a contagem manual, já em si não imune a erros involuntários, pode ser maliciosamente distorcida. A questão que precisa ser mais densamente analisada – daí a importância de se compreender o *fato informático* nesse ambiente eleitoral – reside em saber *se* e, principalmente, *como* as máquinas eletrônicas de votação podem ser melhores, nesse quesito, do que as cédulas de papel.

4 Críticas ao uso de máquinas de votação exclusivamente eletrônicas, no Brasil e no mundo

A partir do momento em que o eleitor escolhe o seu candidato, até a apuração final do resultado, uma série de passos precisa ser realizada. Este artigo é focado nos primeiros desses passos: como as opções do eleitor são colhidas, gravadas e contadas logo nas primeiras etapas, até que cada máquina de votação divulgue os votos que recebeu? Esse é o principal problema de sistemas eletrônicos de votação, porque a tarefa, aparentemente simples, envolve um paradoxo conceitual. Uma vez que cada urna eletrônica divulga, ao final do dia, os votos nela gravados, a conferência paralela do resultado final da eleição pode demandar um esforço hercúleo para os partidos políticos, candidatos, imprensa, ou qualquer um que pretenda auditar ou ao menos observar as eleições políticas. De qualquer modo, é apenas uma questão de coletar os números em cada máquina de votação e realizar a soma todos eles: pode ser trabalhoso, porém, é uma tarefa possível e cada vez mais viável com o aumento da capacidade de processamento dos dispositivos eletrônicos, que vêm gradativamente se tornando mais potentes e mais baratos.[14]

14 Nesse sentido, merece ser comentada a existência do projeto Você Fiscal, conduzido pelo Prof. Diego Aranha, voltado a estimular a conferência das eleições por voluntários do povo, com o uso de aplicativos instalados em

Por outro lado, conferir que cada máquina de votação registrou precisamente a entrada dos dados introduzidos por cada eleitor é uma questão conceitual bastante complexa, quando os votos precisam ser necessariamente secretos e anônimos. Não haveria tal problema se votos identificáveis fossem uma opção. Neste caso, votações eletrônicas seriam, sem qualquer sombra de dúvida, um inigualável meio de se conduzir eleições, uma vez que existem procedimentos confiáveis para auditar e rastrear dados digitais *identificados*. Nos sistemas bancário ou judicial, por exemplo, trafegam dados digitais identificados; no segundo caso os atos são assinados digitalmente por juízes, promotores e advogados, o que lhes confere grande segurança contra adulterações posteriores ao momento em que foram praticados. Fosse aberto o voto, assinaturas digitais também poderiam ser utilizadas para marcar o voto digital, tornando-o inalterável, identificável e rastreável. Em outros cenários em que se faz votações, como em assembleias societárias ou condominiais, nas quais o voto é aberto, o uso de assinaturas digitais para cada voto não seria um problema, de modo que até mesmo eleições *online* podem ser realizadas sem grandes dificuldades adicionais, ou, ao menos, sem mais dificuldades do que as observadas em outros atos da vida que são praticados pela Internet. Mas votos secretos e anônimos são, como já exposto acima, um dos mais importantes métodos a serem preservados em uma eleição democrática.

Há uma porção de tarefas que computadores podem fazer muito melhor do que humanos. Ao executar complexas (ou nem tanto) operações matemáticas ou lidar com gigantescos volumes de dados, sua superioridade é acima de qual-

seus aparelhos celulares, para captura do resultado do boletim de urna e envio dos dados para uma central de totalização independente (disponível em: <http://www.vocefiscal.org/> [acesso em 15/08/2016]).

quer dúvida. Mas conferir a autenticidade e a integridade de informações digitais pode ser um grande problema. Uma vez que computadores podem lidar com informações em taxas altíssimas de velocidade, eles também podem *modificar* tais informações de modo igualmente rápido. No momento, nenhum sistema informático pode ser considerado à prova de falhas, e os jornais frequentemente publicam notícias sobre ataques criminosos direcionados contra serviços *online* de grandes companhias ou de poderosas entidades públicas. Assim sendo, como podem os eleitores confiar que suas escolhas foram, logo no princípio, corretamente registradas na máquina de votação? Pode o software da própria urna eletrônica alterar esse voto registrado até o momento final da eleição? A máquina o somará corretamente ao expedir o chamado "boletim de urna", contendo o total de votos ali armazenados? Quem são os sujeitos que devemos temer e que podem fraudar uma eleição: invasores externos, apenas, ou desenvolvedores, técnicos ou gerentes internos?

Pessoas comuns normalmente confiam naquilo que elas podem ver, mas o que quer que um computador faça ou exteriorize estar fazendo, é apenas o resultado de uma atividade para a qual ele foi especificamente programado. Quando alguém escreve uma letra "x" em uma folha de papel, o "x" que ele pode ver é real e foi uma consequência direta de sua ação física, produzida com uma caneta em punhos, que deixou rastros de tinta que tingiram as fibras do papel. Quando uma tecla é pressionada no teclado do computador, o que aparece na tela de vídeo não é uma consequência direta da ação, mas sim o resultado de uma sequência de comandos de programação. *Uma outra pessoa* previamente programou o computador para exibir na tela *a mesma tecla* que foi pressionada, ou de outro modo nada aconteceria, o computador nada faria por si mesmo! Tudo

o que um computador executa encontra-se previamente programado e estabelecido pelo software nele inserido.

Como afirmado por Rebecca Mercuri:

> Sistemas inteiramente eletrônicos não proporcionam nenhuma forma pela qual o eleitor possa confiavelmente verificar que o voto inserido corresponde àquele que foi registrado, transmitido ou tabulado. Qualquer programador pode escrever um código que exiba uma coisa na tela, registre outra, e ainda imprima outro resultado. Não há nenhum jeito conhecido de assegurar que isso não está acontecendo dentro de um sistema de votação.[15]

Entre outras questões, essa submissão do computador ao que está definido em sua programação é uma das peculiaridades que se deve ter em mente quando se quer interpretar o fato informático, mas a experiência leva a crer que pessoas comuns, não versadas nos meandros da informática, não estão suficientemente conscientes disso.

Em 2000, Bruce Schneier, um dos mais respeitados profissionais da área de segurança da informação, publicou algumas notas sobre os incidentes que ocorreram nas eleições da Flórida daquele ano, dizendo que mais tecnologia não iria resolver tais problemas. Ele afirmou que:

> Certamente, a antiquada tecnologia de votação da Flórida é em parte culpada, mas tecnologias mais novas não iriam magicamente fazer com que os problemas se fossem. Elas poderiam até mesmo tornar piores as coisas, adicionando mais camadas de tradução entre os eleitores e contadores de voto, evitando recontagens.
>
> Eis minhas primeiras preocupações sobre votação por computa-

15 MERCURI, Rebecca. **Rebecca Mercuri's Statement on Electronic Voting**.. Em nossa tradução. No original: "Fully electronic systems do not provide any way that the voter can truly verify that the ballot cast corresponds to that being recorded, transmitted, or tabulated. Any programmer can write code that displays one thing on a screen, records something else, and prints yet another result. There is no known way to ensure that this is not happening inside of a voting system".

> dores: não há uma cédula em papel para retornar. Maquinas de votação computadorizadas, tenham elas como interface teclado e monitor, ou uma tela sensível ao toque como as máquinas de automação bancária, poderiam facilmente tornar as coisas piores. Você precisar confiar que o computador gravou os votos corretamente, tabulou os votos corretamente, e manteve registros precisos. Você não pode retornar para as cédulas em papel e tentar descobrir o que o eleitor queria fazer. E computadores são falíveis; algumas das máquinas de votação computadorizadas desta eleição falharam misteriosa e irrecuperavelmente.[16]

Uma vez que não há nenhuma maneira de olhar dentro da máquina e ver o que ela está realmente fazendo durante o dia da eleição, não há muita coisa que fiscais ou observadores possam conferir ou observar no local da votação. Como dito em relatório de segurança que será mais amplamente comentado adiante, *"as pessoas não podem ver elétrons, então elas não podem observar a contagem dos votos quando um sistema de votação DRE é usado"*.[17] Ou, ainda, como assinalado por Rebeca Mercuri:

> Votação e tabulação eletrônicas fazem com que as tarefas desem-

16 SCHNEIER, Bruce. **Voting and technology**. Em nossa tradução. No original: "Certainly Florida's antiquated voting technology is partially to blame, but newer technology wouldn't magically make the problems go away. It could even make things worse, by adding more translation layers between the voters and the vote counters and preventing recounts. That's my primary concern about computer voting: There is no paper ballot to fall back on. Computerized voting machines, whether they have keyboard and screen or a touch screen ATM-like interface, could easily make things worse. You have to trust the computer to record the votes properly, tabulate the votes properly, and keep accurate records. You can't go back to the paper ballots and try to figure out what the voter wanted to do. And computers are fallible; some of the computer voting machines in this election failed mysteriously and irrecoverably".

