DOI: 10.5335/rbca.v11i2.9056

Revista Brasileira de Computação Aplicada, Julho, 2019

DOI: 10.5335/rbca.v11i2.9056
Vol. 11, Nº 2, pp. 1–12
Homepage: seer.upf.br/index.php/rbca/index

ISSN 2176-6649

ARTIGO ORIGINAL

Urnas Eletrônicas no Brasil: linha do tempo, evolução e falhas e desafios de segurança

Isadora Garcia Ferrão[1], João Otávio Chervinski[1], Sherlon Almeida da Silva[1], Diego Kreutz[1], Roger Immich[2], Fábio Kepler[3] and Rodrigo da Rosa Righi[4]

[1]Laboratório de Estudos Avançados (LEA), Universidade Federal do Pampa (UNIPAMPA) and [2]Instituto de Computação (IC), Universidade Estadual de Campinas (UNICAMP) and [3]Grupo de Inteligência Artificial, Unbabel and [4]Programa Interdisciplinar de Pós-Graduação em Computação Aplicada (PIPCA), Universidade do Vale do Rio dos Sinos (UNISINOS)

*{isadoraferrao9,joaootaviors,sherlonalmeidadasilva}@gmail.com;diego.kreutz@unipampa.edu.br
†roger@ic.unicamp.br;fabio.kepler@gmail.com;rrrighi@unisinos.br

Recebido: 17/01/2019. **Revisado:** 23/04/2019. **Aceito:** 22/05/2019.

Resumo

Mesmo após anos de implantação e evolução do voto eletrônico, as urnas eletrônicas continuam sendo alvo crescente de críticas, tanto por parte de especialistas em segurança da informação quanto pela sociedade. Os principais desafios no uso desse tipo de urnas são garantir a transparência, a auditabilidade e a confiabilidade do sistema de votação, ao mesmo tempo em que garante-se também a integridade, a confidencialidade e a privacidade dos votos. No sistema brasileiro, entretanto, os principais pontos criticados são exatamente a pouca transparência e a restrita auditabilidade das urnas, que nos poucos casos em que foram concedidos à sociedade civil fora de períodos eleitorais, levaram a descobertas de falhas de segurança. Não é surpresa, portanto, que isso, somado à atual impossibilidade de se auditar os resultados eleitorais, coloque em cheque a confiabilidade no sistema. Neste survey, nós apresentamos e analisamos a evolução dos sistemas de votação eletrônica com o objetivo de criar uma linha do tempo e discutir falhas de seguranças e desafios em aberto. Também identificamos e discutimos questões importantes a serem respondidas para que um sistema baseado em urnas eletrônicas possa, de fato, ser um dos principais mecanismos de eleição de representantes em uma democracia.

Palavras-Chave: Urnas eletrônicas, linha do tempo, fraudes, segurança, transparência, democracia.

Abstract

Even after years of implementation and evolution of electronic voting, electronic ballot boxes continue to be a growing target for criticism, both by information security experts and by society. The main challenges in using this type of ballot box are to ensure the transparency, audibility, and reliability of the voting system, while also ensuring the integrity, confidentiality, and privacy of votes. In the Brazilian system, the main points criticized are exactly the lack of transparency and the limited auditability of the ballot boxes, which in the few cases in which they were granted to civil society outside electoral periods led to the discovery of security breaches. It is not surprising, therefore, that this, coupled with the current inability to audit the election results, puts in check the reliability in the system. In this survey, we present and analyze the evolution of electronic voting systems with the objective of creating a timeline and discussing security flaws and open challenges. We have also identified and discussed important questions to be answered so that an electronic ballot-based system may be one of the main mechanisms for electing representatives in a democracy.

Key words: Electronic voting machines, timeline, fraud, security, transparency, democracy.

1 Introdução

Um dos problemas enfrentados por sociedades onde os seus cidadãos participam ativamente das decisões é a adoção de métodos eficientes para formalizar e mensurar a intenção de voto dos eleitores. Atendendo a esta demanda, os métodos de votação tornam-se um recurso imprescindível para os eleitores elegerem os seus representantes nos mais diversos níveis de governos e entidades democráticas (Monteiro et al.; 2001).

Em muitos países, os métodos de votação ainda são manuais, realizados em papel, tornando os processos de votação e apuração demorados e suscetíveis a fraudes e erros humanos. Os sistemas eletrônicos de votação surgiram como uma forma de automatizar esses processos, acelerar a apuração dos votos, e mitigar o erro humano e as fraudes (Petersen and Jaecks; 2005). As fraudes, como as que ocorreram na contagem de votos no Rio de Janeiro em 1994, onde houve fraude em 80% das urnas da 25ª Zona Eleitoral colocando sob suspeita mais de 300 mil votos, são antigas e acompanham as eleições no Brasil desde século XIX (Ricci and Porto Zulini; 2014).

Os sistemas eleitorais baseados em urnas eletrônicas e um cadastro nacional único permitem armazenar os votos dos eleitores de maneira distribuída, e.g. por seção eleitoral, e tornam viável uma apuração centralizada, sem intervenção humana, e rápida quando comparada ao método manual. De fato, a eficiência na apuração dos votos é considerada por muitos a maior vantagem das tecnologias de votação eletrônica (Wang et al.; 2017). Na prática, o uso dessas tecnologias facilita, também, o processo de eleição e apuração em locais de difícil acesso, como aldeias indígenas remotas, cujos dados podem ser transmitidos via satélite para contabilização e integralização.

Apesar dos benefícios, a tecnologia das urnas eletrônicas é alvo recorrente de críticas e ataques que têm por objetivo desvirtuar (ou tornar sem credibilidade) o sistema de votação. No primeiro caso, muitas pessoas não confiam no processo eletrônico, seja por falta de transparência ou pela falta de mecanismos de auditoria, e sugerem a evolução do sistema ou a volta do modelo tradicional, baseado exclusivamente em papel. Já no segundo caso, há suspeitas de governos, partidos e outras instituições que tentam tirar proveito das fragilidades do sistema eletrônico de votação em benefício próprio, ou seja, para manter a influência ou o controle de um estado através da manipulação de parte dos votos.

No Brasil, as urnas eletrônicas são utilizadas para votação de cargos municipais, estaduais e federais (de Freitas[1] and Macadar; 2017). Outros países também realizam processos de votação utilizando urnas eletrônicas, como é o caso de Suíça, Canadá, Austrália, Estados Unidos (em alguns estados), México, Peru, Venezuela, Japão, Coréia do Sul e Índia. A Índia utiliza urnas eletrônicas similares às brasileiras, mas adaptadas à sua realidade eleitoral (TSE; 2014a). O Brasil, contudo, é o único país a possuir quase que uma totalidade de votos pelo meio eletrônico.

As primeiras urnas começaram a operar no Brasil há 22 anos, em 1996. O objetivo original foi mitigar fraudes na contagem de votos e automatizar e agilizar o processo de votação e apuração. Entretanto, atualmente as urnas eletrônicas estão sendo recorrentemente questionadas em diferentes países do mundo. Os principais problemas e desafios estão relacionados à transparência, confiabilidade e segurança do processo como um todo. Como evidência, as auditorias realizadas nas urnas eletrônicas do Brasil nos últimos anos, apesar de limitadas, revelaram problemas de segurança graves, como armazenamento inseguro de chaves criptográficas, vulnerabilidades de injeção de código em bibliotecas do sistema, auto-verificação do software da urna e quebra de integridade e privacidade dos votos dos eleitores (Brunazo and Amílcar; 1999; Rodrigues-Filho et al.; 2006; Aranha et al.; 2012, 2013, 2018, 2016; Gibson et al.; 2016; Ferreira; 2013; Mari; 2014). Embora a detecção de tais falhas seja preferível a ter-se total ignorância de sua existência, a situação é invertida e torna-se preocupante porque, até o momento, levando em conta a nossa extensa pesquisa e conhecimento, não há esclarecimentos nem garantias de que essas falhas tenham sido o resultado de um processo técnico deficitário e não ações mal intencionadas.

Dado esse cenário atual, os principais objetivos deste survey são analisar a evolução das urnas eletrônicas no Brasil, mapear e discutir falhas de segurança existentes e potenciais, e apresentar questões que devem ser respondidas para que o processo de votação seja considerado mais transparente e confiável. As principais contribuições são:

(c_1) um resumo, na forma de linha do tempo, da história das urnas eletrônicas no Brasil;
(c_2) a identificação e discussão das falhas de segurança reportadas por especialistas; e
(c_3) uma discussão sobre questões e caminhos futuros para melhorar a qualidade das urnas e dar maior credibilidade ao processo de votação eletrônica como um todo.

