DA SEGURANÇA À CONFIANÇA: A EVOLUÇÃO DOS MECANISMOS DE SEGURANÇA E AUDITORIA DO SISTEMA ELETRÔNICO DE VOTAÇÃO BRASILEIRO E OS DESAFIOS À LEGITIMIDADE DEMOCRÁTICA

CARLOS ROBERTO DE MENEZES
BRUNO ANDRADE

Sobre os autores:

Carlos Roberto de Menezes: Servidor do TRE-DF desde 1997 (com atuação para o TSE desde 1987), onde foi Chefe de Cartório, Coordenador de Infraestrutura de TI e atualmente chefia a Seção de Apoio às Eleições (SEAEL). Graduado em TI, pós-graduado em Segurança da Informação e em Direito Eleitoral (UERJ), com certificações em governança e segurança (ITIL, COBIT e ISO).

Bruno Andrade: Doutor em Direito da Cidade (UERJ), Mestre em Direito (Estácio de Sá) e especialista em Direito Eleitoral (UCAM). Servidor do CNJ, professor (PUC Minas, IDP, UERJ/CEPED e UPIS), membro da ABRADEP e avaliador do IBEROJUR, é autor e coordenador de obras sobre liberdade de expressão, LGPD e direito eleitoral.

RESUMO

Ao completar três décadas em 2026, o sistema eletrônico de votação brasileiro destaca-se pela contínua evolução de seus mecanismos de segurança, transparência e auditabilidade frente aos desafios da desinformação e da crise de confiança institucional. Por meio de pesquisa qualitativa, exploratória e documental, o artigo analisa normas do ciclo de 2026, documentos técnicos do TSE e literatura especializada, articulando ciência da computação, usabilidade e verificabilidade fim a fim. Argumenta-se que o modelo brasileiro migrou de uma lógica baseada na confiança institucional para uma arquitetura de confiança verificável, sustentada por fiscalização e produção de evidências ao longo do ciclo eleitoral. Conclui-se que a verificabilidade técnica, embora indispensável à legitimidade democrática, não gera automaticamente confiança social — dimensão não aferida empiricamente neste estudo.

Palavras-chave: Sistema eletrônico de votação; segurança eleitoral; auditoria; confiança institucional; legitimidade democrática.

ABSTRACT

Turning three decades old in 2026, Brazil's electronic voting system stands out for the continuous evolution of its security, transparency, and auditability mechanisms amid challenges posed by digital disinformation and declining institutional trust. Through qualitative, exploratory, and documentary research, this article examines 2026 electoral regulations, technical documentation from the Superior Electoral Court (TSE), and peer-reviewed literature, integrating insights from computer science, usability, and end-to-end verifiability. It argues that the Brazilian model has shifted from a paradigm rooted in institutional trust to an architecture of verifiable trust, underpinned by oversight and evidence production throughout the electoral cycle. The study concludes that while technical verifiability is indispensable to democratic legitimacy, it does not automatically foster social trust—a dimension not empirically measured in this research.

Keywords: Electronic voting system; electoral security; auditing; institutional trust; democratic legitimacy.

