

O SISTEMA ELETRÔNICO DE VOTAÇÃO BRASILEIRO

*Claudio Pereira da Silva*¹

*Deilton Ribeiro Brasil*²

Resumo: Inicialmente implantado no ano de 1996 no Brasil, o sistema eletrônico de votação brasileiro é um instrumento de modernização e agilidade no processo democrático do país. Observando a constante recorrência sobre o tema, o presente trabalho tem como objetivo, analisar se esse sistema de votação transmite confiabilidade, garante a normalidade e a legitimidade das eleições. Para tanto aprofundou-se na história, abordando os reais motivos da implantação e os inúmeros desafios, bem como os avanços do sistema de votação eletrônico implantado no Brasil, elencando os mecanismos utilizados pela Justiça Eleitoral para garantir a segurança no processo de votação. A ideia deste trabalho surgiu, em virtude de o sistema eletrônico de votação brasileiro ser alvo de controvérsias e desconfianças por parte de diversos setores da sociedade. E a questão principal investigada foi se o sistema com suas inovações e garantias técnicas, é realmente infalível em termos de segurança e transparência, considerando o contexto de crescente avanço tecnológico e de vigilância cibernética. E se não esteja sujeito a falhas que possam comprometer a legitimidade das eleições. As evidências sugerem que o sistema é eficiente para garantir que o processo eleitoral no Brasil se mantenha íntegro. Essas e outras questões serão abordadas levando em consideração análise bibliográfica, estudo de doutrinas, legislações pertinentes ao objeto de estudo e também se valerá de artigos já publicados, contará com método indutivo, descritivo, onde irá descrever as formas de segurança do sistema eletrônico de votação.

Palavras-chave: Eleição; voto; segurança, urna eletrônica, eleitor, legitimidade.

¹ Graduando em Direito pela Faculdade de Direito Santo Agostinho (FASASETE-AFYA) SW Sete Lagoas/MG. E-mail: seudireitoedever@yahoo.com

² Doutor em Direito pela UNIME, Itália. Doutor em Direito pela UGF-RJ. Professor da graduação e do Mestrado e do Doutorado em Proteção dos Direitos Fundamentais da Universidade de Itaúna (UIT), Faculdade Santo Agostinho (FASASETE-AFYA).

SUMÁRIO: 1.Introdução; 2.Fundamentação teórica; 2.1 Conceitos fundamentais de implantação dos sistema de votação eletrônica, 2.2 Evolução do sistema eletrônico de votação no Brasil, 3.segurança cibernética em sistemas eleitorais; 3.1 Ameaças á segurança cibernéticas em eleições, 3.2 Vulnerabilidade comuns em sistemas de votação eletrônico brasileiro, 4.sistema eletrônico de votação Brasileiro; casos e desafios; 4.1 Descrição da arquitetura e funcionamento do sistema de votação Brasileiro, 4.2 Medidas de Segurança implementadas no sistema de votação Brasileiro, 5. Análise de Casos Incidentais Relacionados à Segurança do Sistema Brasileiro de Votação, 6. considerações finais; Referências.

INTRODUÇÃO

O tema “O Sistema de Votação Eletrônico Brasileiro”, foi ponderado por ser um assunto bastante atual, sendo alvo de debates principalmente às vésperas de campanhas eleitorais.

Implantado no ano de 1996, é considerado de suma importância para manter a democracia do nosso país, trazendo agilidade e eficiência às eleições.

No entanto, enfrenta diversos questionamentos inerentes à confiabilidade do sistema, se realmente é capaz de garantir a normalidade e a legitimidade das eleições no país.

No dia 10 de agosto de 2021, por exemplo, foi protocolada com o intuito de instituir o voto impresso em eleições, plebiscitos e referendos na Câmara dos Deputados a PEC 139/2019, de autoria da deputada federal Bia Kicis (PSL-DF), entretanto, foi rejeitada e arquivada, visto que alcançou apenas 229 votos dos 306 necessários.

Este e outros ataques novamente colocaram em dúvidas o atual sistema eletrônico de votação implantado a mais de duas décadas.

Portanto, indaga-se: o nosso sistema de votação eletrônico brasileiro é capaz de garantir a transparência, a segurança e a lisura do processo eleitoral?

Após notas introdutórias, a seção um, abordará a história para demonstrar os reais motivos que se deram a implementar um sistema de votação eletrônico no Brasil. Indo além do mero senso comum de pensar que a urna eletrônica brasileira foi desenvolvida para somente dar celeridade à apuração e divulgação dos resultados das eleições, demonstrando também a evolução do sistema eletrônico de votação do país.

A seção dois, versará sobre um assunto de extrema importância e grande preocupação dos eleitores brasileiros, a segurança cibernética em sistemas eleitorais, ditando possíveis vulnerabilidades encontradas no mesmo, em testes elaborados pela Justiça Eleitoral, antes de todo pleito de votação acontecer.