O restante deste texto está organizado como segue. Na Seção 2 apresentamos a metodologia utilizada para atingir os objetivos deste trabalho. Na Seção 3 apresentamos uma linha do tempo que mostra a evolução das urnas eletrônicas no Brasil. Na Seção 4 discutimos os mecanismos e os problemas de segurança, e lançamos questões a serem investigadas. Finalmente, na Seção 5, tecemos as últimas considerações.

2 Metodologia

A metodologia adotada neste trabalho para atingir os objetivos propostos pode ser descrita em três etapas. Na primeira etapa foram definidas as palavras-chave que contemplam o escopo da pesquisa (urnas e sistemas de votação eletrônicos), como:

(p_1) urnas;
(p_2) urnas eletrônicas;
(p_3) urnas eletrônicas no Brasil;
(p_4) segurança das urnas eletrônicas;
(p_5) sistemas de votação;
(p_6) sistemas de votação eletrônica;
(p_7) e-Voting; e

(p_8) e-Voting Brazil.

Numa segunda etapa, as palavras-chave foram utilizadas em sistemas de busca como o Google Scholar (https://scholar.google.com.br/), o Google Search (https://www.google.com.br/), o DuckDuckGo (https://duckduckgo.com) e o Bing (https://www.bing.com). A partir dos resultados das máquinas de busca, foram selecionados os trabalhos relacionados com o escopo desta pesquisa. O esquema metodológico para escolha dos trabalhos tem como base duas questões de pesquisa, que são: *Quais são os trabalhos publicados que abordam o tema urnas eletrônicas?* e *Quais são os trabalhos publicados que envolvem questões de segurança nas urnas na prática?* Os resultados das buscas foram analisados e selecionados manualmente.

3 História e evolução das urnas eletrônicas

Esta seção apresenta alguns dos fatos mais marcantes da história e evolução das urnas eletrônicas. O ponto de partida, que levou ao sistema eletrônico de votação, é introduzido na Seção 3.1. Uma linha do tempo das urnas eletrônicas é apresentada na Seção 3.2. Complementarmente, na Seção 3.3 são resumidas as principais evoluções de software e hardware das urnas atuais.

3.1 Registro nacional: o começo de tudo

Até a década de 80 não havia nenhum registro nacional dos eleitores, dando margem para fraudes graves (e.g. no cadastro de eleitores) nas eleições (TSE; 2014a). Em 1985 foram consolidados os cadastros únicos e automatizados dos cerca de 70 milhões de eleitores. Este foi o início de uma nova era para o sistema de votação brasileiro.

Um dos momentos mais marcantes, e de certa forma decisivo para a mudança de votação em papel para voto eletrônico, foram as fraudes generalizadas nas eleições do Rio de Janeiro de 1994. O problema foi tão grave que o Tribunal Eleitoral teve que anular os resultados e realizar uma nova eleição. Naquela época, os eleitores votavam utilizando boletins de voto e a contagem era manual. No momento da contagem, um responsável lia em voz alta o conteúdo da cédula, seguido pela contabilidade do voto. A fraude ocorreu na contagem dos votos.

Depois do incidente de 1994, no início de 1995, o Tribunal Superior Eleitoral (TSE) nomeou uma comissão formada por desembargadores, juristas e funcionários da Justiça Eleitoral para definir como deveria ser realizada a coleta automatizada e informatizada de votos. Um dos principais objetivos era mitigar as fraudes no processo eleitoral. Foi assim que nasceram as urnas e a votação eletrônica. Como ponto de partida, o grupo de especialistas considerou a criação de um pequeno computador que fosse capaz de processar os votos eletronicamente de forma rápida e segura (Camarão; 1997). O resultado dos trabalhos da comissão foi um projeto de lei que estabelece e define o voto eletrônico. O projeto transformou-se na Lei 9.100 de 29 de setembro de 1995.

O primeiro impacto da mudança no processo eleitoral foi o modo de votar. Antes de 1996, os eleitores votavam escrevendo o nome do candidato. Desde então, um dos objetivos do TSE passou a ser a construção de uma urna eletrônica, mais especificamente um equipamento, similar a um computador, com tela, teclado e CPU num mesmo bloco e mecanismos de segurança lógica e física. Outras características essenciais, que deveriam ser levadas em consideração no projeto das urnas, são a fácil interação com os votantes e ser totalmente lacrada, impedindo o acesso às memórias internas do equipamento. Além disso, ao invés de um teclado com várias opções, esperava-se algo mais simples, objetivo e inclusivo (e.g. algo capaz de viabilizar o voto de analfabetos e deficientes visuais). O teclado é a interface com o usuário (cidadão votante), onde são digitados os números dos candidatos de cada eleitor.

O grupo técnico definido para a construção da primeira urna foi composto por três engenheiros do Instituto Nacional de Pesquisas Espaciais (INPE), um do Exército, um da Aeronáutica (Departamento de Ciência e Tecnologia Aeroespacial – DCTA), um da Marinha e um do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD). As urnas eletrônicas foram desenvolvidas entre 1995 e 1996, e aperfeiçoadas em 1997 para o modelo que se tornou o padrão brasileiro.

A transição do processo eleitoral em papel para urnas eletrônicas exigiu um esforço publicitário muito grande do governo. O TSE teve que realizar várias campanhas publicitárias no Brasil, incluindo programas de TV, artigos em jornais, revistas e anúncios em rádios, além de apresentações expondo o sistema eletrônico em sindicatos, escolas, rodoviárias, aeroportos, praças, feiras, entre outros locais (de Freitas[1] and Macadar; 2017).

Na verdade, as campanhas publicitárias continuam até hoje. Em outubro de 2018, poucos dias antes das eleições de primeiro turno, a própria ministra do TSE reforçou que as urnas são seguras segundo a perspectiva do TSE. Após o primeiro turno, as campanhas do TSE tiveram que ser intensificadas para evitar ações organizadas por parte da população com relação à falta de confiança e transparência no processo de votação utilizando as urnas eletrônicas.

Na prática, sob o ponto de vista técnico de sistemas e segurança da informação, sabe-se que não há provas concretas de que as urnas eletrônicas sejam, de fato, seguras e confiáveis. Ao contrário, há um grande receio por parte de especialistas em segurança da informação e de boa parte da população com relação a confiabilidade das urnas.

3.2 Linha do tempo das urnas eletrônicas

A votação no Brasil passou por várias etapas e modificações ao longo dos anos. Já foram utilizadas urnas de vários materiais, desde madeira, metal, lona, até chegar às urnas eletrônicas utilizadas atualmente (Cajado et al.; 2014).

O sistema de votação brasileiro pode ser dividido em duas fases, votação em papel e votação eletrônica. Alguns dos acontecimentos mais marcantes na transição das urnas em papel para as urnas eletrônicas são descritas nesta seção.