INTRODUÇÃO

A introdução do sistema eletrônico de votação nas eleições brasileiras de 1996 constitui um dos mais relevantes processos de transformação tecnológica da história eleitoral contemporânea do país. A substituição progressiva da votação e da apuração baseadas em procedimentos predominantemente manuais por um sistema informatizado modificou não apenas a forma de manifestação da vontade eleitoral, mas também os mecanismos destinados a proteger, verificar e demonstrar a integridade dos resultados. A experiência iniciada em 1996 foi progressivamente ampliada até alcançar todos os municípios brasileiros nas eleições de 2000. Ao longo das três décadas seguintes, a Justiça Eleitoral incorporou mecanismos de identificação biométrica, criptografia, assinatura digital, cadeia de segurança de hardware, Registro Digital do Voto (RDV), Boletim de Urna (BU) com mecanismos de validação, abertura dos códigos-fonte, Testes Públicos de Segurança e diferentes modalidades de auditoria antes, durante e depois da votação. A própria evolução oficial da urna registra a introdução do RDV em 2004, da identificação biométrica a partir de 2006, de mecanismos dedicados de segurança e criptografia a partir da geração UE2009 e do QR Code no Boletim de Urna a partir de 2016 (BRASIL, 2025b). A segurança do sistema eletrônico de votação, portanto, não constitui característica estática de determinado modelo de urna. Trata-se de uma arquitetura composta por diferentes camadas, aperfeiçoada ao longo de sucessivos ciclos eleitorais. Ao mesmo tempo em que essa arquitetura tecnológica e institucional se desenvolveu, ocorreu uma transformação profunda no ambiente de comunicação política. A expansão das redes sociais e das plataformas digitais permitiu que questionamentos sobre a segurança e a legitimidade das eleições alcançassem grandes públicos com velocidade e escala sem precedentes. Pesquisas sobre o ambiente digital brasileiro identificaram a circulação de conteúdos conspiratórios e mensagens de contestação eleitoral relacionadas à segurança das urnas eletrônicas (Dourado; Almeida; Piaia, 2024). Surge, assim, um paradoxo: a crescente sofisticação dos mecanismos técnicos de segurança e auditoria não se traduz necessariamente, na mesma proporção, em aumento da confiança social no sistema eleitoral. O problema de pesquisa deste artigo consiste em verificar em que medida a evolução dos mecanismos de segurança e auditoria do sistema eletrônico de votação brasileiro contribui para a transparência e a legitimidade democrática das eleições diante de um ambiente de crescente desinformação. A hipótese é que o sistema brasileiro evoluiu de uma lógica predominantemente baseada na confiança institucional para uma arquitetura de confiança verificável, na qual a segurança é acompanhada por mecanismos de fiscalização, auditoria e produção de evidências. Entretanto, a existência desses mecanismos não é suficiente, por si só, para converter segurança técnica em confiança social. O percurso metodológico, a constituição do corpus e os limites do estudo são detalhados na seção 1; o marco conceitual que sustenta a análise é fixado na seção 2.

1 PERCURSO METODOLÓGICO

1.1 NATUREZA E RECORTE DA PESQUISA

A pesquisa é qualitativa, exploratória e documental, com dimensão de análise normativa. O recorte temporal compreende o período de 1996 a 2026 e se justifica por dois marcos: a primeira utilização da urna eletrônica, nas eleições municipais de 1996, e a consolidação normativa dos procedimentos de fiscalização e auditoria operada pela Resolução TSE n. 23.758/2026, que encerra o ciclo examinado. No interior desse arco distinguem-se dois momentos: o de informatização e expansão, de 1996 a 2008, voltado sobretudo à automação da votação e da apuração; e o de institucionalização da auditabilidade, de 2009 em diante,

inaugurado pela introdução de dispositivo dedicado à segurança e pela primeira edição do Teste Público de Segurança.

1.2 CONSTITUIÇÃO DO CORPUS

O corpus foi organizado em três estratos, cada qual com critérios próprios de inclusão e exclusão.

O estrato normativo reúne a Lei n. 9.504/1997, o Código Eleitoral, a Resolução TSE n. 23.673/2021, com suas alterações, e a decisão proferida pelo Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade n. 5889. Adotaram-se como critérios a vigência do ato no ciclo eleitoral de 2026 e a pertinência direta aos procedimentos de segurança, fiscalização ou auditoria.

O estrato institucional e técnico abrange documentos publicados pelo próprio Tribunal Superior Eleitoral e de acesso público: a documentação técnica do *software* da urna eletrônica, os materiais sobre a evolução do equipamento, as páginas relativas ao Teste Público de Segurança e ao Ciclo de Transparência e os roteiros de auditoria (Brasil, [s. d.]). O critério de inclusão foi a origem institucional somada à disponibilidade pública; excluíram-se materiais de divulgação desprovidos de conteúdo procedimental.

O estrato acadêmico resultou de busca nas bases SciELO, Portal de Periódicos da CAPES, Biblioteca Digital do Tribunal Superior Eleitoral, Biblioteca Digital da Sociedade Brasileira de Computação e Google Acadêmico, com os descritores "urna eletrônica", "voto eletrônico", "auditoria eleitoral", "*software independence*", "*end-to-end verifiability*" e "desinformação eleitoral", empregados isoladamente e em combinação. O recorte abrange o período de 2012 a 2026, cujo termo inicial corresponde à segunda edição do Teste Público de Segurança, primeira a franquear aos participantes o acesso ao código-fonte. Incluíram-se artigos submetidos a revisão por pares e relatórios técnicos de autoria identificável; excluíram-se textos de natureza opinativa e materiais sem explicitação de procedimento.