17 GONGGRIJP, Rop; et. al. **Nedap/Gr enendaal ES3B voting computer: a security analysis**. Em nossa tradução. No original: "People cannot see electrons, so they cannot observe a vote count when a DRE voting systems is used".

> penhadas pelos funcionários da eleição, fiscais e autoridades sejam puramente procedimentais, e removem a oportunidade de realizar verificações bipartidárias. Qualquer processo computadorizado de eleição é, portanto, confiado ao pequeno grupo de indivíduos que programam, constroem e mantêm as máquinas de votação.[18]

Deste modo, sua proposta para o uso de sistemas eletrônicos de votação é:

> Cabe, portanto, àqueles que estejam envolvidos com eleições que se abstenham de utilizar qualquer sistema que não preveja uma cédula de papel anônima e indiscutível que possa ser verificada de forma independente pelo eleitor antes da confirmação de seu voto, que seja usada pelo comitê eleitoral para demonstrar a veracidade de qualquer totalização do voto eletrônico, e esteja também disponível para auditoria e recontagem manual.[19]

Em 2006, um artigo escrito por Rivest e Wack introduziu o conceito de sistemas de votação cuja auditoria possa ser considerada "dependente do software" ou "independente do software". Tais conceitos indicam modelos em que a verificação da correção dos resultados da eleição depende ou não, de modo essencial, de exame do software do sistema de votação. E assim concluem:

> (...) a habilidade de provar a correção do software se reduz rapidamente conforme o software se torne mais complexo. Seria efe-

18 Idem, ibidem. Em nossa tradução. No original: "Electronic balloting and tabulation makes the tasks performed by poll workers, challengers, and election officials purely procedural, and removes any opportunity to perform bipartisan checks. Any computerized election process is thus entrusted to the small group of individuals who program, construct and maintain the machines."

19 Idem, ibidem. Em nossa tradução. No original: "It is therefore incumbent upon all concerned with elections to refrain from procuring any system that does not provide an indisputable, anonymous paper ballot which can be independently verified by the voter prior to casting, used by the election board to demonstrate the veracity of any electronic vote totals, and also available for manual audit and recount".

> tivamente impossível testar adequadamente os futuros (e atuais) sistemas de votação à busca de falhas ou introdução de fraudes, portanto, estes sistemas sempre remanesceriam suspeitos em sua capacidade de proporcionar eleições seguras e precisas.[20]

Entre nós, o professor da Unicamp, Diego Aranha, que reuniu conhecimentos teóricos e experiências práticas sobre segurança de máquinas eletrônicas de votação, ao participar dos testes públicos permitidos pelo TSE, atestou em trabalho recente que:

> Máquinas de votar do tipo DRE são largamente criticadas na literatura científica, principalmente por suas falhas de projeto e implementação, impossibilidade de auditoria independente de software e vulnerabilidade contra-ataques internos.[21]

Em poucas palavras, esses reconhecidos expertos em segurança informática acreditam que não há melhor maneira de auditar uma eleição do que proporcionando um meio de recontar os votos independentemente do sistema eletrônico, ou do *software* que o controla. Qualquer outro meio de apro-

20 RIVEST R.R.; WACK, J.P. **On the notion of "software independence" in voting systems.** Em nossa tradução. No original: "the ability to prove the correctness of software diminishes rapidly as the software becomes more complex. It would effectively be impossible to adequately test future (and current) voting systems for flaws and introduced fraud, and thus these systems would always remain suspect in their ability to provide secure and accurate elections". Um detalhe interessante da biografia de Ronald Rivest, a título de apresentar suas credenciais à comunidade jurídica, merece comentário: ele é o "R" da sigla "RSA", o nome do algoritmo de assinatura digital que tem sido utilizado nos "processos digitais" e é produzida com o uso dos certificados digitais com que os profissionais do direito se tornaram familiarizados nos anos recentes. Em 1977, ele, juntamente com seus colegas (Adi) Shamir e (Leonard) Adleman desenvolveram o primeiro algoritmo criptográfico de assinatura digital (v. LEVY, Steven. **Crypto: how the code rebels beat the government saving privacy in the digital age**). Seu prestígio na área de segurança da informação é, portanto, inegável.

21 ARANHA, Diego F. et al, **Execução de código arbitrário na urna eletrônica brasileira**.

priadamente auditar uma eleição – dependente, portanto, de auditar o software – seria demasiadamente caro ou praticamente impossível, até mesmo por profundos especialistas, isso sem contar que pode não haver especialistas disponíveis em número suficiente para realizar tal tarefa durante uma agigantada eleição nacional.

Para o cidadão médio importa compreender que um software é uma ferramenta essencialmente alterável e que está constantemente em evolução. O teste de segurança feito hoje – acaso fosse possível fazer um teste extensivo e definitivo – nada diz por si só sobre o software que será utilizado amanhã, na semana seguinte, ou na próxima eleição. Mais do que isso, não soa democrático impedir que cidadãos comuns sejam capazes, por si mesmos, de aferir a confiabilidade de uma eleição política. Diante disso, Rivest e Wack propõem o uso do modelo conhecido pela sigla VVPAT – *Voter Verifiable Paper Audit Trail*, ou, no vernáculo, Trilha de Auditoria em Papel Verificável pelo Eleitor. Os modelos em uso no mundo variam, entre imprimir o voto[22] que o eleitor previamente inseriu diretamente na máquina, ou, no caminho inverso, fazer leitura ótica da cédula previamente preenchida manualmente pelo eleitor.

5 Algumas experiências internacionais

Embora tenha sido bastante disseminada em nosso país a afirmação de que haveria uma exclusiva e pioneira *expertise* brasileira em desenvolver sistemas eletrônicos de

22 Na Argentina, a impressão é feita em cédula que contém um chip, no qual o voto também é gravado em formato digital e posteriormente lido, no momento da totalização (v. BRUNAZO FILHO, Amílcar; CORTIZ, Maria Aparecida. **2º Relatório CMind sobre o Equipamento Argentino de Votação usado em 2011**); embora o modelo também seja passível de críticas (v. AMATO, Francisco et. al, **Vot.Ar: una mala elección**).

votação, que, como já mencionado na introdução, são anunciados como "referência internacional", tais assertivas não se sustentam no exame da literatura ou dos eventos fáticos e políticos que se desenrolaram no cenário mundial nas últimas décadas.

O Brasil não foi pioneiro no emprego de máquinas de votação, nem tão pouco desenvolveu localmente a tecnologia utilizada nas chamadas urnas eletrônicas que, desde o primeiro momento, foram produzidas por fabricantes estrangeiros, fornecedores também no mercado internacional. O Brasil pode merecer algum destaque no cenário internacional por ter organizado eleições nacionais com uso de formas exclusivamente eletrônicas de coleta do voto e, considerando sua expressiva população e número de eleitores, isso pode, de algum modo, representar uma façanha. Mesmo em termos puramente quantitativos, entretanto, não é o Brasil o maior utilizador de novas tecnologias da informação em eleições, sendo, neste quesito, superado pela Índia, que nas eleições de 2009 utilizou 1.378.352 máquinas eletrônicas de votação em suas eleições nacionais.[23]

Por outro lado, se outros países desenvolvidos não adotaram máquinas de votação de forma mais ampla, isso pode ser atribuído ao contexto político dessas nações e não à falta de suficiente expertise tecnológica. Nos EUA, a decisão sobre os métodos de votação é pulverizada em nível local, de tal sorte que cabe a cada Condado a decisão de adotar, ou não, meios eletrônicos de votação.[24] O mesmo

23 PRASAD, Hari, et. al., **Security Analysis of India's Electronic Voting Machines**.

24 A organização Verified Voting divulga informações detalhadas sobre o uso de meios eletrônicos nas eleições norte-americanas, apontando, Condado a Condado, os meios utilizados e, se for o caso, que tipo de equipamento informático é empregado (disponível em <https://www.verifiedvoting.org> [acesso em: 15/08/2016]).

sucedeu na Alemanha, em que a implementação vinha sendo feita gradativamente,[25] até que os modelos de máquinas de votação utilizados foram todos banidos por decisão de sua Suprema Corte, como será comentado adiante. Dada a centralização de poder que se observa no nosso país, em mãos de entidades federais – o que, diga-se, não é uma característica exclusiva da esfera eleitoral – o Brasil impôs e implementou nacionalmente o uso de urnas eletrônicas. Foi essa centralização que proporcionou uma rápida e ampla informatização eleitoral no país, quando comparado com outras nações.