Em 1996 houve a primeira eleição informatizada

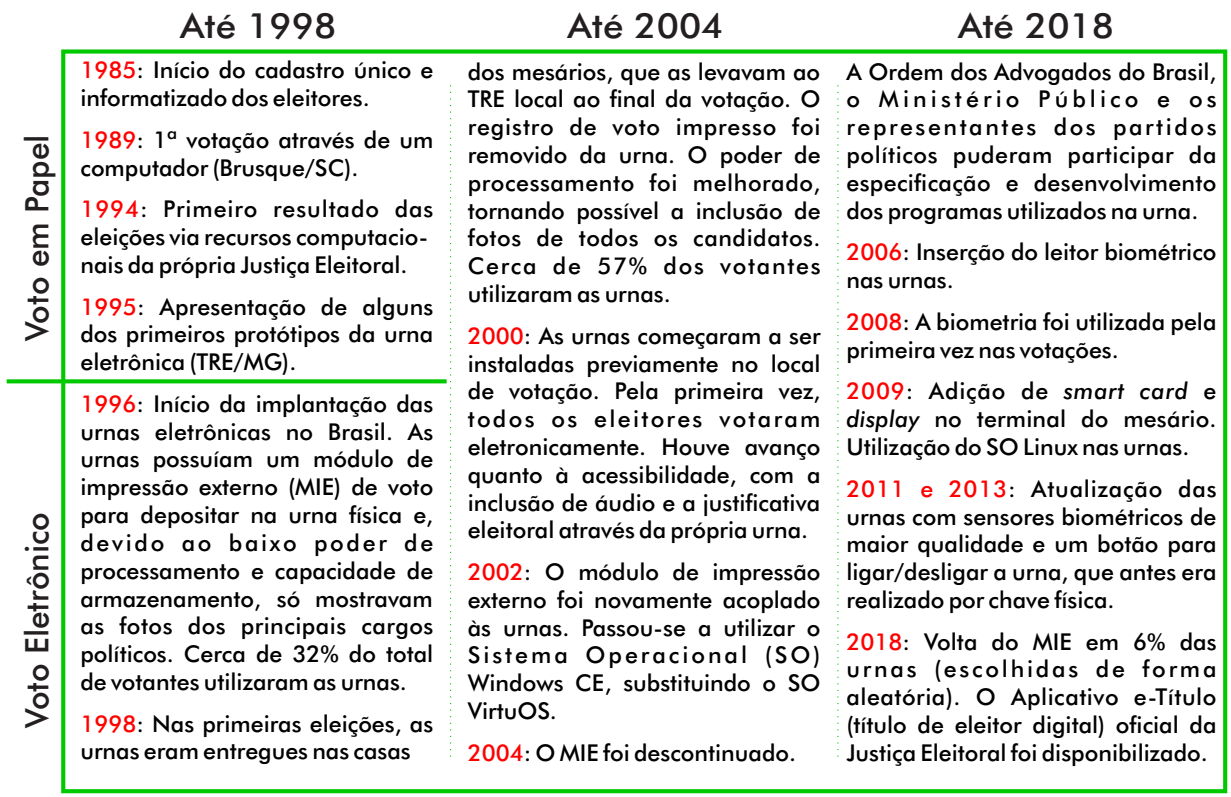

Figura 1: Linha do tempo das urnas eletrônicas no Brasil

no Brasil, totalizando mais de 32 milhões de eleitores brasileiros com os votos coletados e totalizados por meio de mais de 70 mil urnas eletrônicas. Naquela primeira etapa de utilização da urna eletrônica em larga escala, participaram 57 cidades com mais de 200 mil eleitores (Barbosa; 2014). As urnas foram distribuídas com o auxílio de aviões da FAB (Força Aérea Brasileira).

No dia 29 de setembro de 1996, à uma semana do primeiro turno, o então presidente do TSE, ministro Marco Aurélio, afirmou que a justiça eleitoral tinha razões para acreditar que o eleitor não teria dificuldades na hora de votar utilizando as urnas eletrônicas. A máquina desenvolvida era muito simples e havia sido submetida a exaustivos testes (TSE; 2014a).

Até as eleições de 1998/2000, algumas urnas, em algumas regiões eleitorais, eram entregues nas casas dos mesários, sendo que cada mesário era encarregado de levar a urna para o local onde ocorreria o processo eleitoral, conforme indicado pelo respectivo TRE. Isto, obviamente, potencializava o número de problemas, como comprometimento de urnas e votações, uma vez que a confiança residia agora, também, sobre os milhares de mesários.

Em 2000 o TSE articulou um período de testes para que os brasileiros aprendessem a utilizar a urna eletrônica (Klumb and Hoffmann; 2016). Todas as urnas, 186.800 fabricadas naquele ano e mais 168 mil urnas usadas na eleição anterior, foram disponibilizadas para o treinamento em TREs de todo o país.

A primeira eleição totalmente informatizada ocorreu em 2000, quando as urnas eletrônicas estavam sendo distribuídas em todo o país. Desde então, a Justiça Eleitoral vem melhorando e ampliando o parque de urnas eletrônicas para atender o crescente número de eleitores (Andrade; 2015).

O número de urnas, desde a primeira eleição em 1996, vem crescendo com o passar do tempo. Em 1996 e 2000 haviam aproximadamente 70.000 e 350.000 urnas, respectivamente. Segundo engenheiro especializado em segurança de dados, Prof. Amilcar Brunazo Filho, em uma audiência pública realizada pela Comissão de Constituição, Justiça e Cidadania, em março de 2018, hoje existem em torno de 600.000 urnas eletrônicas (Martins; 2018a,b; Agência Senado; 2018). A Figura 1 resume a linha do tempo da transição das urnas em papel para as urnas eletrônicas.

3.3 Evolução do software e hardware

Paralelo à história da votação eletrônica, há também a evolução tecnológica dos componentes de hardware e software das urnas. Como pode ser observado na Figura 2, as urnas passaram por diferentes ciclos evolutivos. De 1996 a 2013, houveram pelo menos nove atualizações técnicas de componentes como (1) processador/CPU, (2) memória, (3) armazenamento, (4) sistema operacional e (5) medidas. O objetivo principal das evoluções de hardware e software é oferecer uma solução mais robusta e completa possível.

Em 1998, 2004 e 2009 houveram atualizações arquiteturais significativas, onde as urnas passaram por mudanças de hardware em termos de CPU (80386SX, Cyrix, Geode, Intel ATOM) e outros

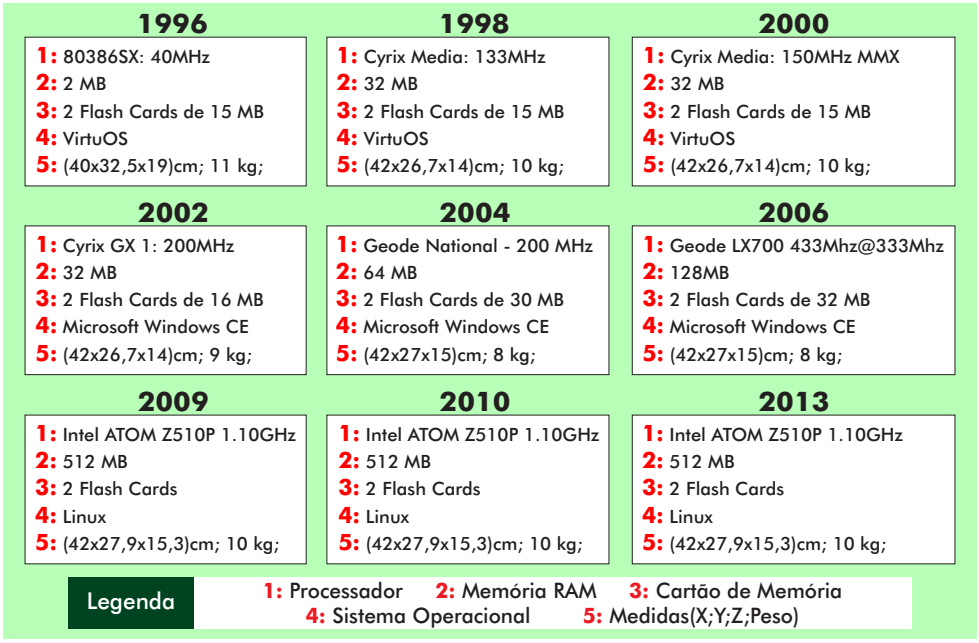

Figura 2: Evolução do hardware e software das urnas eletrônicas no Brasil

componentes. Atualmente são utilizados *flash cards* (cartões de armazenamento) com memória de 512MB, mas já foram utilizados modelos com capacidades inferiores. Assim como qualquer computador, as urnas necessitam de dispositivos para armazenamento de dados. Os *flash cards* são utilizados para leitura e gravação de dados, como armazenamento do sistema operacional, componentes de software, dados de candidatos, eleitores e da seção eleitoral da urna. Conforme o número de votantes por seção eleitoral aumenta e os programas são atualizados, as tecnologias de hardware também necessitam de atualização para dar conta das demandas de armazenamento e processamento, por exemplo.

O modelo mais recente das urnas eletrônicas utiliza o processador Atom de 1,10 GHz, fabricado pela Intel, e a placa-mãe Ubiqconn (Andrade; 2015). O terminal de votação tem também um display LCD de 10,1 para permitir a visualização de votos.

Em 2002, o TSE iniciou a substituição do sistema operacional original (VirtuOS) pelo Microsoft Windows CE. Sete anos depois, em 2009, os sistemas operacionais de todas as urnas eletrônicas foram migrados para o Linux, agora com suporte da equipe técnica do próprio TSE. A mudança teve três objetivos essenciais, promover a unificação dos sistemas usados nas urnas, reduzir custos, e contribuir para a auditabilidade do código-fonte das urnas (Macedo; 2018; Extra; 2007). Na Seção 4.1 são apresentadas e discutidas algumas questões de segurança envolvidas nessa migração de sistema operacional.

Vale ressaltar que há um custo significativo ao erário público no que diz respeito a fabricação e/ou atualização das urnas. Como exemplo, até 2009 havia um custo aproximado de 100 dólares por urna em licenças de sistemas operacionais. Com a migração para Linux, a economia estimada na época, até 2019 Macedo (2018) (i.e. considerando um período de 10 anos), ficou em 15 milhões de reais devido ao uso de novos programas. Entretanto, considerando que hoje existem 600 mil urnas, a economia bruta em licenças de sistema operacional representa um montante aproximado de 60 milhões de dólares. Isto demonstra que uma simples decisão técnica pode representar um montante expressivo ao erário público.