A seção três, tratará de apresentar a arquitetura e o funcionamento do sistema de votação Brasileiro, as medidas de segurança adotadas para manter a transparência sem afetar o sigilo do voto, como tratará também do processo de auditoria e fiscalização.

Este trabalho tem como objetivo geral, analisar como funciona o sistema eletrônico de votação Brasileiro, como também, se o trabalho efetuado pelo Tribunal Superior Eleitoral tem apresentado efeitos positivos em relação a problemática apresentada.

Dessa forma, para viabilizar o teste de hipótese, realiza-se uma pesquisa de finalidade básica estratégica, objetivo descritivo e exploratório, sob o método indutivo, com abordagem qualitativa e realizada com procedimentos bibliográficos.

Partindo da hipótese de que o sistema de votação eletrônico adotado no Brasil é seguro e transparente, visto os esforços depreendidos pelo TSE com diversas auditorias e testes públicos, com liberação do código-fonte da urna eletrônica permitindo verificar possíveis falhas e fraudes na urna eletrônica.

Ao chegar nas considerações finais, verificar-se-a se os objetivos foram atendidos, com a confirmação da hipótese, indicando, portanto, se o Sistema Brasileiro de Votação eletrônico, garante a normalidade e a legitimidade das eleições no país, e se o faz de forma transparente, permitindo nas etapas do processo eleitoral, a participação dos cidadãos.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção aborda os conceitos fundamentais de implantação dos sistemas de votação eletrônica, que foram introduzidos para eliminar fraudes e melhorar a eficiência na contagem dos votos. O Brasil é o país pioneiro no uso de urnas eletrônicas em pleitos de votação, com constantes melhorias tecnológicas.

2.1 CONCEITOS FUNDAMENTAIS DE IMPLANTAÇÃO DO SISTEMA DE VOTAÇÃO ELETRÔNICA

Embora, seja comum ouvir dizer que a urna eletrônica brasileira foi desenvolvida para dar celeridade à apuração e divulgação dos resultados das eleições, na verdade, é apenas uma consequência do modelo eletrônico. Voltaremos um pouco na história para compreendermos os motivos da implantação do voto eletrônico no Brasil, e identificar problemas e vícios inerentes ao processo de votação e apuração que ocorriam nas eleições até o ano de 1994.

O primeiro problema estava relacionado com a interpretação da vontade do eleitor. No modelo de cédulas em papel era permitido ao eleitor votar em um determinado candidato ou legenda de partido (nos cargos proporcionais) identificando o nome ou número do candidato desejado. Ocorre que, frequentemente, havia problemas com a caligrafia, ou o eleitor escrevia o nome incompleto, ou ainda, utilizava um apelido para o candidato. Esses problemas acarretavam em situações de homonímia (vários candidatos com o mesmo nome) ou de impossibilidade de identificar com clareza o candidato a que se destina o voto. Essas situações poderiam incorrer na anulação do voto ou destinação a outro candidato, por solicitação dos fiscais presentes, ficando a decisão à critério da junta eleitoral responsável pela apuração.

O segundo problema estava relacionado à manipulação dos resultados, seja a partir da cédulas (marcação de votos em cédulas em branco ou troca de cédulas) ou dos mapas de votação (alteração das tabelas de resultados após a contagem dos votos), o chamado mapismo. Eram frequentes as denúncias de manipulação de resultados, assim como os recursos e pedidos de impugnação de seções eleitorais e anulação dos resultados baseadas nesses vícios. Conforme Cunha(2009), em 1994 houve mais oito mil recursos interpostos em todo o Estado do Rio Grande do Sul, tendo por objeto o escrutínio daquelas eleições gerais.

O terceiro problema, diz respeito ao sigilo do voto do eleitor, que frequentemente era coagido a votar em determinado candidato – o chamado voto a cabresto e os famosos currais eleitorais. Havia ainda a fraude por compra de votos, que privilegiava a elite econômica local. A própria caligrafia do eleitor ou a inclusão de

marcas na cédula de papel muitas vezes poderiam incorrer na identificação da pessoa que havia preenchido aquela cédula.

As características do modelo utilizado anteriormente ao advento da urna eletrônica não permitiam a implantação do controle necessário do processo. Esse modelo dependia de uma forte e intensa fiscalização por todas as partes interessadas – prejudicando os partidos menores e que não dispunham de tantos fiscais – e da idoneidade absoluta das pessoas envolvidas em todas as fases do processo, o que acabava se tornando um verdadeiro tormento para os juízes eleitorais, maculando o processo eleitoral e colocando em cheque a transparência e confiabilidade das eleições em todo o país.

Com a evolução da tecnologia, era natural que se pensasse em um modelo eletrônico de votação que viesse suprir as necessidades do processo eleitoral e ao mesmo tempo tentar corrigir as falhas e vícios do modelo existente até então. Em 1995, o TSE criou a Comissão de Informatização das Eleições, composta por desembargadores, juízes e técnicos em informática.