Por outro lado, o Brasil utiliza a mesma tecnologia empregada desde a sua primeira eleição eletrônica. Embora a classificação desses equipamentos em gerações possa se sujeitar a critérios variados, adotando a classificação apresentada por Amílcar Brunazo Filho, pode-se afirmar que o desenvolvimento dessas tecnologias eleitorais já produziu três diferentes gerações de equipamentos. [26] O Brasil, porém, ainda utiliza máquinas de primeira geração, que outros países têm banido ou substituído por equipamentos mais confiáveis. Tais equipamentos de primeira geração são também conhecidos pela sigla DRE – *Direct Recording Eletronic machines* – pois têm como característica registrar os votos diretamente em uma base de dados interna, fazendo-o em meio exclusivamente eletrônico.

A Holanda foi o primeiro país que, após empregar máquinas eletrônicas de votação, decidiu abandoná-las para retornar às cédulas em papel, por decisão de suas autoridades, tomada em 2007.[27] Naquele país, eram utilizadas

25 SEEDORF, Sebastian. **Germany: The Public Nature of Elections and its Consequences for E-Voting**.

26 BRUNAZO FILHO, Amílcar, **Modelos e Gerações dos equipamentos de votação eletrônica**.

27 Dutch pull the plug on e-voting. The Register, 01/10/2007. Disponível em:

máquinas DRE e, apesar de críticas pontualmente feitas por especialistas, as autoridades e o fabricante garantiam que o sistema era à prova de falhas. Em 2006, um grupo de ativistas, formado por especialistas em segurança da informação, intitulado "Wij vertrouwen stemcomputers niet" (nós não confiamos em computadores de votação), logrou obter três desses equipamentos, que depois submeteriam a testes independentes: as máquinas lhes foram fornecidas por duas diferentes municipalidades, a que eles se referem apenas pelas letras A e B, tendo a primeira lhes emprestado um dos equipamentos e a segunda vendeu-lhes dois deles. Assim, afirmando terem posse e propriedade legais sobre as máquinas de votação, os expertos fizeram testes de segurança que sequer podem ser considerados exaustivos – duraram apenas um mês – mas que foram suficientes para expor as fragilidades dos tais aparelhos. Narraram como um terceiro poderia violar os sistemas caso lograsse se aproximar dos equipamentos, apontando ainda que o sistema não era, evidentemente, nem um pouco imune a uma fraude interna. Com a divulgação do *paper*,[28] um juiz decidiu pela proibição do uso desses equipamentos que, em seguida, foram definitivamente banidos pela própria autoridade eleitoral daquele país. Desde então, a Holanda voltou a utilizar cédulas em papel.

Pouco depois, na Alemanha, a questão foi submetida ao Poder Judiciário, que também determinou a cessação do uso de máquinas DRE por decisão da Suprema Corte Federal.[29] O

<http://www.theregister.co.uk/2007/10/01/dutch_pull_plug_on_evoting>.

28 GONGGRIJP, Rop; et. al. **Nedap/Groenendaal ES3B voting computer: a security analysis**.

29 Versão em inglês da decisão está disponível em: <http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html>

emprego de máquinas de votação na Alemanha, embora antigo, era bastante restrito, dado que cabia ao poder local optar, ou não, pelo seu uso. Diferentemente do que ocorrera pouco antes na Holanda, a decisão não foi fruto do clamor gerado pela demonstração de insegurança dos equipamentos, mas por razões principiológicas. Entendeu a Corte alemã que os meios eletrônicos de votação em uso violavam o princípio da publicidade das eleições, impedindo que cidadãos comuns, sem conhecimento profundo de tecnologia, ou sem necessitar realizar extensos exames periciais nos equipamentos, pudessem acompanhar todos os passos de uma eleição. Segundo Sebastian Seedorf, ao comentar tal decisão:

> Somente um governo eleito pode legitimamente exercer poder em uma democracia. A legitimidade é baseada no fato de que o povo sabe que a eleição e seu específico resultado final é uma genuína expressão de sua vontade. Para a Corte, uma eleição sem a confiança do eleitorado é insuficiente. Não é suficiente que uma eleição seja simplesmente livre e justa e que um governo tenha sido democraticamente eleito – o povo também precisa estar confiante de que esse foi o caso. O fato e a percepção do fato formam as duas faces de uma mesma moeda: conformidade com os princípios constitucionais de uma eleição (que uma eleição seja livre, justa, secreta etc.) e confiança nessa conformidade constituem precondições para uma democracia viável.[30]

30 SEEDORF, Sebastian, **Germany: The public nature of elections and its consequences for e-voting**. Em nossa tradução. No original: "Only an elected government can legitimately exercise power in a democracy. This legitimacy is based on the fact that the people know that the election with its specific outcome result is a genuine expression of their will. For the Court, an election without the trust of the electorate in insufficient. It is not enough that an election simply is free and fair and that a government has been democratically elected – the people must also be confident that this has been the case. The fact and the perception of the fact form the two sides of the same coin: compliance with the constitutional election principles (that an election has been free, fair, secret etc.) and confidence in compliance with them, constitute preconditions for a viable democracy".

Segundo o mesmo autor, embora o Tribunal não tenha terminantemente proibido o uso de equipamentos eletrônicos de votação, mas apenas proibido equipamentos que não se adequassem ao caráter público de uma eleição, desde essa decisão as votações foram realizadas exclusivamente com cédulas de papel.

Na Índia, equipamentos eletrônicos de votação eram utilizados desde a década de 1980. Do mesmo modo, autoridades asseguravam que o sistema era imune a falhas ou fraudes. Um ativista hindu, todavia, alegando ter recebido um dos equipamentos de fontes anônimas – nem foi dito como o equipamento teria sido obtido pelas tais fontes – realizou testes de segurança com apoio de outros expertos internacionais, produzindo, tal como ocorrera anos antes na Holanda, um *paper*[31] descritivo em que apontou várias fragilidades das máquinas de votação e demonstrou como poderiam ser fraudadas. As repercussões da divulgação foram mais dramáticas gerando, inicialmente em desfavor do perito, a acusação de prática criminosa na obtenção dos equipamentos.[32] Mas a evidência de que a segurança das máquinas era frágil levou a Corte Constitucional da Índia a também decidir pela sua substituição.[33] Segundo Barley e Sharma, nesse julgamento de 2013:

> a Suprema Corte decidiu que uma trilha de papel é um requerimento indispensável de eleições livres e justas e que a confiança dos eleitores no sistema somente poderia ser alcançada por meio

31 PRASAD, Hari K. et al, **Security Analysis of India's Electronic Voting Machines**.

32 Polícia prende hacker indiano que identificou falha em urna eletrônica. G1, 22/08/2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/08/policia-prende-hacker-indiano-que-identificou-falha-em-urna-eletronica.html>.

33 Civil Appeal No. 9093 of 2013, disponível em: <https://www.eff.org/document/dr-subramanian-swamy-vs-election-commission-india>.