Em 2018, para a implantação do voto impresso nas eleições, o custo foi estimado em 1,8 bilhão de reais pelo TSE (Lellis; 2018). Segundo Pedro Dourado de Rezende, Prof. de Ciência da Computação da Universidade de Brasília (UnB), em uma audiência pública realizada pela Comissão de Constituição, Justiça e Cidadania, em março de 2018, o TSE firmou um contrato, sem licitação, de 7 milhões de reais com uma entidade sem fins lucrativos, chamada Flextronics, para produzir um modelo de votação eletrônica com voto impresso (Martins; 2018a,b; Agência Senado; 2018). O resultado foi uma urna que imprime votos ao preço de R$ 3.700,00. Segundo Prof. Pedro, um desperdício totalmente desnecessário uma vez que o software das urnas atuais já está preparado para dialogar com uma impressora (e.g. as urnas já imprimem o boletim de urna), sendo desnecessária a contratação de uma empresa para desenvolver toda uma replicação do sistema na urna a pretesto de precisar imprimir o voto. Novamente, este é mais um exemplo claro de como decisões técnicas, por vezes precipitadas ou interesseiras, podem impactar negativamente o erário público.

4 Segurança nas Urnas Eletrônicas

Sistemas de votação eletrônica facilitam o processo eleitoral ao fornecerem mecanismos mais eficientes para o transporte (e.g. via dispositivos de armazenamento como cartões *flash* e *drives* USB) e a contagem dos votos. Porém, o uso de sistemas digitais também introduz um conjunto de preocupações quanto a autenticidade, integridade, confidencialidade e confiabilidade dos votos

contabilizados. Isso deve-se principalmente à falta de transparência no sistema e falta de mecanismos efetivos que permitam à sociedade realizar auditorias no processo de votação. Estudos anteriores indicam que aspectos como transparência do processo e dos sistemas são alguns dos requisitos fundamentais de um sistema de votação eletrônica em uma democracia (Pinto et al.; 2004). As seções a seguir (4.1 e 4.2) apresentam e discutem questões relativas à segurança das urnas eletrônicas brasileiras.

4.1 Recursos e mecanismos de segurança das urnas

A urna eletrônica é um microcomputador desenvolvido e personalizado para o processo eleitoral brasileiro. Essa máquina não possui conexão com a Internet e é composta pelo terminal do mesário, onde o eleitor é identificado, e o terminal do eleitor, onde o voto é registrado. As urnas eletrônicas são projetadas para funcionar mesmo no caso de falta de energia elétrica, evitando assim a interrupção do processo de votação e/ou a eventual perda de dados. A bateria interna das urnas proporciona uma autonomia de cerca de 12 horas (TSE; 2013).

Os dados do processo de votação são armazenados em cartões de memória *flash* e podem ser transferidos de uma urna para outra, tornando possível a substituição de equipamentos em caso de falhas técnicas. A urna utiliza dois cartões, denominados *flash card* interno e *flash card* externo. O cartão interno é utilizado para armazenar o sistema operacional das urnas, os dados de aplicações e dados relativos à eleição, como informações dos candidatos e dos eleitores. O cartão externo pode ser usado como *backup* dos dados do cartão interno, podendo ser utilizado em caso de defeito na urna, ou como *flash* de carga, isto é, ser utilizado para instalar as aplicações que a urna necessita durante uma eleição.

O teclado das urnas é composto por teclas numéricas de 0 à 9 e mais três teclas, a tecla "Confirma" para confirmar e gravar o voto, a tecla "Corrige" para apagar os números já digitados no campo de entrada atual e a tecla "Branco" para abdicar do voto para o cargo em questão. Desde a primeira versão das urnas, datada de 1996, todas as teclas possuem um código em braile que indica a sua função. Em 2000 as urnas passaram a contar também com um sistema de áudio que permite a utilização de fones auriculares, com o objetivo de tornar o processo de votação ainda mais acessível à pessoas portadoras de deficiências (TSE; 2014b).

O teclado de votação é automaticamente desabilitado quando os circuitos internos detectam a conexão de um teclado externo na parte traseira da urna. O uso de teclados externos é necessário para a realização de testes e manutenção antes da distribuição das urnas. Entretanto, o uso desses teclados é barrado através do uso de lacres físicos de segurança (Dufloth et al.; 2014). Caso o lacre de segurança de uma urna seja violado, o aparelho deverá passar por um processo de auditoria.

No que diz respeito à algoritmos criptográficos, são utilizados o Message Digest 5 (MD5) e o Assina para garantir a integridade e autenticidade dos dados. O MD5 é uma função de *hash* criptográfica que fornece um resumo criptográfico, ou *digest*, de 128 bits a partir de um conjunto de dados de tamanho arbitrário (Dufloth et al.; 2014). O algoritmo MD5 é utilizado para gerar um resumo criptográfico para cada um dos arquivos da árvore de diretórios da aplicação de votação. Os nomes dos arquivos e os seus devidos resumos são gravados, um por linha, num arquivo com extensão .CRC. O algoritmo Assina é utilizado para fornecer uma camada extra de segurança ao computar um resumo criptográfico de 256 bits dos *digests* gerados pelo MD5, com o objetivo de fornecer garantias adicionais de integridade e autenticidade dos votos.

Todas as urnas eletrônicas compartilham uma mesma chave criptográfica para cifrar os conteúdos das mídias. Segundo relatado pelo professor Dr. Diego de Freitas Aranha, da Universidade Estadual de Campinas (UNICAMP), em uma audiência pública realizada pela Comissão de Constituição, Justiça e Cidadania, em março de 2018, a chave que é utilizada no procedimento de cifragem está declarada em texto plano no código-fonte da urna eletrônica (Aranha; 2018; Martins; 2018a; Aranha et al.; 2018). Um representante do TSE afirma que o órgão alterou o método de armazenamento das chaves, e que elas são agora armazenadas em hardware e lidas para a memória principal quando o sistema das urnas está em execução (Casado; 2018). Como estratégia única de proteção do sigilo do voto, as urnas eletrônicas armazenam os votos registrados em uma tabela chamada de Registro Digital do Voto (RDV). O RDV embaralha a ordem dos votos para desassociar a ordem de inserção e a ordem de armazenamento dos votos.

As urnas eletrônicas utilizaram de 1996 à 2000 o sistema operacional VirtuOS, que foi desenvolvido no Brasil por uma empresa chamada MICROBASE e que oferece funcionalidades similares ao MS-DOS (Dufloth et al.; 2014). O VirtuOS oferece recursos como processamento concorrente utilizando *threads*, que são utilizadas para garantir otimização nas urnas durante o processo eleitoral. Em 2002, 2004 e 2006 algumas urnas passaram a utilizar o sistema operacional Windows CE, desenvolvido com foco em sistemas embarcados, o que gerou controvérsias devido aos gastos com a aquisição de licenças e a dificuldade de inspeção do código do sistema, que é proprietário. Outra preocupação foi a possibilidade de fraude através da utilização de arquivos .dll (*Dynamic-link Library*) alterados para a realização de operações maliciosas.

No quesito de software e aplicações, a urna eletrônica possui o que é chamado pelo TSE de 'Ecossistema da Urna', que consiste em um conjunto de 28 aplicativos que automatizam as tarefas necessárias para o funcionamento do aparelho. Eis alguns exemplos de aplicativos, que vale a pena destacar:

(a_1) **Sistema Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica**: responsável por gerar as mídias de instalação e de votação;
(a_2) **Sistema de Carga de Urna Eletrônica**: permite instalar o sistema operacional, software e dados de eleições nas urnas;
(a_3) **Sistema de Auto-teste da Urna Eletrônica**: verifica o funcionamento dos componentes da

urna;

(a_4) **Sistema Vota**: apura os resultados da seção eleitoral; e

(a_5) sistema que, no momento da inicialização das urnas eletrônicas, verifica se os programas nela instalados foram assinados digitalmente pelo TSE.

Como mencionado na Seção 3.2, em 2008 ocorreu uma migração dos sistemas de todas as urnas eletrônicas para um ambiente de software baseado em Linux. Além das questões de redução de custos, a atualização também foi motivada pelo aspecto da segurança e da transparência das urnas, uma vez que os especialistas sugerem a adoção de software livre. Como princípio, o software livre tem seu código aberto, logo, quanto mais pessoas tem acesso ao código, maiores são as chances de erros serem detectados (SBPC; 2002) e de aumentar significativamente a robustez do software em termos de confiabilidade e segurança (Wheeler; 2015).