1.3 PROCEDIMENTO DE ANÁLISE

A análise documental desenvolveu-se em três movimentos. No primeiro, procedeu-se ao levantamento e à leitura integral do corpus, com registro das passagens pertinentes ao objeto. No segundo, cada mecanismo de segurança, fiscalização ou auditoria identificado foi submetido a protocolo uniforme de extração, composto por seis campos: base normativa, momento do ciclo eleitoral em que opera, objeto declarado de verificação, agente habilitado a conduzi-lo, tipo de evidência que produz e limite reconhecido na literatura técnica. No terceiro, os registros assim constituídos foram confrontados entre si e com as avaliações independentes disponíveis, de modo a analisar convergências e divergências.

1.4 CONSTRUÇÃO DA MATRIZ DE AUDITABILIDADE

A matriz apresentada na seção 9 não decorre de arranjo intuitivo. Suas colunas correspondem aos campos do protocolo descrito na subseção anterior, e seu eixo temporal reproduz a sequência dos capítulos da Resolução TSE n. 23.673/2021, que organiza os procedimentos conforme a cronologia do ciclo eleitoral. Cada célula foi validada por cotejo com o dispositivo normativo correspondente e, quando cabível, com a documentação técnica. A matriz constitui instrumento descritivo: ordena mecanismos segundo momento, objeto e natureza da verificação, sem aferir a eficácia individual de cada um deles.

1.5 LIMITES DO ESTUDO

Quatro limites devem ser consignados. O primeiro é que o estudo não afere empiricamente a confiança social no sistema eletrônico de votação: descreve a arquitetura de verificabilidade e discute sua relação com a legitimidade, mas a mensuração da confiança demandaria desenho de pesquisa diverso, de natureza quantitativa e amparado em levantamentos de opinião. O segundo é que a pesquisa não teve acesso ao código-fonte dos sistemas eleitorais, de modo que as afirmações sobre o funcionamento interno dos programas repousam em documentação institucional e em relatórios de terceiros. O terceiro é que a descrição dos procedimentos depende, em medida relevante, de fontes produzidas pela própria autoridade eleitoral, circunstância atenuada, mas não eliminada, pelo cotejo com avaliações externas. O quarto é que a revisão de literatura não pretende exaustividade: privilegia os trabalhos de maior circulação no debate brasileiro e as contribuições internacionais diretamente pertinentes aos conceitos mobilizados.

2 MARCO CONCEITUAL: AUDITABILIDADE, VERIFICABILIDADE E CONFIANÇA

2.1 TRÊS PLANOS FREQUENTEMENTE SOBREPOSTOS

O debate sobre o sistema eletrônico de votação costuma reunir sob um mesmo rótulo realidades distintas. Convém separá-las antes de descrever a arquitetura.

A auditabilidade é propriedade do desenho institucional: designa a existência de procedimentos, registros e prerrogativas que tornam o processo examinável por terceiros. Trata-se de atributo normativo, aferível pela leitura dos atos que o instituem.

A verificabilidade é propriedade da evidência: designa a possibilidade de que terceiro, de posse dos registros disponíveis, confirme ou refute asserção determinada sobre o resultado. Distingue-se da auditabilidade porque não basta que o exame seja permitido; é preciso que os elementos examinados autorizem conclusão. E comporta gradação conforme a verificação dependa, ou não, da integridade do próprio sistema examinado. Rivest (2008) denomina independente de *software* o sistema em que alteração indetectada no programa não é capaz de produzir alteração indetectada no resultado da eleição.

A confiança é atitude social: designa a disposição do corpo de eleitores a aceitar o resultado proclamado. Constitui variável empírica, aferível por levantamentos de opinião, e não consequência lógica da existência dos mecanismos. Um sistema pode ser auditável e verificável sem ser socialmente confiado, assim como pode ser socialmente confiado sem jamais ter sido auditado.