> de transparência, a qual necessita a exigência de introduzir um acurado e verificável sistema de votação. Entretanto, no mesmo fôlego, a Corte paradoxalmente permitiu à Comissão Eleitoral introduzir o sistema VVPAT em fases.[34]

Os três cenários apontados podem ser comparados à situação brasileira em diversos aspectos. Em primeiro lugar, em todos eles havia uma confiança não demonstrada – e que se mostrou equivocada – na infalibilidade de equipamentos eletrônicos que fazem apenas registro digital dos votos (isto, é, máquinas DRE). Em segundo lugar, conquanto as máquinas de Holanda e Índia sejam diferentes entre si e diferentes das que emprega nossa Justiça Eleitoral, os problemas técnicos foram evidenciados somente quando os equipamentos puderam ser escrutinados por profissionais experientes, sem quaisquer limitações de ordem prática, técnica, legal, procedimental, ou temporal, o que reproduz o cenário em que um fraudador real atuaria. Ficou evidenciado, portanto, que tais equipamentos só contam com a questionável "segurança por obscuridade", modelo que vem sendo veementemente considerado inseguro pelos especialistas.[35] Criminosos

34 BAILEY, Rishab; SHARMA, Rohit; **E-voting case law in India**. Em nossa tradução. No original: "the Supreme Court held that the 'paper trail' is an indispensable requirement of free and fair elections and that the confidence of voters in the system could only be achieved through transparency which necessitated the need to introduce an accurate verifiable system of voting. However, in the same breath, the Court paradoxically allowed the Election Commission to introduce the VVPAT system in a phased manner".

35 Considera-se "segurança por obscuridade" um modelo cuja segurança dependa de esconder de terceiros como o sistema funciona. Sua segurança é considerada fraca, pois, tão logo seu funcionamento seja compreendido – o que, de modo mais ou menos árduo, pode ser inevitável – todas as defesas desmoronam, sendo precisamente isso que ocorreu com os supra comentados testes feitos nas máquinas de votação holandesas e indianas. Seguro, para as modernas exigências, é o sistema que se mantenha íntegro, não obstante todo o seu funcionamento seja conhecido. Bruce Schneier, em prefácio de sua prestigiada obra sobre criptografia aplicada, faz uma ótima analogia sobre o que pode ser considerado segurança, em contraposição à

que desejassem fraudar as eleições certamente não teriam dificuldade – sequer estariam preocupados com os freios morais ou legais – em obter ao menos uma das centenas de milhares de urnas eletrônicas existentes no país para tentar desvendar meios de violá-las. Em terceiro lugar, o cenário político-jurídico não é diverso. Busca-se, em todas as democracias, realizar eleições transparentes, públicas, auditáveis e secretas. E sequer se diga que o quadro sociopolítico brasileiro possa conter qualquer peculiaridade a justificar o emprego de máquinas DRE. Nesse caso, o exemplo da Índia é por demais significativo. Embora não tão extenso territorialmente como o Brasil, trata-se de país com gritantes contrastes sociais e econômicos; há uma população de analfabetos muitíssimo superior; há locais pouco desenvolvidos em que não há energia elétrica disponível para alimentar os equipamentos; suas eleições passadas retratam históricos de corrupção e coação sobre eleitores comparáveis aos que já se sucederam em nosso país,[36] fatos esses que são comumente apontados no Brasil como justificativa bastante e suficiente para o emprego de máquinas exclusivamente eletrônicas nas votações. Portanto, a experiência desses três países para restringir a análise aos três casos mais visíveis de mudança de rumos, merece ser considerada no Brasil.

mera obscuridade: "Se eu pego uma carta, tranco-a em um cofre, escondo o cofre em algum lugar de Nova York e então peço a você para tentar ler a carta, isso não é segurança. Isso é obscuridade. Por outro lado, se eu pego uma carta e a tranco em um cofre, e depois lhe entrego o cofre juntamente com o seu projeto, mais uma centena de cofres idênticos, com suas combinações, de modo que você e os melhores arrombadores de cofre do mundo possam estudar o mecanismo da tranca – e você assim mesmo não consegue abrir o cofre e ler a carta – isso é segurança" (**Applied Cryptography**, p. xix).

36 BAILEY, Rishab; SHARMA, Rohit, ob. cit.

6 A pouca auditabilidade das urnas eletrônicas brasileiras e seus riscos para a democracia

6.1 Métodos de auditoria empregados no Brasil

Durante as últimas duas décadas, o Brasil experimentou um movimento pendular em que ora a lei determina o uso de trilhas físicas, ora o método é revogado, sem que as trilhas físicas sejam extensivamente empregadas. E, ao invés delas, outros meios de auditoria foram tentados, o que será comentado neste subtítulo.

6.2 Votação paralela

O primeiro método usado para conferir a votação eletrônica nas eleições brasileiras ficou conhecido como votação paralela, uma prática que se iniciou em 2002[37] e pode ser assim resumidamente explicada: a) dois dias antes da eleição, quando todas as urnas eletrônicas já estão posicionadas nas suas respectivas seções de votação, quatro delas são escolhidas aleatoriamente em uma audiência pública realizada em cada um dos Tribunais Regionais; b) em seguida agentes na eventual companhia de fiscais de partidos que voluntariamente se apresentem, vão o mais rápido possível às seções de votação onde estão instaladas as máquinas sorteadas, que são dali retiradas, substituídas por outras para serem usadas na eleição, e trazidas para a Capital, onde a apuração paralela será realizada; caso as máquinas sorteadas estejam lotadas em seções distantes centenas de quilômetros da Capital, podem se passar algumas horas entre o momento do

37 A votação paralela é prevista no art. 66, § 6º, da Lei nº 9.504/1997, introduzido pela Lei nº 10.408/2002 (disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10408.htm>).

sorteio e sua "captura"; c) é solicitado a fiscais de partidos e outros observadores presentes que preencham cédulas de voto simulado que serão usadas na apuração paralela; d) no domingo de eleição, durante o mesmo horário da votação, as urnas eletrônicas sorteadas são ligadas e usadas como se ainda estivessem no seu lugar de origem; os votos simulados previamente preenchidos são inseridos nessas urnas durante um procedimento bastante formal e lento, registrado em uma câmara de vídeo; e) ao final do dia, as urnas assim auditadas divulgam os boletins de urna, com os votos nelas registrados, e seu resultado é comparado com os votos simulados que nela foram inseridos.

O objetivo de tal método de auditoria seria provar que qualquer urna eletrônica aleatoriamente escolhida está trabalhando adequadamente e soma corretamente todos os votos nela inseridos. De fato, esse tipo de teste pode ser útil para conferir erros involuntários de programação, mas é bastante duvidoso que seja capaz de evitar fraudes perpetradas por um ataque interno. Uma vez que máquinas eletrônicas de votação são tão complexas como qualquer outro computador, há incontáveis meios com que um fraudador interno, com suficiente acesso ao código de programação, poderia contar para evitar ser detectado por esse tipo de teste. Tudo o que o fraudador interno precisaria seria um tipo de "interruptor" (provavelmente desenhado por *software*) que liga e desliga as rotinas de fraude. Se o software detectar qualquer sinal de que a urna eletrônica não está no seu local de votação (então, ela pode estar sendo auditada), a fraude pode ser desligada. A forma como a votação paralela é conduzida faz com que as urnas eletrônicas trabalhem em condições muitíssimo diversas das que estão no ambiente normal de votação. Por exemplo, como pode ser observado nesses testes, o intervalo de tempo entre quaisquer dois votos subsequentes é irreal,

pois cada voto simulado precisa ser gravado em vídeo, ser inserido em um segundo computador (usado para somar paralelamente os votos), seguindo-se um procedimento formal e demorado, de modo que se passam vários minutos entre um voto e seu subsequente. Em condições reais, três ou quatro eleitores teriam usado a urna eletrônica em um intervalo desses. Por outro lado, as urnas testadas recebem votos durante intervalos de tempo regulares, espalhados ao longo do dia de votação, enquanto as máquinas que estão nas seções de votação podem ficar inoperantes por vários minutos, uma vez que o fluxo real de eleitores não é constante. Como assinalado no relatório holandês, a votação paralela não é um método confiável de auditoria pois "*o criador do software que desvia votos pode executar uns poucos testes que distinguiriam uma eleição real e as mais rigorosas e disciplinadas votações paralelas*".[38] O método é também criticado no chamado "relatório Brennan", um extenso estudo realizado nos Estados Unidos sobre a segurança de sistemas de votação:

> No entanto, mesmo sob as melhores circunstâncias, o teste paralelo é uma medida de segurança imperfeita. O teste cria uma "corrida armamentista" entre os testadores e o atacante, mas é uma corrida em que os testadores nunca podem ter certeza de que eles venceram.[39]

38 GONGGRIJP et. al, ob. cit. Em nossa tradução. No original: "the author of the vote-stealing software can perform quite a few tests that would discriminate between a real election and anything but the most rigorous and disciplined parallel tests".