Entre as principais premissas estabelecidas pela comissão para orientar a elaboração do projeto da urna, cita: o sistema deverá estar consoante com a legislação eleitoral então existente; o voto deverá ser registrado numericamente; o eleitor terá o direito de ver a descrição de seu candidato escolhido, inclusive sua foto, antes de confirmar o voto; o equipamento para registro do voto deverá ser de uso exclusivo; o equipamento deverá ser pequeno, compacto, leve e poder ser transportado sem sofrer danos; e o eleitor poderá corrigir seu voto antes de confirmá-lo e poderá também votar em branco. (CUNHA, 2009).

A criação desse sistema visava eliminar fraudes e garantir maior segurança e transparência ao processo eleitoral. A urna eletrônica se destacou por sua capacidade de reduzir a interferência humana no processo eleitoral e por proporcionar uma apuração rápida dos resultados. Desde sua implementação, passou por diversas auditorias e testes públicos que confirmaram sua integridade e segurança.

2.2 EVOLUÇÃO DO SISTEMA ELETRÔNICO DE VOTAÇÃO NO BRASIL

Iniciou-se a primeira eleição com o sistema de urna no ano de 1996, quando foram realizadas eleições municipais em todo o país. Nesse pleito eleitoral, a urna eletrônica foi utilizada em todas as capitais e também nos municípios com mais de 200 mil eleitores.

A partir das eleições de 2000, o Brasil passou a adotar a votação totalmente eletrônica, utilizando uma solução padrão para todo o país. Ao longo dos anos, diversas modificações foram introduzidas no software e no hardware da urna eletrônica, por recomendação de especialistas, para atender demandas dos partidos políticos ou para resolver questões e problemas encontrados a partir das experiências com os pleitos anteriores.

Um dos conjuntos mais importantes de mudanças introduzidas e que levaram à consolidação da maturidade da urna eletrônica, foram as sugestões apontadas pelo relatório apresentado por especialistas da Universidade Estadual de Campinas, em 2002, denominado Relatório 17 Unicamp¹⁰, após minuciosa investigação e análise do código da urna em 2002.

Esse relatório apresentou “um conjunto de recomendações cujo objetivo é o aumento da segurança e da confiabilidade do Sistema Informatizado de Eleições, em especial de seu componente mais sensível que é a urna eletrônica”.

A seguir, listamos as recomendações apontadas, que podem ser conferidas a partir da página 37 do relatório:

a) Desenvolvimento dos aplicativos de votação baseados em blocos estáveis permanentes para todas as eleições; b) Formalização do ciclo de desenvolvimento do software; c) Avaliação do código-fonte do núcleo do aplicativo e seus componentes acessórios por especialistas em informática independentes do TSE; d) Compilação e determinação de resumos criptográficos dos arquivos em sessão pública; e) Verificação, por representantes partidários, dos resumos criptográficos dos arquivos instalados nas urnas carregadas com o software; f) Revisão do procedimento de preparação da urna para o segundo turno; g) Impressão do boletim de urna antes do ciframento dos resultados da votação; h) Substituição do uso de ciframento por assinaturas digitais como forma de autenticação dos boletins de urna.

O Relatório da Unicamp aponta que “O sistema eletrônico de votação

implantado no Brasil a partir de 1996 é um sistema robusto, seguro e confiável atendendo a todos os requisitos do sistema eleitoral brasileiro”. E conclui dizendo que:

Como resultado da avaliação realizada conclui-se que o sistema eletrônico de votação analisado atende as exigências fundamentais do processo eleitoral, ou seja, o respeito a expressão do voto do eleitor e a garantia do seu sigilo. Conclui-se também que a segurança e a confiabilidade do sistema de votação eletrônico podem ainda ser aprimoradas pela adoção de procedimentos e modificações apontados (...)

(...) A confiabilidade do processo eleitoral depende crucialmente do controle sobre todas as etapas de sua condução, que deve ser exercido pela sociedade por meio dos partidos políticos, dos fiscais, dos mesários, dos juízes eleitorais e dos próprios eleitores. Algumas das recomendações acima só terão seus objetivos totalmente atendidos se houver a efetiva fiscalização e acompanhamento por representantes aptos a fazê-lo. (UNICAMP, 2002, pág. 46 e 47).

O sistema eletrônico continuou a evoluir. Nas eleições gerais de 2002, conforme mudança instituída pela Lei nº 10.408/2002 em busca de maior segurança do pleito, foram adquiridos módulos de impressão externa de votos. O uso desse equipamento seria obrigatório a partir das eleições municipais de 2004; no entanto, a Justiça Eleitoral antecipou seu uso para teste. O eleitor deveria conferir o voto visualmente antes que ele fosse depositado em uma urna lacrada.

Entretanto, as experiências com a impressão mostraram que essa prática não contribuiu para aumentar a segurança. O Relatório das Eleições 2002 indicou que houve problemas significativos relacionados à impressão dos votos, como travamentos nas impressoras e aumento nas filas nas seções eleitorais.