4.2 Vulnerabilidades nas urnas eletrônicas

Durante as suas mais de duas décadas de existência, as urnas eletrônicas já foram submetidas à diferentes processos de aprimoramento ou atualização com o objetivo de melhorar a sua usabilidade e segurança. Existem, porém, mecanismos de segurança presentes nas urnas que utilizam tecnologias ultrapassadas ou estratégias ineficazes frente à capacidade de um atacante dado o cenário atual da tecnologia. Nesta seção são apresentadas e discutidas vulnerabilidades descobertas e corrigidas, vulnerabilidades existentes, possíveis vetores de ataque que podem ser explorados por um agente malicioso para interferir nos resultados das eleições e, por fim, aspectos que podem ser melhorados para aumentar a transparência e confiabilidade do sistema de votação como um todo, o que é essencial em uma democracia.

Para o restante desta subseção, considere como agente externo uma pessoa que interage com a urna eletrônica, mas não tem participação em nenhum órgão que regula as urnas e nem nas etapas do processo de programação e construção do equipamento. Diferentemente, considere como agente interno uma pessoa que possui acesso privilegiado ao processo de programação ou construção das urnas eletrônicas, isto é, capaz de interferir no projeto do hardware ou software da urna.

4.2.1 *Ameaças e vulnerabilidades corrigidas*

Acesso físico às urnas. Nas primeiras eleições, as urnas eletrônicas eram entregues para os mesários em suas casas, que ficavam encarregados de levá-las aos respectivos locais de votação. Essa estratégia negligenciou a possibilidade de ataques e alteração dos componentes das urnas pelos mesários, possivelmente devido ao fato do conhecimento técnico sobre computadores na época não ser tão difundido quanto atualmente. Um agravante foi o fato do ocorrido ter acontecido em um período introdutório das urnas eletrônicas, onde modificações nos aparelhos possuíam grandes chances de passarem despercebidas pelos votantes.

Chaves presentes no código-fonte. A chave utilizada para a cifragem dos dados armazenados nas mídias da urna é armazenada em texto plano, no módulo que acessa as mídias e realiza a sua cifragem. Isso significa que esse mecanismo não oferece segurança alguma mediante ação de um agente interno que possua acesso ao código-fonte das urnas. Após inspecionar o código e descobrir a chave, um atacante obtém "a chave do reino" para ter acesso aos dados armazenados em todas as mídias de todas as urnas eletrônicas. Este problema gravíssimo de segurança, uma falha que qualquer especialista em segurança da informação evitaria a todo custo desde o primeiro protótipo de um projeto de um sistema seguro, foi aparentemente resolvido apenas em 2017/2018, ou seja, mais de duas décadas depois do nascimento da urna eletrônica ainda havia um problema de segurança crasso.

4.2.2 *Vulnerabilidades existentes*

Verificação de integridade inadequada. As urnas possuem um mecanismo que verifica a integridade do software com o objetivo de detectar qualquer alteração no sistema entre a etapa de produção e a etapa da sua execução (Aranha et al.; 2013). Todas as urnas realizam essa verificação, porém, existem urnas eletrônicas com e sem módulos de segurança em hardware para auxiliar no processo. As urnas sem módulo de segurança em hardware efetuam a verificação de si próprias no momento da inicialização do sistema. Para que esse processo seja interrompido, basta que um agente interno malicioso altere algumas das linhas de código dos programas das urnas que executam essa tarefa. Como forma de mitigar o problema, um mecanismo de segurança adicional pode ser implementado no sistema básico de entrada e saída (BIOS) para verificar a integridade do software que, posteriormente, realiza a verificação do sistema. Entretanto, o problema de garantir a verificação de integridade é simplesmente transferido do software para a BIOS, que pode também ser alterada por um agente interno malicioso.

As urnas mais modernas utilizam o módulo de segurança em hardware para verificar o conteúdo da BIOS. Neste caso, para interferir nas operações do módulo de segurança, é necessário que um agente interno da empresa fabricante do dispositivo de segurança desative a funcionalidade ou adultere as chaves contidas no dispositivo. O problema é que essas chaves podem ser alteradas de modo que sejam iguais as chaves utilizadas para assinar o software malicioso. A execução de um ataque deste tipo permitiria a execução de software malicioso nas urnas eletrônicas, potencialmente executando operações indesejadas que podem interferir nos resultados das eleições. Para evitar esse tipo de ataque são necessários testes exaustivos e minuciosos nos módulos de hardware e software. Entretanto, como o sistema é fechado e as auditorias são extremamente limitadas, torna-se quase impossível saber se algum ataque desse tipo já ocorreu ou não. Devido a estas urnas possuírem, ou já terem possuído, problemas graves de segurança, como por exemplo, uso de MD5, senhas no código-fonte, verificação de integridade através do próprio software da urna, é necessário mais do que uma declaração do TSE para garantir que as urnas são confiáveis.

Chaves presentes na memória volátil. Segundo foi informado por um representante do TSE, a chave

única para a cifragem das mídias da urna não é mais visível no código. Ela é armazenada em hardware e lida para a memória principal quando o sistema das urnas está em execução (Casado; 2018). O fato da chave ser lida somente em tempo de execução não elimina a possibilidade de ataques que possam recuperar a chave. Na prática, ataques à memória, em tempo de execução, são comuns nos dias atuais.

Um agente malicioso pode inserir no código-fonte da urna instruções que realizam uma inspeção nos dados presentes na memória principal. Com isso, o atacante consegue uma cópia da chave durante a execução do sistema e pode usar ela para decifrar os dados armazenados nas mídias da urna ou gravar ela no *flash card*. Com uma cópia da chave em mãos, o atacante pode decifrar os dados contidos nos *flash cards* de todas as urnas. Uma solução para esse problema é a utilização de tecnologias que criam partições protegidas (seguras) na memória, utilizando tecnologias como a Intel SGX (Costan and Devadas; 2016) e ARM TrustedZone (Winter; 2008). Com o suporte de tecnologias desse tipo, pode-se isolar os componentes de software que lidam com dados sensíveis das demais partes do sistema. Com isso, evita-se o vazamento de material crítico como as chaves secretas, que representam os pilares de segurança dos sistemas.

Uso de chave única para a cifragem dos dados. Todas as urnas eletrônicas utilizadas no país recebem a mesma chave criptográfica para realizarem a cifragem das mídias de armazenamento do dispositivo (TSE; 2016). Os programas cifrados incluem o software de votação e mecanismos de segurança e dados como a chave RSA utilizada para a assinatura digital do software das urnas, que pode ser usada para falsificar e assinar um software que será então aceito pelas urnas. Em resumo, a integridade dos dados gerados pelas urnas eletrônicas depende de uma única chave, compartilhada entre centenas de milhares de dispositivos. O TSE argumenta que o uso de múltiplas chaves pode permitir a execução de algum ataque estatístico que revele características do texto plano, porém, esses ataques vem sendo estudados na literatura e não apresentam perigo relevante (Aranha et al.; 2013). Ao contrário, o uso de múltiplas chaves dificultaria consideravelmente o comprometimento de todo o sistema. Hoje, um atacante precisa comprometer uma única chave, o que é factível, como discutido anteriormente, para ter acesso aos dados de todas as urnas. Na prática, grandes provedores de armazenamento seguro de dados, que precisam oferecer altos níveis de segurança aos seus clientes, como o Google BigQuery (Google Cloud; 2018), utilizam uma chave por bloco de dados, por exemplo. Isto significa que para acessar os dados de um cliente podem ser necessárias centenas de chaves, o que dificulta consideravelmente o trabalho do atacante.

Utilização de algoritmos obsoletos. As urnas eletrônicas utilizam algoritmos de *hash* e assinatura de dados Message Digest 5 (MD5) e Assina, respectivamente. Em 2004, foi demonstrado que o algoritmo MD5 é inseguro pois o mesmo não oferece a resistência à colisões que era esperada. A partir de então o seu uso foi desaconselhado, sendo fortemente recomendada a migração para funções de *hash* criptográficas mais robustas, como a SHA-256 e SHA-512. O algoritmo Assina é de propriedade do TSE, ou seja, não teve sua segurança verificada e auditada pela comunidade de segurança da informação, o que coloca em cheque a sua utilização. Recomenda-se a utilização de primitivas criptográficas estabelecidas na comunidade mundial de segurança (e.g. HMAC-SHA256), devido ao esforço conjunto que é empregado na realização de testes para a busca de vulnerabilidades nas mesmas.