39 NORDEN, Lawrence et al. **The Machinery of Democracy: voting system security, accessibility, usability and cost**. Em nossa tradução. No original: "even under the best of circumstances, parallel testing is an imperfect security measure. The testing creates an 'arms-race' between the testers and the attacker, but the race is one in which the testers can never be certain that they have prevailed".

Em conclusão, sabendo como a votação paralela será executada, um atacante imaginativo que consiga comprometer o software da urna é capaz de criar dúzias de "alarmes" para detectar diferentes sinais de que a máquina não está em seu local de votação, a indicar que está sendo auditada, e, assim, desligar as programações fraudatórias. Portanto, esse método de auditoria não é eficiente contra um atacante experiente e premeditado. Pode servir, de qualquer modo, para detectar erros involuntários. Mas, mesmo assim, se erros involuntários forem detectados em apenas quatro máquinas, o que pode ser feito com as demais? Teriam elas os mesmos problemas? Se elas também têm os mesmos erros, como os verdadeiros votos poderão ser recuperados? Parece claro, assim, que se trata de um sistema útil enquanto ateste que erros não foram detectados. Não soa compatível com um pensamento crítico e científico, que deveria estar aberto à possibilidade de que ambos os cenários pudessem ser apontados, isto é, tanto erros como acertos no confronto com o resultado final.[40]

6.3 Auditoria do código de programação

Em 2003, uma nova Lei[41] estabeleceu um segundo método de auditoria e que foi posto em prática durante a

40 O TSE, entretanto, dá à apuração paralela uma dimensão não corroborada pela comunidade científica, afirmando que "a simulação da votação, que foi filmada continuamente, comprovou que cada voto foi registrado na urna sem nenhuma anormalidade e que a soma, ao final, correspondeu ao que ocorreu no primeiro turno, com todos os votos aproveitados normalmente" (TSE, **Eleições 2018: auditorias confirmam segurança das urnas eletrônicas em SP e MG**, com divulgação de alguns dados referentes à votação paralela realizada em 2018).

41 Lei nº 10.704/2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2003/L10.740.htm >.

eleição de 2004. Observadores externos foram autorizados a examinar o software usado nas urnas eletrônicas e nos sistemas de totalização. Pode parecer uma forma adequada de fiscalizar a eleição pois, afinal, se o software é correto, seus resultados deverão ser corretos. As dificuldades de auditar o imenso volume de linhas de código de programação, todavia, mostraram-se imensas, como, aliás, é sustentado pelos especialistas acima citados.

Note-se que essa auditoria tem sido realizada sob regras extremamente restritivas, impostas pela autoridade eleitoral brasileira. Nenhum fiscal é autorizado a levar consigo o código-fonte dos programas, nem utilizar seus próprios equipamentos para examiná-lo. O §2º, do art. 66, da lei nº 9.504/1997, com redação dada pela supracitada Lei nº 10.740/2003, diz que a análise dos programas será feita "nas dependências do Tribunal Superior Eleitoral". Não se permite, portanto, aos fiscais, o mesmo acesso que os especialistas holandeses e indianos tiveram às máquinas de votação de seus respectivos países, como já narrado acima. As únicas operações permitidas consistem em ler as linhas de programação na tela de alguns computadores disponíveis na sede do Tribunal Superior Eleitoral. Entretanto, o código fonte a ser examinado se estende por dezenas de milhares de arquivos em formato texto (txt), de modo que pouco pode ser testado a partir da mera permissão para ler algumas dessas linhas, de alguns desses arquivos, nas telas dos computadores disponibilizados. Mesmo que fiscais pudessem levar consigo o código-fonte e tentar o mais possível localizar falhas ou potenciais fraudes – é de se destacar que isso não é uma tarefa ordinariamente fácil e talvez somente alguns poucos e altamente especializados profissionais de segurança da informação possam ser capazes de detectar fraudes mais sofisticadas – conferir que o código revisado

está correto ainda não é o suficiente. Isto porque conferir posteriormente que o código revisado é o mesmo que gerou o software final usado na eleição não é tarefa simples.

De acordo com os procedimentos desse método de auditoria: a) o código-fonte dos programas estaria disponível para exame (nos termos postos acima) por algumas semanas; b) em data determinada, em cerimônia formal com a presença de todos os fiscais, o código seria compilado[42] e o arquivo executável daí resultante seria digitalmente assinado por eles; c) posteriormente, os arquivos executáveis seriam instalados em cada urna eletrônica, sendo facultado aos fiscais conferir a veracidade das assinaturas digitais, testando-as diretamente em cada uma das urnas.

À parte o fato de que não foi proporcionado um acesso direto ao código-fonte, todo esse método de auditoria aparenta ser inútil para repelir fraudes internas. A compilação e cerimônia de assinatura aparenta ser uma tarefa "puramente procedimental", para repetir as sábias palavras da professora Rebecca Mercuri.[43] Uma vez que é impossível entrar dentro do computador, ou dentro dos *chips* de silício, para vigiar o que está acontecendo ali, tudo que os fiscais podem observar é um funcionário da Corte eleitoral operando um computador e dando a ele alguns comandos com o uso do teclado. Não há absolutamente nenhuma maneira de assegurar, naquele fatídico momento, que o código compilado era o mesmo que foi (superficialmente) revisado nas semanas anteriores. Quando a compilação é terminada, os fiscais usam suas chaves criptográficas privadas para assinar os arquivos executáveis, mas toda a operação é feita no mesmo

42 Compilação é o nome dado à conversão do código-fonte (arquivos de texto, legíveis, contendo comandos escritos) para os arquivos executáveis, que serão compreendidos e utilizados pelo computador.

43 v. nota 17.

computador do Tribunal. Não há como demonstrar que os arquivos assinados são os mesmos que resultaram da prévia compilação. Finalmente, conferir se as assinaturas digitais são verazes em cada uma das centenas de milhares de urnas eletrônicas, uma a uma, é uma tarefa quase impossível. O melhor que pode ser feito é apenas proceder a esse teste por amostragem. Mesmo assim, conferir uma assinatura digital em um computador desconhecido (as próprias urnas eletrônicas) é uma operação duvidosa, especialmente se é justamente esse computador o objeto de auditoria. Ora, se uma urna foi "contaminada" por código de programação indevido, quem quer que o tenha feito teve acesso suficiente ao sistema para boicotar também a conferência das assinaturas, isto é, fazer com que a tela da máquina auditada exiba a informação de que as assinaturas estão corretas, já que se considera improvável a falsificação das próprias assinaturas digitais. Mas um sistema adulterado em que se execute tal tentativa de conferência pode, mesmo diante de assinaturas falsas, fazer com que a tela das urnas exiba a informação de que são verdadeiras. Por fim, conferir que o software não foi alterado, numa checagem feita vários dias antes da eleição, não é prova racional bastante e suficiente de que o mesmo software estará ali no dia da eleição.

Como conclusão, tudo o que esse método produz pode ser assim resumido: solicita-se aos fiscais que assinem alguns arquivos executáveis que não podem ser provados como o verdadeiro resultado da compilação, que, por sua vez, foi feita por um software compilador desconhecido, usando códigos-fonte que não se pode assegurar que sejam os mesmos que já não foram completamente esquadrinhados. E, depois disso, o trabalho de conferir as assinaturas em cada urna eletrônica (ou, ao menos, em um número representativo delas) não se mostra uma tarefa simples, especialmente ao

longo de um país de dimensões continentais como o Brasil.

6.4 Testes públicos de segurança

Um terceiro método de auditoria foi implementado em 2009. É um tipo de competição aberta à inscrição de grupos de expertos em informática para que tentem desferir ataques para testar eventuais vulnerabilidades do sistema, a respeito do sigilo dos votos, da disponibilidade das urnas ou o risco de falhas durante o dia da eleição, entre outras questões relacionadas à segurança. Nos meios profissionais da informática, tais testes são conhecidos como "testes de penetração".