Em resposta às dificuldades enfrentadas durante esse pleito, foi decidido eliminar o voto impresso em favor do Registro Digital do Voto (RDV), instituído pela Lei nº 10.740/2003.

A auditoria tornou-se um aspecto crucial na evolução do sistema eletrônico. O TSE implementou uma série de medidas para garantir a transparência e a segurança das eleições. As agremiações políticas puderam solicitar auditorias em

urnas adicionais até 30 dias após o pleito. Essas auditorias confirmaram a integridade das urnas auditadas e reforçaram a confiança no sistema.

3.SEGURANÇA CIBERNÉTICA EM SISTEMAS ELEITORAIS

Nesta seção, serão discutidas as possíveis ameaças à segurança cibernética em eleições, que incluem tentativas de fraudes e ataques a sistemas de transmissão de dados.

Apesar das robustas medidas de segurança, há possibilidade de vulnerabilidades serem exploradas por hackers, exigindo uma constante vigilância.

3.1 AMEAÇAS À SEGURANÇA CIBERNÉTICA EM ELEIÇÕES

A segurança cibernética em eleições, tornou-se uma questão de crescente preocupação nas últimas décadas, especialmente à medida que a tecnologia se torna um componente central dos processos democráticos.

Com a digitalização das urnas, o registro de eleitores e a transmissão de resultados, as eleições estão mais suscetíveis a uma variedade de ameaças cibernéticas que podem comprometer a integridade, a confidencialidade e a disponibilidade dos dados eleitorais.

As ameaças à segurança cibernética em eleições podem ser categorizadas em várias formas, incluindo ataques de hackers, desinformação e manipulação de dados.

Ataques direcionados, como phishing e ransomware, podem visar sistemas eleitorais e funcionários envolvidos no processo, com o intuito de roubar informações sensíveis ou causar interrupções.

Além disso, a desinformação é uma ameaça significativa, pois pode influenciar a opinião pública e criar desconfiança nas instituições democráticas.

Campanhas de desinformação, muitas vezes coordenadas por atores externos, buscam manipular a narrativa em torno das eleições, polarizando a sociedade e minando a confiança no processo eleitoral.

As consequências dessas ameaças podem ser graves. A manipulação de resultados eleitorais pode levar a questionar a legitimidade de um governo, em quanto, vazamentos de dados pessoais de eleitores podem resultar em violações de privacidade.

Além disso, a propagação de desinformação pode desestabilizar o ambiente político, gerando tensões sociais e afetando a participação cidadã nas eleições.

Para enfrentar essas ameaças, é essencial que o Brasil implemente robustas medidas de segurança cibernética. Isso inclui a realização de auditorias de segurança nos sistemas eleitorais, a capacitação de funcionários para identificar e responder a ataques cibernéticos e a promoção da alfabetização midiática entre os eleitores para que possam discernir informações confiáveis de fontes fraudulentas.

3.2 VULNERABILIDADES COMUS EM SISTEMAS DE VOTAÇÃO ELETRÔNICA BRASILEIRO

A votação eletrônica no Brasil, implementada em 1996, trouxe avanços significativos na agilidade e na transparência do processo eleitoral. No entanto, como qualquer sistema tecnológico, as urnas eletrônicas não estão isentas de vulnerabilidades.

Especialistas têm identificado e documentado diversas fragilidades que podem comprometer a integridade do sistema, levando a preocupações sobre a segurança do voto eletrônico.

Um dos estudos mais relevantes sobre as vulnerabilidades das urnas eletrônicas foi conduzido por Diego F. Aranha e sua equipe da Universidade Estadual de Campinas (Unicamp). Durante os Testes Públicos de Segurança organizados pelo Tribunal Superior Eleitoral (TSE), a equipe conseguiu identificar falhas no software da urna eletrônica que poderiam ser exploradas para fraudes eleitorais. Entre as vulnerabilidades detectadas, destacam-se a possibilidade de recuperação da ordem dos votos computados e a manipulação de mensagens exibidas ao eleitor, o que poderia ser utilizado para influenciar o voto de forma indevida.

Além disso, o relatório de Aranha enfatiza que todo software é potencialmente vulnerável, o que torna imprescindível a adoção de um registro físico do voto como um mecanismo adicional de segurança.

Essa prática é recomendada pela comunidade técnica internacional e é uma medida que outros países que utilizam votação eletrônica já implementaram para garantir a transparência do processo eleitoral.

A experiência anterior da equipe em testes semelhantes revelou que era possível quebrar o sigilo dos votos, permitindo a recuperação dos votos em ordem e comprometendo a privacidade do eleitor.

Outro estudo relevante foi realizado pelo TSE, que promoveu auditorias regulares nas urnas eletrônicas. Essas auditorias incluem o Teste Público de Segurança (TPS), onde especialistas são convidados a tentar invadir o sistema e identificar falhas. Desde 2009, quando esse teste foi iniciado, nenhum ataque conseguiu alterar o resultado das eleições, mas algumas vulnerabilidades foram encontradas e corrigidas ao longo dos anos.