Fraude dos mesários. Pessoas que participam das eleições como mesários possuem acesso ao material de registro de comparecimento às sessões eleitorais. Um mesário mal intencionado pode fraudar a assinatura de um cidadão que não compareceu à sua sessão eleitoral e realizar o voto em seu lugar. A implantação da identificação biométrica ajuda a mitigar esse problema ao liberar o processo de votação somente após a identificação da digital, porém é possível burlar o uso da identificação biométrica ao alegar falhas na identificação, sendo necessário realizar o registro em caderno físico, como ocorreu em algumas sessões eleitorais durante as eleições de 2018. Entretanto, um ataque desse gênero possui pouco impacto, pois depende do não comparecimento dos votantes e, também, parte do pressuposto que o eleitor em questão irá manter-se ignorante ao fato do recebimento de notificação caso não compareça a sessão eleitoral.

Quebra de Sigilo do Registro Digital do Voto. O RDV foi projetado para permitir que os eleitores possam realizar a verificação dos seus votos de maneira independente, contribuindo com a fiscalização dos procedimentos realizados nas eleições. O RDV armazena os votos de maneira embaralhada para evitar a associação da ordem dos votos armazenados e a ordem dos votantes em cada seção eleitoral. O problema reside no fato do RDV ser gerado pela mesma aplicação que gera o boletim de urna, que contêm o número total de votos para cada candidato em uma dada urna eletrônica. Isso significa que se o software que gera o boletim de urna for modificado, o RDV sofrerá um impacto direto, não oferecendo garantia nenhuma contra fraudes.

Existe ainda a possibilidade de quebra do sigilo do voto armazenado no RDV devido à má implementação do mecanismo de geração de números pseudo-aleatórios, que é essencial para o processo de embaralhamento de votos. Pesquisadores identificaram a utilização de um gerador de números pseudo-aleatórios inadequado dado o nível de segurança necessário em uma eleição (Aranha et al.; 2013). O gerador foi desenvolvido utilizando as funções `rand()/srand()` da linguagem de programação C, que aceita uma semente de inicialização de 32 bits, um valor considerado pequeno para os padrões atuais de segurança da informação. Além da escolha inadequada de gerador, a semente, o valor que é passado como entrada para que o gerador gere uma sequência de números pseudo-aleatória, consiste em uma leitura de tempo do sistema, utilizando a chamada de função `time()` no momento de inicialização da urna. Isto facilita o trabalho de um agente malicioso.

O que torna a situação ainda mais grave é o fato da hora de início da votação ser impressa obrigatoriamente em um documento chamado

zerésima. A impressão da zerésima é obrigatória pois serve para mostrar que a urna eletrônica ainda não possui votos registrados. Juntamente com o relatório da urna é impressa a hora local, que é o valor utilizado como semente para o embaralhamento dos votos. O conhecimento da hora impressa na zerésima permite a reprodução dos números aleatórios gerados, e, portanto, permite a identificação da ordem dos votos. Para que os votos sejam correlacionados a identidades, basta ter acesso à informações de registro de votantes.

4.2.3 *Aspectos a serem discutidos e melhorados*

A seguir são apresentadas algumas perguntas, sobre o sistema de urnas eletrônicas no Brasil, que necessitam de maior reflexão. Ao longo do texto, iremos discutir diferentes assuntos que levam a possíveis respostas a estas perguntas.

(p_1) *Quais as estratégias e mecanismos mais urgentes para melhorar a transparência, confiabilidade e auditabilidade do sistema de votação eletrônica do Brasil?*
(p_2) *Quê tipo de transformações são necessárias para simplificar e reduzir custos do sistema eleitoral brasileiro?*
(p_3) *Votação online, segura, transparente e confiável, é possível?*
(p_4) *Países como a Estônia são um exemplo em potencial a seguir?*

Negligência quanto à ação de agentes internos. Embora várias medidas sejam tomadas visando a segurança da urna eletrônica contra agentes externos, um agente interno malicioso pode possuir acesso à parte mais importante das urnas, o código-fonte. Embora representantes do TSE argumentem que é inviável que agentes internos sejam capazes de realizar fraudes (Rohr; 2012), ainda falta transparência nas medidas tomadas pelo TSE para prevenir a ação maliciosa de agentes internos. Vale ressaltar também que, segundo relatórios especializados, mais de 50% dos incidentes de segurança são causadas por agentes internos (Cybersecurity Insiders; 2018; IBM Security; 2018; Gogan; 2017).

Ausência de auditoria do processo eleitoral. Alguns especialistas em Tecnologia da Informação apontam que uma das fraquezas das urnas eletrônicas é a ausência de auditoria, onde sem a representação material do voto é impossível auditar os resultados eleitorais (Dufloth et al.; 2014; de Freitas[1] and Macadar; 2017; Aranha et al.; 2018; Aranha; 2018). Desta forma, é fácil afirmar, de maneira leviana, que a urna eletrônica completa 22 anos sem registro de fraudes (GaúchaZH; 2018). Portanto, como uma maneira adicional de verificar a credibilidade dos votos nas urnas eletrônicas, foi proposta, por especialistas em urnas eletrônicas como o professor e pesquisador Diego de Freitas Aranha, a adoção do uso da impressão de votos nas eleições.

A adoção dos votos impressos pode ser visualizado sob duas perspectivas. De um lado, segundo especialistas, a impressão de uma porcentagem dos votos já seria um avanço à democracia, pois isto contribuiria para a auditoria nas seções eleitorais ao comparar o número de votos em papel com o número de votos registrados nas urnas e permitir que o eleitor visualize como seu voto foi registrado no equipamento. Por outro lado, o STF suspendeu a adoção dos votos impressos nas eleições sob a afirmação de que isto apresentaria um retrocesso para o processo eleitoral. Um dos argumentos é que impressão do voto pode contribuir para a ocorrência de votos de cabresto (manipulação e compra de votos). Para resolver o impasse, o voto impresso poderia ser depositado em urna anexa ao sistema de votação. Entretanto, mesmo assim, é difícil garantir que o votante irá efetivamente depositar o seu voto na urna física. Uma solução simples seria adicionar um QR Code único no verso do voto. Este QR Code pode, então, ser facilmente lido e validado pela urna anexa, que armazena a cópia física dos votos dos eleitores. Neste caso, o processo de votação termina apenas com o sinal sonoro da urna anexa, confirmando o depósito do voto físico por parte do eleitor. Outra solução seria a urna eletrônica imprimir e depositar automaticamente os votos do eleitor na urna anexa. Neste caso, o eleitor teria apenas alguns segundos para visualizar e confirmar o seu voto impresso.

Atualmente, sem um meio de comprovar que os resultados gerados pelo software estão corretos e não foram adulterados, só resta aos eleitores confiar, sem o respaldo técnico necessário, no funcionamento das urnas. Esses fatores influenciam negativamente na transparência do processo eleitoral.

Ausência de auditoria do código-fonte. Outro aspecto frágil das urnas é o código-fonte. A credibilidade das urnas é colocada em dúvida a cada eleição. Disponibilizar o código-fonte para a comunidade facilitaria o trabalho de especialistas e contribuiria para a transparência e evolução do sistema de votação eletrônico. Apenas em 2018 o TSE ponderou a opção de disponibilizar o código-fonte das urnas entre as eleições de 2020 e 2022. Por hora, o TSE avalia questões legais, pois algumas partes do código foram implementadas por empresas privadas e, possivelmente, não serão liberadas. Entretanto, vale ressaltar que o código-fonte das urnas eletrônicas foi produzido às custas do erário público. Como tal, os contratos de desenvolvimento deveriam incluir cláusulas contratuais explicitas que permitem ao governo federal realizar o que bem entender com o código, como publicá-lo em domínio público (e.g. no portal do Software Público Brasileiro https://softwarepublico.gov.br).

A utilização de um software cujo código-fonte é aberto e público é um requisito básico de segurança, transparência e democracia. Como já foi demonstrado várias vezes na prática, um código que pode ser inspecionado por todos é menos sujeito à falhas (e.g. Linux (https://www.linux.org/), OpenSSL (https://www.openssl.org/), Apache (https://www.apache.org/)). Além disso, as eventuais falhas podem ser identificadas e corrigidas por milhões de usuários, o que trás agilidade ao processo.

Tamanho e complexidade demasiada do código-fonte. O código empregado na realização de eleições no Brasil é composto de milhões de linhas. Essa quantia de informações por si só inviabiliza uma auditoria completa do código-fonte das urnas. Uma grande parte dessas linhas de código são provenientes de componentes do sistema operacional, que normalmente não necessitariam de auditoria, porém, o TSE realiza modificações em componentes

do sistema operacional para adicionar informações sobre os módulos da urna (Aranha et al.; 2013). A prática de alterar o código do sistema operacional pode acabar introduzindo novas vulnerabilidades em componentes essenciais do sistema. Uma solução ideal deveria prezar pela redução da quantidade de linhas de código através da criação de componentes reutilizáveis, entre outras boas práticas de engenharia de software.