Note-se, todavia, que os testes autorizados, e do modo como o foram, não podem ser considerados um completo teste de penetração, uma vez que os participantes devem seguir regras bastante restritivas definidas pelo TSE. A Resolução nº 23.444/2015, do TSE, que "dispõe sobre a realização periódica do Teste Público de Segurança (TPS) nos sistemas eleitorais que especifica", cria todo um conjunto formal de procedimentos e limites impensáveis em um cenário real, isto é, um quadro em que um criminoso tentasse manipular os resultados de uma eleição verdadeira. A título de breve referência, encontram-se previstas, nessa Resolução, quatro comissões formadas por membros da Justiça Eleitoral (Comissão Organizadora, Comissão Reguladora, Comissão Avaliadora e Comissão de Comunicação Institucional) para atuar nesses testes. A Comissão Reguladora, em especial, tem como suas atribuições, entre outras, "definir os procedimentos e a metodologia utilizados" e "aprovar os planos de testes elaborados pelo(s) técnico(s) e/ou grupos de técnicos" (art. 9º). A burocratização do teste de penetração ainda prevê uma divisão em fases formalmente definidas (arts. 17 a 20).

Crimes informáticos, evidentemente, não são orientados por metodologias criadas por suas vítimas, sequer seguem planos previamente aprovados por elas, daí se podendo concluir pelo caráter extremamente artificial e restritivo desses testes de segurança oficialmente autorizados.

Em poucas palavras, os expertos não podem tentar qualquer tipo de ataque que tenham habilidade técnica em perpetrar, mas somente aqueles que são previstos nas regras instituídas pelo departamento técnico daquela Corte. Mesmo assim, em cada edição desse teste público, algo de falho foi descoberto pelos profissionais que dele tomaram parte. Em 2009, o grupo vencedor conseguiu capturar ondas eletromagnéticas emitidas pelo teclado das urnas, enquanto o eleitor digitava, e isso foi suficiente para que fosse desvelado o voto então inserido, em clara ameaça ao seu sigilo.[44]

Em 2012, uma das equipes foi bem-sucedida em reverter a ordem aleatória do registro digital do voto, de modo que foi possível recuperar a sequência cronológica em que os votos foram inseridos na urna, expondo outra grave ameaça ao sigilo do voto. Como desdobramento, essa equipe publicou um relatório sobre as vulnerabilidades encontradas, com sugestões para o aprimoramento da segurança do sistema brasileiro de votação eletrônica.[45] Além de algumas falhas de segurança que foram detectadas, o relatório também aponta que a auditoria permitida pelo TSE é um "*modelo inapropriado de ataque*", uma vez que "*ênfase significativa é colocada no desenho de características de segurança resistentes apenas a*

44 TSE encerra testes do sistema eletrônico premiando melhores contribuições. <http://agencia.tse.jus.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1255520>

45 ARANHA, D.F. et al. **Software vulnerabilities in the Brazilian voting machine**. In Design, Development, and Use of Secure Electronic Voting Systems.

atacantes externos, quando as ameaças internas representam um risco muito mais alto".[46]

De fato, ameaças internas não podem ser detectadas por esse tipo de teste. Mesmo que as equipes participantes fossem autorizadas a livremente executar amplos testes de penetração, ou revisar completamente o software, não há meio de assegurar que o software revisado será exatamente o mesmo que estará instalado nas urnas eletrônicas durante a eleição, em centenas de milhares delas.

Ainda de acordo com os relatórios dessa equipe de especialistas, que detectou a falha reportada:

> Nós apresentamos uma coleção de vulnerabilidades de software nas urnas eletrônicas brasileiras, o que permitiu a eficiente, exata e não rastreável recuperação da ordem dos votos inseridos eletronicamente. Associando a informação com a lista ordenada de eleitores, obtida externamente, isso permite uma completa violação do sigilo do voto. O registro cronológico público dos eventos mantido pelas urnas eletrônicas também permite a recuperação de um específico voto, inserido em um dado momento no tempo. As consequências dessas vulnerabilidades foram discutidas sob um modelo de ataque realista e mitigações foram sugeridas. Várias falhas adicionais no software e em seu processo de desenvolvimento foram detectadas e discutidas com recomendações concretas para sua mitigação. Em particular, foi demonstrado como derrotar o único mecanismo empregado pela urna eletrônica para proteger o sigilo do voto.
>
> .....
>
> Em particular, nós podemos concluir que não houve nenhuma melhoria significativa em segurança nos últimos 10 anos. Proteção inadequada do sigilo do voto, a impossibilidade prática de realizar uma completa ou minimamente efetiva revisão do software e a verificação insuficiente da integridade do software são preocu-

46 Idem, ibidem. Em nossa tradução. No original: "significant emphasis is put on the design of security features resistant only to outsider attackers, when insider threats present a much higher risk".

> pantes. Uma vez que essas três propriedades são críticas para garantir o sigilo e integridade dos votos, os autores repetem as conclusões do relatório supracitado e defendem a reintrodução de trilhas de autoria em papel verificáveis pelo eleitor para permitir uma simples verificação dos resultados de forma independente do software. Trilhas de auditoria em papel distribuem o procedimento de auditoria entre todos os eleitores, que se tornam responsáveis por verificar que os seus votos foram corretamente registrados pela urna eletrônica, desde que uma auditoria seja feita posteriormente para conferir que a contagem eletrônica e manual de votos são equivalentes.
>
> .....
>
> Nós acreditamos que, por essa razão, diante dos severos problemas de segurança discutidos nesse relatório, o software usado no sistema de votação brasileiro não satisfaz mínimas e plausíveis exigências de segurança e transparência.[47]

47 Idem, ibidem. Em nossa tradução. No original: "We presented a collection of software vulnerabilities in the Brazilian voting machines which allowed the efficient, exact and untraceable recovery of the ordered votes cast electronically. Associating this information with the ordered list of electors, obtained externally, allows a complete violation of ballot anonymity. The public chronological record of events kept by the voting machines also allows recovering a specific vote cast in a given instant of time. The consequences of these vulnerabilities were discussed under a realistic attacker model and mitigations were suggested. Several additional flaws in the software and its development process were detected and discussed with concrete recommendations for mitigation. In particular, it was demonstrated how to defeat the only mechanism employed by the voting machine to protect ballot secrecy. (...) In particular, we can conclude that there was no significant improvement in security in the last 10 years. Inadequate protection of ballot secrecy, the impossibility in practice of performing a full or minimally effective software review and the insufficient verification of software integrity are still worrisome. Since these three properties are critical to guarantee the anonymity and integrity of votes, the authors repeat the conclusions of the aforementioned report and defend the reintroduction of voter-verified paper audit trails to allow simple software-independent verification of results. Paper audit trails distribute the auditing procedure among all electors, who become responsible for verifying that their votes were correctly registered by the voting machine, as long as an audit is done afterwards to check that the electronic and manual vote counts are equivalent. (...) We believe that,

No último teste, realizado em 2017, a equipe comandada pelo Professor Diego Aranha logrou alcançar o estágio *máximo e final* de uma invasão a sistemas digitais: conseguiu demonstrar que, violando o *flash card* que dá carga dos programas em cada uma das urnas, é possível *executar código arbitrário* nas máquinas. Nesse nível de invasão, o atacante assume o comando da máquina invadida, podendo determinar que ela execute o que o invasor quiser, como descrito no relatório publicado pela equipe participante:

> Foi possível executar código arbitrário na urna eletrônica. Como apresentado anteriormente, foram várias as demonstrações de que os ataques obtinham total controle sobre o software da urna eletrônica.[48]

No cenário de uma eleição, o grupo poderia, então, fazer a urna eletrônica desviar votos. Ao final, o mesmo relatório conclui:

> O software de votação da urna eletrônica brasileira ainda não satisfaz requisitos mínimos de segurança e transparência e está muito aquém da maturidade esperada de um sistema crítico em produção há mais de 20 anos. Recomenda-se ao TSE revisar cuidadosamente suas práticas de desenvolvimento e considerar novamente a adoção do voto impresso para fornecer garantias fortes do funcionamento correto do sistema no dia das eleições, acompanhando a experiência de outros países. Espera-se que os resultados aqui descritos contribuam com o debate no país a respeito da introdução de um registro físico de votos individuais como uma forma de aprimorar segurança e transparência do sistema de votação.[49]

---

for this reason, and in light of the severe security problems discussed in this report, the software used in the Brazilian voting system does not satisfy minimal and plausible security and transparency requirements".