Essas auditorias são importantes não apenas para identificar falhas, mas também para reforçar a confiança da sociedade no sistema eleitoral. As vulnerabilidades identificadas não se limitam apenas ao software. O hardware das urnas também apresenta riscos.

Embora as urnas sejam projetadas com medidas de segurança rigorosas, como lacres físicos e hardware criptográfico que impede alterações não autorizadas, ainda existem preocupações sobre possíveis ataques físicos ou manipulações durante o processo eleitoral.

O fato de as urnas não estarem conectadas à internet é uma barreira significativa contra ataques cibernéticos; no entanto, isso não elimina completamente as possibilidades de manipulação se um acesso físico for obtido.

A discussão sobre a implementação do voto impresso nas eleições brasileiras também reflete as preocupações acerca da segurança das urnas eletrônicas. Defensores do voto impresso argumentam que ele poderia servir como um registro físico adicional para auditoria e recontagem em caso de disputas eleitorais. No entanto, críticos apontam que isso pode introduzir novos riscos e complicações no processo.

Em suma, embora o sistema de votação eletrônico brasileiro tenha avançado significativamente desde sua implementação, as vulnerabilidades identificadas por especialistas ressaltam a necessidade contínua de vigilância e melhorias.

A realização regular de testes públicos de segurança e auditorias é crucial para garantir a integridade do processo eleitoral e aumentar a confiança pública nas eleições. A adoção de medidas adicionais, como o registro físico do voto, pode ser uma solução viável para mitigar riscos associados às fraudes eleitorais.

4 O SISTEMA DE VOTAÇÃO (URNA ELETRÔNICA)

A trajetória da urna eletrônica é marcada por inovações constantes, com melhorias tecnológicas implementadas ao longo dos anos. A cada eleição, novos modelos são introduzidos, incorporando avanços em segurança e usabilidade.

As urnas mais recentes incluem recursos como leitores biométricos e certificação de segurança por laboratórios credenciados, refletindo um compromisso contínuo com a integridade do sistema eleitoral (TRE-PR, 2024).

4.1 DESCRIÇÃO DA ARQUITETURA E FUNCIONAMENTO DO SISTEMA DE VOTAÇÃO BRASILEIRO

A arquitetura e o funcionamento do sistema de votação eletrônico brasileiro são projetados para garantir a integridade, segurança e transparência do processo eleitoral. Desde a sua implementação em 1996, as urnas eletrônicas têm se mostrado um marco na modernização das eleições no Brasil, utilizando tecnologia avançada para coletar e apurar votos de forma rápida e confiável.

O sistema de votação brasileiro é composto por dois principais módulos: o terminal do eleitor e o terminal do mesário. O terminal do eleitor é onde o voto é registrado, enquanto o terminal do mesário é utilizado para habilitar os eleitores e controlar o processo de votação.

Cada urna eletrônica é um microcomputador isolado, projetado para operar sem conexão à internet, o que minimiza as vulnerabilidades a ataques cibernéticos.

A segurança física das urnas é reforçada por lacres de segurança que evidenciam qualquer tentativa de violação (TRE-SP, 2021). Cada urna possui um hardware criptográfico que assegura a autenticidade dos dados coletados e impede a execução de softwares não autorizados.

A arquitetura da urna inclui múltiplas camadas de proteção, totalizando cerca

de 30 mecanismos distintos que garantem sua inviolabilidade. Por exemplo, a urna só pode ser ativada pelo software desenvolvido pelo Tribunal Superior Eleitoral (TSE), e qualquer tentativa de uso de programas não autorizados resulta no bloqueio imediato do equipamento (CNJ, 2021).

O funcionamento da urna eletrônica inicia-se com a habilitação do mesário, que verifica a situação regular do eleitor através do terminal correspondente. Uma vez autorizado, o eleitor se dirige ao terminal do eleitor, onde registra seu voto. O sistema utiliza criptografia simétrica e assimétrica para proteger as informações sobre os votos individuais e os resultados coletados. Cada voto é criptografado e assinado digitalmente antes de ser transmitido ao TSE (TSE, 2024). A transmissão dos dados ocorre após o encerramento da votação, utilizando uma conexão segura.

Embora as urnas não estejam conectadas à internet durante o processo de votação, os resultados são enviados ao TSE através de redes seguras após a apuração local. Essa abordagem garante que os dados sejam protegidos contra acessos não autorizados durante todo o processo eleitoral.

Além das características técnicas mencionadas, as urnas eletrônicas são submetidas a rigorosos testes públicos de segurança antes de cada eleição. Esses testes envolvem especialistas que tentam identificar vulnerabilidades no sistema, permitindo que o TSE faça as correções necessárias antes das eleições (TRE-PR, 2024). A transparência é um princípio fundamental; portanto, o código-fonte da urna é disponibilizado para representantes dos partidos políticos e observadores internacionais.