2.2 O ALCANCE DA EXPRESSÃO CONFIANÇA VERIFICÁVEL

A expressão confiança verificável, adotada neste estudo e anunciada em seu título, designa o modelo normativo em que a autoridade institucional deixa de operar isoladamente e passa a ser acompanhada por evidências conferíveis por terceiros. Descreve, portanto, uma transformação na estrutura da relação entre instituição e sociedade, e não um estado de opinião pública.

Duas delimitações se impõem. A primeira é que a expressão não afirma que a confiança social tenha sido efetivamente produzida pela verificação; essa relação causal constitui hipótese que o presente artigo não testa, pelas razões consignadas na subseção 1.5. A segunda é que a expressão não supõe que todo mecanismo de verificação possua idêntico alcance: como se demonstrará na seção 9, os mecanismos da arquitetura brasileira distribuem-se por categorias distintas quanto ao tipo de asserção que autorizam, e a conferência entre registros produzidos pelo próprio sistema não equivale, por si só, à verificação independente da correspondência entre o resultado apurado e a vontade manifestada pelo eleitor.

Essas delimitações não enfraquecem a tese sustentada adiante. Ao contrário, permitem enunciá-la com a precisão que o objeto exige.

3 TRÊS DÉCADAS DE EVOLUÇÃO DO SISTEMA ELETRÔNICO DE VOTAÇÃO

A primeira experiência de utilização da urna eletrônica ocorreu nas eleições municipais de 1996, em 57 municípios. Em 1998, a votação eletrônica alcançou 537 municípios e, nas eleições municipais de 2000, passou a ser utilizada em todo o país. A evolução posterior incorporou sucessivas gerações de *hardware* e *software* e novos mecanismos de segurança e fiscalização (BRASIL, 2025b). A trajetória pode ser resumida em alguns marcos fundamentais.

Quadro 1 – Marcos da evolução do sistema eletrônico de votação (1996-2026)

Período	Marco tecnológico ou institucional
1996	Primeira utilização da urna eletrônica em 57 municípios
1998	Ampliação para 537 municípios
2000	Informatização integral da votação
2002	Ampliação das possibilidades de auditoria e primeira Cerimônia de Lacração dos Sistemas
2004	Introdução do Registro Digital do Voto
2006	Introdução da identificação biométrica
2008	Expansão da identificação biométrica
2009	Introdução de dispositivo dedicado à segurança e criptografia; primeiro Teste Público de Segurança
2012	Segunda edição do Teste Público de Segurança
2016	QR Code no Boletim de Urna e terceira edição do Teste Público de Segurança
2020/22	Nova geração de hardware, maior capacidade computacional; aperfeiçoamentos de segurança; utilização do Teste de Integridade com Biometria
2025	Oitava edição do Teste Público de Segurança e abertura dos códigos-fonte das Eleições
2026	Aperfeiçoamento normativo dos procedimentos de auditoria e consolidação do Teste de Integridade com Biometria

Fonte: elaboração própria a partir de BRASIL (2025b).

Essa evolução demonstra que a segurança eleitoral não deve ser compreendida como uma propriedade adquirida definitivamente em 1996. Ao contrário, ela resulta de um processo contínuo de desenvolvimento, avaliação e aperfeiçoamento. Em 2004, o Registro Digital do Voto passou a constituir um importante mecanismo de registro e conferência. Em 2009, a Justiça Eleitoral introduziu dispositivo dedicado à segurança e à criptografia, estabelecendo uma arquitetura em que o conjunto formado pela urna e pelo sistema de votação deve ser autenticado para funcionar. Em 2016, os Boletins de Urna passaram a incorporar QR Code, ampliando as possibilidades de conferência dos resultados. Já a geração UE2020 incorporou a certificação ICP-Brasil do perímetro criptográfico do *hardware*, enquanto a UE2022 manteve essa geração tecnológica com aperfeiçoamentos de processamento, interação e segurança (Brasil, 2025b). A história do sistema eletrônico de votação revela, portanto, uma

transição de uma tecnologia inicialmente voltada, sobretudo, à automação da votação e da apuração para uma arquitetura mais abrangente de segurança, fiscalização e auditabilidade.

4 A ARQUITETURA DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO

A segurança do sistema eletrônico de votação brasileiro não está concentrada em um único mecanismo. Ela resulta da combinação de diferentes medidas físicas, lógicas, criptográficas e procedimentais. A Resolução TSE n. 23.673/2021, com suas alterações, define conceitos como assinatura digital, auditoria, cadeia de custódia, compilação, lacração, Registro Digital do Voto, resumo digital, tabelas de correspondência e Teste de Autenticidade dos Sistemas Eleitorais (Brasil, 2021, art. 2º, I, IV, IX, XI e XII).