Os boletins de urna são inócuos na verificação da contabilização dos votos. Os boletins de urna, também conhecidos como BUs, são um instrumento que servem para auditoria de uma etapa apenas do processo de votação, que é o de totalização dos votos. O boletim da urna pode apenas fazer a verificação de que a totalização está correta. Entretanto, os BUs não tem nenhum efeito para verificar se o software da urna está contabilizando os votos corretamente.

Os testes de votação paralela são inefetivos. A verificação paralela, realizada pelo TSE, também denominada de auditoria, não tem efeito nenhum como teste de segurança sobre um software malicioso (Martins; 2018a). Um software malicioso tem formas simples e práticas de verificar se é uma eleição verdadeira ou uma eleição paralela, de auditoria. Por exemplo, com a identificação biométrica[1], no teste paralelo, durante o dia da eleição, a identificação biométrica dos eleitores vai falhar em 100% dos casos, algo fácil de ser detectado em um software malicioso, alterando o comportamento do mesmo no teste de votação paralela. Vale ressaltar ainda que um software malicioso, após alterar a contabilização dos votos da urna, pode apagar todo e qualquer rastro de execução, incluindo trechos de seu próprio código.

Avaliar melhor alternativas e exemplos externos. Outros países, como a Estônia, um dos países mais avançados em termos de identidade e sociedade digital, os eleitores podem votar online (Carpanez; 2018). Em outubro de 2017, aproximadamente 30% da população estoniana votou online, seja via computador ou celular. Um sistema de votação online é incomparavelmente mais econômico e prático que um sistema baseado em urnas eletrônicas. Claro que não é possível comparar as duas realidades distantes, pois a Estônia é um país vanguarda em termos de identidade e vida digital, simplificada e desburocratizada. Partindo deste exemplo, podemos elencar diferentes questões. *Como a Estônia chegou a esse ponto? O voto online naquele país é transparente, seguro e auditável? O exemplo da Estônia poderia, eventualmente, servir para o Brasil? O sistema da Estônia é, de fato, robusto? Quantos ataques o sistema da Estônia já sofreu?* Segundo especialistas, há diferentes tipos de vulnerabilidades e potenciais problemas de segurança com o sistema da Estônia (Springall et al.; 2014; Arthur; 2014). E, de fato, nos últimos anos ocorreram incidentes graves de segurança relacionados a uma grande gama de vulnerabilidades criptográficas no sistema de identificação digital dos e-cidadãos, o que afeta diretamente sistemas como o das eleições (Leyden; 2017; Aasmae; 2018). A substituição de um modelo de votação através das urnas eletrônicas por um modelo de votação online não significa a erradicação de todos problemas do processo eleitoral. Embora um sistema online torne o processo eleitoral mais prático, os sistemas de votação ficam vulneráveis à ataques e intervenções maliciosas. É necessário avaliar se os benefícios trazidos pela votação online justificam a adoção de um sistema que potencialmente possui mais fragilidades em termos de segurança. Enfim, são questões pertinentes e que podem contribuir com o desenvolvimento de um sistema de votação eletrônica que efetivamente atenda os preceitos mais básicos de uma democracia. Em outras palavras, não podemos confiar, às cegas, num sistema criado e imposto por uma única entidade governamental. Para responder a estas questões, faz-se necessária uma discussão, a nível técnico, com especialistas da Estônia, responsáveis pelo sistema de votação, por exemplo.

[1]Nas eleições de 2018, aproximadamente 50% dos 147 milhões de eleitores vão utilizar identificação biométrica para se identificar na hora de votar (Jornal Nacional; 2018).

5 Considerações Finais

As urnas eletrônicas, cuja história e evolução é apresentada na Seção 3, existem no Brasil a mais de 20 anos. Entretanto, apesar da idade e dos ciclos evolutivos, ainda persistem diferentes problemas relacionados à transparência, confiabilidade e segurança (autenticidade, integridade e confidencialidade de programas e dados) dos sistemas utilizados nas urnas brasileiras.

Conforme discutimos na Seção 4, algumas falhas de segurança graves, como chaves armazenadas em código-fonte, chaves carregadas para a memória, chave única, primitivas criptográficas vulneráveis (e.g. MD5) ou não verificadas (e.g. Assina), entre outras, indicam que há uma clara falta de preocupação ou compromisso com a democracia por parte do TSE. Até hoje, não há nenhum método viável para auditar os resultados de uma eleição, o que pode ser considerado por alguns uma falha gravíssima no sistema democrático brasileiro.

Apesar de ser uma das questões mais controversas das urnas eletrônicas, hoje, o voto impresso é uma das maneiras mais aceitas para garantir a auditoria. Vale ressaltar que não é necessário imprimir todos os votos, ou seja, com apenas uma porcentagem deles já é possível comprovar as tendências de voto e assegurar que elas estão se refletindo nas urnas.

Vale ressaltar também outras questões, como os custos envolvidos nas diversas atualizações de hardware e software das urnas eletrônicas. Por exemplo, em 2018, o TSE orçou em 1,8 bilhão de reais a implantação do voto impresso. Como discutido na Seção 3.3, um investimento nessa ordem não é necessário para implantar voto impresso utilizando a tecnologia já disponível nas urnas eletrônicas.

Além disso, medidas como a disponibilização do código-fonte das urnas deveriam ter sido adotadas a muito tempo pelo TSE, pois é essencial, para o processo de segurança, a auditabilidade do código. Há diferentes exemplos práticos nesse sentido, como as bibliotecas de criptografia mais utilizadas na Internet, que são abertas e de código livre. Entretanto, nem por isso são mais vulneráveis. Ao contrário, são mais robustas, dominando o mercado.

Finalmente, exemplos de outros países, como o da

Estônia, podem ajudar a identificar fraquezas e forças de sistemas de votação eletrônica no sentido de criar soluções mais transparentes, seguras e que levem, ao mesmo tempo, a redução de custos. Os desafios são muitos e é preciso unir esforços da comunidade e dos países para preservar e, no futuro, colher os frutos de uma democracia em seu sentido mais pleno.

Agradecimentos e Informações Adicionais

Gostaríamos de agradecer aos comentários e sugestões dos revisores anônimos, que nos permitiram dar mais qualidade ao paper.

Vale ressaltar também que os quatro primeiros autores (Isadora Garcia Ferrão, João Otávio Chervinski, Sherlon Almeida da Silva e Diego Kreutz) contribuíram de forma equivalente no desenvolvimento do trabalho e na escrita do paper.

Referências

Aasmae, K. (2018). Estonia's ID card fiasco: 'we've no intention of letting a good crisis go to waste'. https://zd.net/2ZINc54 (Acessado em: 22 de Maio de 2019).

Agência Senado (2018). Participantes de audiência veem má vontade do TSE com voto impresso. https://goo.gl/sLgbvN (Acessado em: 22 de Maio de 2019).

Andrade, P. G. S. (2015). A fraude da urna eletrônica. https://jus.com.br/artigos/1549/a-fraude-da-urna-eletronica (Acessado em: 22 de Maio de 2019).

Aranha, D. (2018). É Possível Fraudar as Urnas Eletrônicas? Especialista Diego Aranha Responde na CCJ do Senado Federal. https://www.youtube.com/watch?v=_UxcgU6CGds (Acessado em: 22 de Maio de 2019).

Aranha, D., Barbosa, P., Cardoso, T., Luders, C. and Matias, P. (2018). The return of software vulnerabilities in the brazilian voting machine, *Conference on Cryptographic Hardware and Embedded Systems*. doi.org/10.13140/RG.2.2.16240.97287.

Aranha, D. F., Karam, M. M., de Miranda, A. and Scarel, F. (2013). Vulnerabilidades no software da urna eletrônica brasileira, *dos Testes Públicos de Segurança do Sistema Eletrônico de Votação do Tribunal Superior Eleitoral.* . https://bit.ly/2Er3tTt (Acessado em: 22 de Maio de 2019).

Aranha, D. F., Ribeiro, H. and Paraense, A. L. O. (2016). Crowdsourced integrity verification of election results, *Annals of Telecommunications* **71**(7–8): 287–297. https://doi.org/10.1007/s12243-016-0511-1.

Aranha, D., Karam, M., Miranda, A. and Scarel, F. (2012). Software vulnerabilities in the brazilian voting machine. https://bit.ly/2YJ2zcI (Acessado em: 22 de Maio de 2019).

Arthur, C. (2014). Estonian e-voting shouldn't be used in european elections, say security experts. https://bit.ly/2Egkj4z (Acessado em: 22 de Maio de 2019).