A acessibilidade também é uma preocupação central na arquitetura das urnas eletrônicas. As máquinas são projetadas para serem utilizadas por todos os cidadãos, incluindo aqueles com deficiência visual ou motora. Recursos como teclados em Braille e saídas de áudio garantem que todos possam participar plenamente do processo eleitoral (TRE-SP, 2021).

4.2 MEDIDAS DE SEGURANÇA IMPLEMENTADAS NO SISTEMA DE VOTAÇÃO BRASILEIRO

As medidas de segurança implementadas no sistema de votação eletrônico

brasileiro são fundamentais para garantir a normalidade e a legitimidade das eleições. Desde a sua introdução, o sistema tem sido aprimorado constantemente para enfrentar os desafios da segurança cibernética e assegurar a confiança do eleitorado. Diversos artigos e relatórios publicados por especialistas e instituições relevantes destacam as principais características e mecanismos de segurança adotados.

A arquitetura do sistema de votação eletrônico é projetada para ser robusta e segura. As urnas eletrônicas operam com software desenvolvido exclusivamente pelo Tribunal Superior Eleitoral (TSE), que é auditável e testado antes de cada eleição. O TSE realiza Testes Públicos de Segurança (TPS), onde especialistas são convidados a tentar identificar vulnerabilidades no sistema. Esses testes são uma oportunidade crucial para detectar falhas e implementar correções antes do pleito, garantindo que o software utilizado nas urnas seja confiável (TRE-SC, 2023).

Um dos pilares da segurança do sistema é a auditabilidade. O processo eleitoral brasileiro conta com pelo menos 26 oportunidades de auditoria, que incluem desde a verificação do código-fonte das urnas até a lacração dos equipamentos antes da votação. A Comissão de Transparência das Eleições (CTE) e outras entidades fiscalizadoras têm acesso a esses processos, permitindo uma supervisão independente e rigorosa (TRE-SE, 2023). Além disso, o Tribunal de Contas da União (TCU) também realiza auditorias externas, assegurando que todas as etapas do processo eleitoral sejam monitoradas adequadamente.

As urnas eletrônicas são projetadas para operarem sem conexão à internet durante a votação, o que reduz significativamente o risco de ataques cibernéticos. A segurança física das urnas é garantida por lacres que evidenciam qualquer tentativa de violação. Além disso, as informações sobre os votos são criptografadas, garantindo que os dados não possam ser acessados ou manipulados indevidamente durante o processo (CNJ, 2021).

A legislação brasileira também desempenha um papel crucial na proteção da legitimidade das eleições. O artigo 14, §9º da Constituição Federal estabelece medidas para proteger a normalidade e legitimidade do pleito, permitindo à Justiça Eleitoral atuar contra abusos de poder político que possam comprometer a equidade do processo eleitoral (Bernardi, 2013). A efetividade dessas normas é fundamental para assegurar que todos os candidatos tenham igualdade de condições durante as

eleições.

Além das medidas técnicas e legais, o TSE tem promovido campanhas de conscientização sobre a importância da segurança eleitoral e da participação cidadã. A educação sobre o funcionamento do sistema de votação eletrônico é essencial para aumentar a confiança do eleitorado e combater desinformações que possam surgir durante o processo eleitoral.

Em suma, as medidas de segurança implementadas no sistema de votação eletrônico brasileiro são abrangentes e multifacetadas. Elas incluem uma arquitetura segura, auditorias rigorosas, proteção contra fraudes, mecanismos legais eficazes e esforços educacionais para promover a confiança pública no sistema eleitoral. Essas iniciativas não apenas garantem a integridade das eleições, mas também fortalecem a democracia no Brasil.

5 ANÁLISE DE CASOS INCIDENTAIS RELACIONADOS A SEGURANÇA DO SISTEMA BRASILEIRO DE VOTAÇÃO

Nos últimos anos, o sistema de votação eletrônico brasileiro enfrentou uma série de incidentes que colocaram em questão sua segurança e integridade.

Um dos casos mais notáveis ocorreu durante as eleições de 2022, quando o então presidente da República questionou publicamente a confiabilidade das urnas eletrônicas, alimentando um clima de desconfiança em torno do sistema eleitoral. Essa situação foi exacerbada pela disseminação de desinformação nas redes sociais, que teve um impacto significativo na percepção pública sobre a legitimidade do processo eleitoral (Migalhas, 2022).

A Comissão de Transparência das Eleições e o Programa Permanente de Enfrentamento à Desinformação (PPED) foram instituídos pelo Tribunal Superior Eleitoral (TSE) como resposta a esses desafios.

O objetivo dessa iniciativa é garantir a transparência do processo e combater as alegações infundadas que surgiram durante o período eleitoral. No entanto, mesmo com essas medidas, a desinformação continua sendo um desafio premente, com campanhas que visam desacreditar a Justiça Eleitoral e criar um ambiente de insegurança entre os eleitores (Conjur, 2022).