48 ARANHA, Diego F. et al, **Execução de código arbitrário na urna eletrônica brasileira**.

49 Idem, ibidem.

Enfim, mesmo diante de poucos e restritos testes – que não podem ser comparados ao pleno acesso que os expertos holandeses e indianos tiveram às máquinas de votação de seus países – nossa urna eletrônica apresentou vulnerabilidades inaceitáveis para uma eleição justa, pública, segura e democrática. É de se duvidar de sua alegada segurança, pois não se conhece equipamento eletrônico imune a falhas involuntárias ou a ataques premeditados e, como dito, a experiência internacional não dá elementos em favor dessa suposta inexpugnabilidade.

Conclusões

Auditar uma eleição é tarefa ainda mais difícil do que auditar qualquer outro tipo de sistema informatizado. Duas características principais fazem uma eleição eletrônica um desafio singular, de modo que auditá-la é uma tarefa mais complexa do que auditar sistemas eletrônicos usados em outros cenários: a exigência de sigilo do voto e o fato de que a eleição é realizada inteira e exclusivamente em um único dia. A experiência brasileira encaixa-se perfeitamente como um exemplo disso a confirmar as críticas de expertos internacionais. Todos os três métodos de auditoria descritos neste artigo, e que têm sido usados para conferir a confiabilidade das urnas eletrônicas por mais de uma década, provaram ser insuficientes, ou são veementemente repelidos por estudos internacionais, especialmente por não ser um meio eficaz para evitar um ataque interno.

A pesquisa feita também não corrobora as afirmações de que o Brasil seja "referência internacional" em sistemas de votação eletrônica. Há, no mundo, uma larga profusão de estudos sobre *e-voting*, das quais as referências deste artigo são uma mera amostra e, neles, a experiência brasileira

é raramente mencionada, menos ainda é tomada como um modelo a ser seguido. Ademais, máquinas DRE, como a brasileira, são equipamentos corriqueiramente conhecidos nos meios tecnológicos – sendo, aliás, alvo de duras críticas, como as que foram exibidas neste artigo – não se podendo considerá-las como uma inovação tecnológica nacional. Anote-se que também na literatura brasileira produzida pelos profissionais da área de segurança da informação é recomendado o uso de trilhas físicas.

Ao que tudo indica, a título de conclusão, não há meio de conduzir uma eleição que preencha simultaneamente estas três características: a) receba votos anônimos; b) seja publicamente auditável; c) seja 100% digital (como nas máquinas DRE). Apenas dois desses requisitos podem ser oferecidos ao mesmo tempo. Se tolerável o voto aberto, como em votações societárias, corporativas, ou condominiais, uma eleição por registros exclusivamente digitais pode ser transparente e totalmente auditável. Nas democracias, uma eleição política não pode abrir mão dos dois primeiros itens. A chave para obter segurança, sigilo do voto e transparência é abandonar o uso de sistemas totalmente digitais de registro do voto, com a adoção de máquinas de votação que sigam o modelo de auditoria independente do software, com trilhas físicas auditáveis (VVPAT).

Pela terceira vez em nosso país, o uso de trilhas físicas foi objeto de previsão legal, dispondo a lei sobre sua utilização para as eleições de 2018,[50] mas teve, por ora, seu cumprimento suspenso por decisão do STF proferida em medida cautelar à Adin 5.889.[51] Na esteira dos estudos técnicos,

50 Lei nº 13.165/2015, que introduziu o art. 59-A na Lei nº 9.504/1997 (disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13165.htm)

51

tanto nacionais como internacionais, bem como das melhores práticas adotadas noutros países, é de se esperar que essa lei prevaleça e que o julgamento de mérito da Adin 5.889 não confirme a decisão provisória, em nome do aprimoramento do processo eleitoral brasileiro.

Referências

ALEMANHA. Corte Constitucional Federal. **Judgment of the Second Senate of 3 March 2009 on the basis of the oral hearing of 28 October 2008 –** 2 BvC 3/07, 2 BvC 4/07. Disponível em: <http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html> [acesso em 05/12/2017].

ALVAREZ, R. Michael; HALL, Thad E. **Electronic Elections: the perils and promises of digital democracy**. Princeton: Princeton University Press, 2008 (e-book).

AMATO, Francisco; et. al. **Vot.Ar: una mala elección**. Disponível em: <https://ivan.barreraoro.com.ar/vot-ar-una-mala-eleccion/> [acesso em 05/12/2017].

ARANHA, Diego F. et al. **Software vulnerabilities in the Brazilian voting machine. In Design, Development, and Use of Secure Electronic Voting Systems**. USA: IGI Global (2014), <https://sites.google.com/site/dfaranha/pubs/aranha-karam-miranda-scarel-12-book> [acesso em 05/12/2017].

ARANHA, Diego F et al. **The return of software vulnerabilities in the Brazilian voting machine**. Research Gate (mar/2018). Disponível em <https://www.researchgate.net/publication/323470546_The_Return_of_Software_Vulnerabilities_in_the_Brazilian_Voting_Machine> [acesso em 05/11/2018].

ARANHA, Diego F. et al. **Execução de código arbitrário na urna eletrônica brasileira**. Research Gate (jul/2018). Disponível em <https://www.researchgate.net/publication/326261911_Execucao_de_codigo_arbitrario_na_urna_eletronica_brasileira> [acesso em 05/11/2018].

BAILEY, Rishab; SHARMA, Rohit. **E-Voting case law in India**. In: MAURER, Ardita Driza; BARRAT, Jordi (Organizers). E-Voting Case Law. Surrey: Ashgate Publishing, 2015.

BARRETO JUNIOR, Irineu Francisco; LEITE, Beatriz Salles Ferreira. Responsabilidade civil dos provedores de aplicações por ato de terceiro na lei 12.965/14 (marco civil da internet). **Revista Brasileira de Estudos Políticos**. Belo Horizonte, n. 115, pp. 391-438. jul./dez. 2017.

BRASIL. **Decreto nº 21.076, de 24 de fevereiro de 1932 (Código Eleitoral)**. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/1930-1939/decreto-21076-24-fevereiro-1932-507583-publicacaooriginal-1-pe.html> [acesso em 05/12/2017]

BRASIL. **Decreto nº 3.029, de 9 de janeiro de 1881.** Disponível em <http://www2.camara.leg.br/legin/fed/decret/1824-1899/decreto-3029-9-janeiro-1881-546079-publicacaooriginal-59786-pl.html> [acesso em 05/12/2017].

BRASIL. **Lei nº 1.164, de 24 de julho de 1950 (Código Eleitoral)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/1950-1969/L1164.htm> [acesso em 05/12/2017].

BRASIL. **Lei nº 13.165/2015**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13165.htm> [acesso em 05/12/2017].

BRASIL. **Lei nº 4.737/1965**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L4737.htm> [acesso em 05/12/2017].

BRASIL. **Lei nº 9.504/1997**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9504.htm> [acesso em 05/12/2017].

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.444/2015**. Disponível em <http://www.tse.jus.br/legislacao/codigo-eleitoral/normas-editadas-pelo-tse/resolucao-no-23-444-de-30-de-abril-de-2015-2013-brasilia-2013-df> [acesso em 05/11/2018].

BRASIL. Tribunal Superior Eleitoral. **Eleições 2018: auditorias confirmam segurança das urnas eletrônicas em SP e MG**. Disponível em <http://www.tse.jus.br/imprensa/noticias-tse/2018/Outubro/eleicoes-2018-auditorias-confirmam-seguranca-das-urnas-eletronicas-em-sp-e-mg> [acesso em 05/11/2018].

BRASIL. Tribunal Superior Eleitoral. **Biometria e urna eletrônica**. Disponível em: <http://www.tse.jus.br/eleitor-e-eleicoes/eleicoes/urna-eletronica/biometria-e-urna-eletronica> [acesso em 05/12/2017].

BRASIL. Tribunal Superior Eleitoral. **TSE realizou maior eleição municipal da história em 2016**. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2017/Julho/tse-realizou-maior-eleicao-municipal-da-historia-em-2016> [acesso em 05/12/2017].