Barbosa, P. B. (2014). Avanços na tecnologia desenvolvida pela justiça eleitoral no brasil e seus efeitos na contemporaneidade, *Estudos Eleitorais* **9**: 91–115. https://bit.ly/2QmyH2Q (Acessado em: 22 de Maio de 2019).

Brunazo, A. and Amílcar, A. (1999). A segurança do voto na urna eletrônica brasileira, *Simpósio sobre Segurança en Informática. São Paulo: Instituto Tecnológico de Aeronáutica (ITA), Divisão de Ciência da Computação (CTA)* . https://bit.ly/2JXJnUi (Acessado em: 22 de Maio de 2019).

Cajado, A. F. R., Dornelles, T. and Pereira, A. C. (2014). *Eleições no Brasil: uma história de 500 anos*, Tribunal Superior Eleitoral. http://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/704 (Acessado em: 22 de Maio de 2019).

Camarão, P. C. B. (1997). *O voto informatizado: Legitimidade democrática*, Empresa das Artes.

Carpanez, J. (2018). Votação via internet, identidade universal e histórico médico online: o que faz da Estônia um país digital... https://goo.gl/JGd58S(Acessado em: 22 de Maio de 2019).

Casado, L. (2018). Justiça eleitoral diz que eliminou fragilidade das urnas eletrônicas. https://goo.gl/x7zFHd (Acessado em: 22 de Maio de 2019).

Costan, V. and Devadas, S. (2016). Intel SGX explained., *IACR Cryptology ePrint Archive* **2016**(086): 1–118. https://eprint.iacr.org/2016/086.pdf (Acessado em: 22 de Maio de 2019).

Cybersecurity Insiders (2018). Insider threat - 2018 report. http://tiny.cc/2c3z5y (Acessado em: 22 de Maio de 2019).

de Freitas[1], J. L. and Macadar, M. A. (2017). The brazilian electronic voting system: evolution and challenges, *The International Conference for Electronic Voting (E-Vote-ID)*, p. 59. https://bit.ly/2JWDXc3 (Acessado em: 22 de Maio de 2019).

Dufloth, S. C., Freitas, D. R. R. and Horta, C. J. G. (2014). Sistema brasileiro de votação eletrônica: aspectos do contexto atual sob as perspectivas técnico-operacional e legal, *Revista Uniabeu* **7**(17): 377–392. https://bit.ly/2YLvk8x (Acessado em: 22 de Maio de 2019).

Extra (2007). Urnas eletrônicas terão novo sistema operacional em 2008. https://goo.gl/7YyMsi (Acessado em: 22 de Maio de 2019).

Ferreira, L. (2013). Grupo hacker diz que urnas eletrônicas do brasil são propositalmente falhas e acusa vulnerabilidades. https://goo.gl/DJK4dM (Acessado em: 22 de Maio de 2019).

GaúchaZH (2018). Urna eletrônica completa 22 anos sem registros de fraudes. https://goo.gl/Uytnbh (Acessado em: 22 de Maio de 2019).

Gibson, J. P., Krimmer, R., Teague, V. and Pomares, J. (2016). A review of e-voting: the past, present and future, *Annals of Telecommunications* **71**(7–8): 279–286. https://doi.org/10.1007/s12243-016-0525-8.

Gogan, M. (2017). Insider threats as the main security threat in 2017. http://tiny.cc/wd3z5y (Acessado em: 22 de Maio de 2019).

Google Cloud (2018). Protecting Data with Cloud KMS Keys. https://cloud.google.com/bigquery/docs/customer-managed-encryption (Acessado em: 22 de Maio de 2019).

IBM Security (2018). 2018 IBM X-Force Threat Intelligence Index. http://tiny.cc/2b3z5y (Acessado em: 22 de Maio de 2019).

Jornal Nacional (2018). Urna eletrônica no brasil completa 22 anos com muito mais segurança. https://goo.gl/Jjzbkc (Acessado em: 22 de Maio de 2019).

Klumb, R. and Hoffmann, M. G. (2016). Inovação no setor público e evolução dos modelos de administração pública: o caso do TRE-SC, *Cadernos Gestão Pública e Cidadania* **21**(69). https://bit.ly/2M5WWDX (Acessado em: 22 de Maio de 2019).

Lellis, L. (2018). Conheça a preparação da urna eletrônica e o caminho do voto. https://goo.gl/HeJdrh (Acessado em: 22 de Maio de 2019).

Leyden, J. (2017). Estonia government locks down id smartcards: Refresh or else. https://bit.ly/2VEejv7 (Acessado em: 22 de Maio de 2019).

Macedo, D. (2018). Sistema usado nas urnas eletrônicas reduz custos em cerca de 4 milhões. https://goo.gl/NoivbZ (Acessado em: 22 de Maio de 2019).

Mari, A. (2014). Fraud possible in brazil's e-voting system. https://www.zdnet.com/article/fraud-possible-in-brazils-e-voting-system/ (Acessado em: 22 de Maio de 2019).

Martins, L. (2018a). Comissão de constituição, justiça e cidadania - 4a reunião extraordinária da 4a sessão legislativa ordinária da 55a legislatura. https://www12.senado.leg.br/multimidia/evento/78888 (Acessado em: 22 de Maio de 2019).

Martins, L. (2018b). Urnas: audiência pública. https://www.youtube.com/watch?v=ot-mkyyMCTw (Acessado em: 22 de Maio de 2019).

Monteiro, A., Soares, N., Oliveira, R. and Antunes, P. (2001). Sistemas electrónicos de votação. https://bit.ly/2VHActl (Acessado em: 22 de Maio de 2019).

Petersen, S. D. and Jaecks, H. K. (2005). Combination electronic and paper ballot voting system. https://bit.ly/2K0amhZ (Acessado em: 22 de Maio de 2019).

Pinto, R. R., Simões, F. and Antures, P. (2004). Estudo dos requisitos para um sistema de votação electrónica, *Technical report*, Faculdade de Ciências da Universidade de Lisboa. http://www.di.fc.ul.pt/~paa/reports/di-fcul-tr-04-2.pdf (Acessado em: 22 de Maio de 2019).

Ricci, P. and Porto Zulini, J. (2014). Partidos, competição política e fraude eleitoral: a tônica das eleições na primeira república, *Dados-Revista de Ciências Sociais* **57**(2). https://bit.ly/30Cc5jj (Acessado em: 22 de Maio de 2019).

Rodrigues-Filho, J., Alexander, C. J. and Batista, L. C. (2006). E-voting in brazil-the risks to democracy, *Lecture Notes in Informatics* pp. 85–94. https://oro.open.ac.uk/12543/1/12543.pdf (Acessado em: 22 de Maio de 2019).

Rohr, A. (2012). Falha na urna brasileira 'reproduzia fielmente' erro de 1995, diz professor. https://goo.gl/nsgWSs (Acessado em: 22 de Maio de 2019).

SBPC (2002). Software livre e urna eletrônica. https://goo.gl/JKE9E2 (Acessado em: 22 de Maio de 2019).

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014). Security analysis of the estonian internet voting system, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, ACM, New York, NY, USA, pp. 703–715. http://doi.acm.org/10.1145/2660267.2660315.

TSE (2013). Urna modelo 2013 (ue2013). https://goo.gl/fRmGiZ (Acessado em: 22 de Maio de 2019).

TSE (2014a). Conheça a história da urna eletrônica brasileira, que completa 18 anos. https://goo.gl/MmmpFN (Acessado em: 22 de Maio de 2019).

TSE (2014b). Informações e dados estatísticos sobre as eleições 2014. https://goo.gl/GgmQys (Acessado em: 22 de Maio de 2019).

TSE (2016). Série urna eletrônica: investimento em tecnologia aprimora a segurança do voto. https://goo.gl/wnpjjT (Acessado em: 22 de Maio de 2019).

Wang, K.-H., Mondal, S. K., Chan, K. and Xie, X. (2017). A review of contemporary e-voting: Requirements, technology, systems and usability, *Data Science and Pattern Recognition* **1**(1): 31–47. https://bit.ly/2LZW8QH (Acessado em: 22 de Maio de 2019).

Wheeler, D. A. (2015). Why open source software/free software (oss/fs, floss, or foss)? look at the numbers. https://dwheeler.com/oss_fs_why.html (Acessado em: 22 de Maio de 2019).

Winter, J. (2008). Trusted computing building blocks for embedded linux-based arm trustzone platforms, *Proceedings of the 3rd ACM workshop on Scalable trusted computing*, ACM, pp. 21–30. https://doi.org/10.1145/1456455.1456460.