Outro incidente relevante foi o envolvimento das Forças Armadas na fiscalização das urnas eletrônicas durante as eleições. Embora essa ação tenha sido vista como uma medida de transparência, também gerou preocupações sobre a militarização do processo eleitoral e a possibilidade de interferência política. A presença das Forças Armadas nas eleições foi criticada por alguns setores da sociedade civil como uma tentativa de legitimar dúvidas sobre a integridade do sistema (Migalhas, 2022).

5.1 DESAFIOS E CRÍTICAS EM RELAÇÃO A INTEGRIDADE DO SISTEMA

Os desafios enfrentados pelo sistema de votação eletrônico brasileiro são multifacetados e refletem um ambiente político polarizado. A desinformação e as teorias da conspiração têm se proliferado nas redes sociais, dificultando o trabalho da Justiça Eleitoral em restaurar a confiança pública no sistema.

Especialistas apontam que essa desinformação não apenas compromete a percepção da integridade das eleições, mas também pode levar ao aumento da violência política, como evidenciado por um aumento de 400% nos atos violentos relacionados ao processo eleitoral (Migalhas, 2022).

Além disso, o uso crescente de algoritmos pelas plataformas digitais para direcionar informações ao público tem levantado preocupações sobre manipulação e controle da narrativa eleitoral.

Durante um seminário realizado pelo TSE e pela Fundação Getulio Vargas, especialistas discutiram como esses algoritmos podem contribuir para a polarização política e desinformação, dificultando ainda mais a integridade do debate democrático (TSE, 2024). As recomendações incluem monitoramento ativo da desinformação e treinamento para funcionários que lidam diretamente com o público para identificar táticas enganosas.

Por fim, é importante destacar que a legislação brasileira ainda carece de regras específicas para regular o comportamento das plataformas digitais durante períodos eleitorais.

Embora algumas iniciativas tenham sido tomadas para combater a desinformação e proteger a integridade cívica, há uma necessidade urgente de

desenvolver políticas abrangentes que abordem esses desafios de forma eficaz (InternetLab, 2023).

6 CONSIDERAÇÕES FINAIS

Ao longo deste trabalho, foi possível analisar de forma detalhada o sistema de votação eletrônico brasileiro e suas implicações para a normalidade e legitimidade das eleições no país.

A partir da hipótese inicial, que se propôs a investigar se o sistema eletrônico de votação Brasileiro realmente garante a transparência e a legitimidade dos pleitos eleitorais, foi possível concluir que, o sistema eletrônico de votação Brasileiro garante sim a normalidade e a legitimidade das eleições no país, o sistema contribui conscientemente para garantir a regularidade e a confiança nas eleições brasileiras.

No entanto, tal conclusão não é simples e exige uma análise crítica, que deve considerar não apenas os aspectos técnicos da urna eletrônica, mas também os fatores externos que afetam diretamente a percepção pública sobre o sistema.

Os ataques externos, como a disseminação de fake news e outras formas de desinformação, tentam prejudicar a normalidade e legitimidade das eleições no Brasil de várias maneiras.

A atuação rápida do TSE em responder a esses ataques tem sido primordial para neutraliza-los e conduzindo os pleitos das eleições de forma transparente, refutando todos os ataques dirigidos contra o sistema eletrônico de votação.

O modelo de votação eletrônica implementado no Brasil, desde sua criação em 1996, consolidou-se como um marco importante no combate à manipulação e à fraude eleitoral.

A arquitetura do sistema, composta por múltiplas camadas de segurança, e os rigorosos procedimentos de auditoria, como os Testes Públicos de Segurança (TPS) e a disponibilização do código-fonte, garantem que o processo de votação seja minimamente vulnerável a fraude externa.

A ausência de conexão das urnas eletrônicas à internet durante o processo de votação representa uma segurança essencial contra ataques cibernéticos, o que, em tese, dificulta significativamente qualquer tentativa de interferência maliciosa nos

resultados. O sistema possui mecanismos sólidos de segurança, como criptografia e auditorias independentes, garantindo que o processo eleitoral ocorra de forma íntegra e justa.

Portanto, ao se considerar o cenário atual, fica claro que o sistema de votação eletrônica no Brasil, embora com limitações e desafios, continua a ser um instrumento fundamental para a preservação da integridade das eleições.

Contudo, a resposta a esses desafios passa por um esforço conjunto da sociedade, das instituições eleitorais e dos próprios participantes (eleitores), no sentido de fortalecer a transparência, a educação digital e a proteção contra as ameaças externas, de modo a garantir que o sistema continue a distinguir o papel de um pilar da democracia.

REFERÊNCIAS

ARANHA, Diego F. Vulnerabilidades no software da urna eletrônica brasileira. Disponível em: <https://dfaranja.github.io/publication/aranhakms13/>. Acesso em: 12 set. 2024.

BARRETO, Irineu. Fake News: Anatomia da Desinformação, Discurso de Ódio e Erosão da Democracia. (Coleção direito eleitoral) . Rio de Janeiro: Saraiva Jur, 2022. E-book. pág.10. ISBN 9786555598841. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555598841/>. Acesso em: 17 out. 2024.