BRASIL. **TSE encerra testes do sistema eletrônico premiando melhores contribuições**. <http://www.investidura.com.br/biblioteca-juridica/resenhas/etica/123261-tse-encerra-testes-do-sistema-eletronico-premiando-melhores-contribuicoes> [acesso em 05/12/2017].

BRUNAZO FILHO, Amílcar; CORTIZ, Maria Aparecida. **2º Relatório CMind sobre o Equipamento Argentino de Votação usado em 2011**. Disponível em: <http://www.

brunazo.eng.br/voto-e/textos/CMind-2-Argentina-2011.htm> [acesso em 05/11/2017].

BRUNAZO FILHO, Amílcar; CORTIZ, Maria Aparecida. **Fraudes e defesas no voto eletrônico**. São Paulo: All Print, 2006)

BRUNAZO FILHO, Amílcar; MARCACINI, Augusto Tavares Rosa. **Legal Aspects of E-Voting in Brazil**. In: MAURER, Ardita Driza; BARRAT, Jordi (Organizers). E-Voting Case Law. Surrey: Ashgate Publishing, 2015.

BRUNAZO FILHO, Amílcar. **Modelos e Gerações dos equipamentos de votação eletrônica**, 2014. Disponível em: <http://www.brunazo.eng.br/voto-e/textos/modelosUE.htm> [acesso em 05/12/2017].

DUTCH pull the plug on e-voting. The Register, 01/10/2007. Disponível em: <http://www.theregister.co.uk/2007/10/01/dutch_pull_plug_on_evoting> [acesso em 05/12/2017].

GONGGRIJP, Rop; et. al. **Nedap/Groenendaal ES3B voting computer: a security analysis**, 2006. Disponível em: <http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b--en.pdf> [acesso em 05/12/2017].

GRAAF, Jeroen van de. **O mito da urna**. Disponível em: <https://inscrypt.dcc.ufmg.br/wp-content/uploads/2017/11/o-mito-da-urna.pdf> [acesso em 05/12/2017].

HÁ 30 anos, 'JB' revelou escândalo do Proconsult e derrubou fraude na eleição. Jornal do Brasil, 27/11/2012. Disponível em: <http://www.jb.com.br/pais/noticias/2012/11/27/ha-30-anos-jb-revelou-escandalo-do-proconsult-e-derrubou-fraude-na-eleicao/> [acesso em 05/12/2017].

HERRNSON, Paul S. et al. **Voting Technology: The not-so-simple act of casting a ballot**. Washington: Brookings Institution Press, 2008 (e-book).

INDIA. Suprema Corte da Índia. **Civil Appeal No. 9093 of 2013**. Disponível em: <https://www.eff.org/document/dr-subramanian-swamy-vs-election-commission-india> [acesso em 05/12/2017].

LEVY, Steven. **Crypto: how the code rebels beat the government saving privacy in the digital age**. New York: Penguin Books, 2001.

MACIEL, Ana Rosa Reis. **Brasil: do voto de cabresto ao voto eletrônico**. Portal de e-governo, inclusão digital e sociedade do conhecimento, UFSC. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/brasil-do-voto-de-cabresto--ao-voto-eletrônico> [acesso em 05/12/2017].

MERCURI, Rebecca. **Rebecca Mercuri's Statement on Electronic Voting**. <http://www.notablesoftware.com/RMstatement.html> [acesso em 05/12/2017].

MERCURI, Rebecca. **Electronic Vote Tabulation Checks & Balances**. Ph.D. thesis, defended on 27 October 2000 at the School of Engineering and Applied Science of the University of Pennsylvania, Philadelphia, PA, USA.

NADAF, Ronaldo Moises. **Modelo Brasileiro de Votação Mecatrônica Independente de Software ou Votação Mecatrônica**. XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2014/0046.pdf> [acesso em 05/12/2017].

NEISSER, Fernando. e-Leitor: **O voto impresso e a falsa sensação de segurança**. Jota, 20/05/2016. Disponível em: <https://jota.info/colunas/e-leitor/e-leitor-o-voto-

-impresso-e-falsa-sensacao-de-seguranca-20052016> [acesso em 05/12/2017].

NORDEN, L.D. et al. **The Machinery of Democracy: voting system security, accessibility, usability and cost**. New York: Brennan Center of Justice, NYU, 2006. Disponível em: <http://www.brennancenter.org/sites/default/files/publications/Machinery_Democracy.pdf> [acesso em 05/12/2017].

POLÍCIA prende hacker indiano que identificou falha em urna eletrônica. G1, 22/08/2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/08/policia-prende-hacker-indiano-que-identificou-falha-em-urna-eletronica.html> [acesso em 05/12/2017]

PRASAD, Hari K.; HALDERMAN, J. Alex; GONGGRIJP, Rop. **Security Analysis of India's Electronic Voting Machines**, 2010. Disponível em: <https://indiaevm.org/evm_tr2010-jul29.pdf> [acesso em 05/12/2017].

REZENDE, Pedro Antônio Dourado. **Devagar com o andor da urna: Comentários sobre testes de penetração no TSE e de sua cobertura midiática**. Disponível em: <http://cic.unb.br/~rezende/trabs/penetracao.html> [acesso em 05/12/2017].

RIVEST, Ronald L.; VIRZA, Madars. **Software Independence Revisited**. Disponível em: <https://people.csail.mit.edu/rivest/pubs/RV16.pdf> [acesso em 05/12/2017].

RIVEST, Ronald L., WACK, John P. **On the notion of "software independence" in voting systems**, National Institute of Standards and Technology (NIST), USA (28 July 2006) <http://people.csail.mit.edu/rivest/pubs/RW06.pdf > [acesso em 05/12/2017].

ROCHA, Felipe Melo de Assis. **Inconstitucionalidade da urna eletrônica**. Revista Direito e Liberdade, v. 3, n. 2, 2005. Disponível em: <http://www.esmarn.tjrn.jus.br/revistas/index.php/revista_direito_e_liberdade/article/view/280> [acesso em 05/12/2017].

SANTANO, Ana Cláudia. **Voto impresso: por que tanta resistência? Resposta ao artigo 'O voto impresso e a falsa sensação de segurança' de Fernando Neisser**. Academia.edu, jul/2016. Disponível em <https://www.academia.edu/33045447> [acesso em 05/11/2018].

SCHNEIER, Bruce, **Applied cryptography** (2nd edition), John Wiley & Sons, New York, 1996.

SCHNEIER, Bruce, **Designing Voting Machines to Minimize Coercion**. Disponível em: <https://www.schneier.com/crypto-gram-0707.html#8> [acesso em 05/12/2017].

SCHNEIER, Bruce, **Voting and technology**. Disponível em: <https://www.schneier.com/crypto-gram-0012.html#1> [acesso em 05/12/2017].

SCHNEIER, Bruce. **Internet Voting vs. Large-Value e-Commerce**. Disponível em: <https://www.schneier.com/crypto-gram-0102.html#10> [acesso em 05/12/2017].

SEEDORF, Sebastian. **Germany: The Public Nature of Elections and its Consequences for E-Voting**. In: MAURER, Ardita Driza; BARRAT, Jordi (Organizers). E-Voting Case Law. Surrey: Ashgate Publishing, 2015.

STEINGRABER, Ronivaldo; SIGNOR, Diogo; SILVA, Elder Mauricio. What is needed to change the result of an election: an analysis with agent-based models. Revista Brasileira de Estudos Políticos, v. 116, 2018. Disponível em <https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/581> [acesso em 05/11/2018].

VOGEL, Luiz Henrique. **A segurança do voto eletrônico e as propostas de fiscalização da apuração pela sociedade**, 2011. Brasília: Câmara dos Deputados – Consultoria Legislativa. Disponível em: <http://bd.camara.leg.br/bd/bitstream/handle/bdcamara/5945/seguranca_voto_vogel.pdf?sequence=3> [acesso em 05/12/2017].

Recebido em 06/02/2018.

Aprovado em 20/09/2018.

Augusto Tavares Rosa Marcacini
E-mail: amarcacini@gmail.com

Irineu Francisco Barreto Junior
E-mail: neubarreto@hotmail.com