CNJ. "CNJ Serviço: saiba porque a urna eletrônica é segura e avançada." Disponível em: CNJ Serviço: saiba porque a urna eletrônica é segura e avançada - Portal CNJ. Acesso em: 15 out. 2024.

CNJ. "CNJ Serviço: saiba porque a urna eletrônica é segura e avançada." Disponível em: CNJ Serviço: saiba porque a urna eletrônica é segura e avançada - Portal CNJ. Acesso em: 02 nov. 2024.

CONJUR. "Justiça Eleitoral, 90 anos, encara o maior desafio de sua história." Disponível em: Justiça Eleitoral, 90 anos, encara o maior desafio de sua história (conjur.com.br). Acesso em: 08 nov. 2024.

Diário Oficial da União: Brasília, DF, 24 jul. 2003.TSE. Histórico da Urna Eletrônica. [2021]. Disponível em: <https://www.tre-sp.jus.br/eleicoes/biometria-e-urna-eletronica/historico-da-urna-eletronica>

INTERNETLAB. "Compromisso com a democracia: Integridade eleitoral e o Estado Democrático de Direito nas políticas de plataformas digitais." Disponível em: Plataformas deixam a desejar na proteção da integridade eleitoral (desinformante.com.br). Acesso em: 12 nov. 2024.

SENADO. Teste feito por equipe da Unicamp revelou falhas de segurança nas urnas eletrônicas. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/03/06/teste-feito-por-equipe-da-unicamp-revelou-falhas-de-seguranca-nas-urnas-eletronicas>. Acesso em: 12 set. 2024.

VELOSO, Carlos Mário da S.; AGRA, Walber M. Elementos de Direito Eleitoral - 8ª Edição 2023 . 8ª edição. Rio de Janeiro: Saraiva Jur, 2023. E-book. pág.364. ISBN 9786555598810. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555598810/>. Acesso em: 17 nov. 2024.

TRE-SP. Histórico da Urna Eletrônica. [2021]. Disponível em: <https://www.tre-sp.jus.br/eleicoes/biometria-e-urna-eletronica/historico-da-urna-eletronica>

TRE-MT. Artigo: A confiabilidade das urnas eletrônicas e do processo eleitoral brasileiro. Disponível em: <https://www.tre-mt.jus.br/comunicacao/noticias/2021/Agosto/artigo-a-confiabilidade-das-urnas-eletronicas-e-do-processo-eleitoral-brasileiro>. Acesso em: 17 set. 2024.

TRE-SP. Saiba mais sobre a segurança da urna eletrônica. Disponível em: <https://www.tre-sp.jus.br/comunicacao/noticias/2024/Outubro/saiba-mais-sobre-a-seguranca-da-urna-eletronica>. Acesso em: 17 set.nov. 2024.

TRE-GO. Entenda por que não é possível fraudar a urna eletrônica. Disponível em: <https://www.tre-go.jus.br/comunicacao/noticias/2024/Fevereiro/entenda-por-que-nao-e-possivel-fraudar-a-urna-eletronica>. Acesso em: 15 out. 2024.

TRE-SP. "Por dentro da urna: como funciona o hardware da máquina de votar." Disponível em: Por dentro da urna: como funciona o hardware da máquina de votar — Tribunal Regional Eleitoral de São Paulo (tre-sp.jus.br). Acesso em: 15 out. 2024.

TSE. "Como nasce uma urna: por trás da máquina." Disponível em: Como nasce uma urna: por trás da máquina, o esforço para essa produção da inteligência humana — Tribunal Superior Eleitoral (tse.jus.br). Acesso em: 15 out. 2024.

TRE-PR. "Detalhes técnicos das urnas eletrônicas 2020 e 2022." Disponível em: Detalhes técnicos das urnas eletrônicas 2020 e 2022 (justicaeleitoral.jus.br). Acesso em: 28 out.. 2024.

TRE-SC. "Você sabia que o sistema eletrônico de votação é totalmente auditável?" Disponível em: Abuso do poder político e o rigor de sua punição pela Justiça Eleitoral

do Brasil: efetividade da norma constitucional de tutela da legitimidade das eleições — Tribunal Regional Eleitoral de Santa Catarina (tre-sc.jus.br). Acesso em: 28 out. 2024.

TRE-SE. "Você sabia que o sistema eletrônico de votação é totalmente auditável?" Disponível em: Você sabia que o sistema eletrônico de votação é totalmente auditável? — Tribunal Regional Eleitoral de Sergipe (tre-se.jus.br). Acesso em: 02 nov. 2024.

TSE. "Especialistas apresentam sugestões para lidar com desafios criados por algoritmos em contextos eleitorais." Disponível em: Especialistas apresentam sugestões para lidar com desafios criados por algoritmos em contextos eleitorais — Tribunal Superior Eleitoral (tse.jus.br). Acesso em: 12 nov. 2024.