A segurança física envolve a proteção dos equipamentos, o controle dos ambientes e a utilização de lacres e procedimentos de preparação e custódia. A lacração dos sistemas ocorre após a apresentação e conferência dos programas, que são assinados digitalmente e gravados em mídias apropriadas. A resolução estabelece também procedimento específico de lacração das urnas, com lacres físicos nas interfaces de conexão e no gabinete (Brasil, 2021, arts. 19 a 27). Essa camada é relevante porque reduz a possibilidade de intervenção física não autorizada entre a preparação do equipamento e sua utilização.

A segurança lógica envolve os programas responsáveis pela preparação, votação, apuração, transmissão e totalização. A regulamentação determina que os sistemas eleitorais sejam submetidos a processos de desenvolvimento, compilação, assinatura e lacração. A compilação transforma os códigos-fonte em arquivos executáveis, permitindo posteriormente a comparação entre aquilo que foi desenvolvido e aquilo que efetivamente será instalado.

A assinatura digital permite verificar a autenticidade de documentos e sistemas. De acordo com a Resolução TSE n. 23.673/2021, ela utiliza operações matemáticas baseadas em criptografia assimétrica para comprovar a origem do documento ou sistema (BRASIL, 2021, art. 2º, I). A assinatura digital é especialmente relevante porque permite verificar se determinado arquivo ou programa corresponde ao conteúdo autorizado.

O resumo digital, conhecido como hash, é uma sequência produzida matematicamente a partir de um arquivo. Uma alteração no arquivo original produz outro resumo digital. A função do mecanismo é permitir a conferência de integridade. Assim, o hash não precisa "provar" que o conteúdo é correto em termos absolutos; ele permite verificar se o conteúdo conferido permanece idêntico ao conteúdo previamente utilizado como referência.

No plano da cadeia de segurança, a Justiça Eleitoral também utiliza mecanismos associados ao hardware. Segundo documentação institucional, a geração UE2009 introduziu dispositivo dedicado à segurança e à criptografia, estabelecendo uma arquitetura em que a urna e seu respectivo sistema de votação precisam ser autênticos para funcionar (Brasil, 2025b). A importância dessa arquitetura reside na combinação das barreiras. Um eventual comprometimento de uma camada não significa automaticamente o comprometimento de todo o sistema. Essa característica permite compreender a segurança eleitoral a partir do conceito de defesa em profundidade, no qual diferentes mecanismos atuam sucessivamente para prevenir, detectar ou dificultar alterações indevidas.

5 FISCALIZAÇÃO DO CÓDIGO-FONTE E TESTE PÚBLICO DE SEGURANÇA

5.1 ACESSO DAS ENTIDADES FISCALIZADORAS AOS SISTEMAS

Um dos elementos mais relevantes da arquitetura brasileira é a possibilidade de fiscalização dos sistemas eleitorais por entidades legitimadas. A Resolução TSE n. 23.673/2021 assegura às entidades fiscalizadoras acesso antecipado aos sistemas desenvolvidos pelo TSE a

partir de 12 meses antes do primeiro turno, até a etapa de compilação, em ambiente específico e sob supervisão do Tribunal (Brasil, 2021, arts. 9º e 10). Para as Eleições 2026, os códigos-fonte foram disponibilizados em outubro de 2025. As inspeções permaneceram disponíveis ao longo do ciclo pré-eleitoral, antes da Cerimônia de Assinatura Digital e Lacração dos Sistemas Eleitorais. A norma contempla diversas categorias de entidades fiscalizadoras, entre elas partidos políticos e federações, Ministério Público, Defensoria Pública, Congresso Nacional, Controladoria-Geral da União, Polícia Federal, Sociedade Brasileira de Computação, Conselho Federal de Engenharia e Agronomia, Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Tribunal de Contas da União, entidades privadas sem fins lucrativos credenciadas e departamentos de tecnologia da informação de universidades credenciadas (Brasil, 2021, art. 9º, § 1º). Essa estrutura tem importância democrática porque permite que a confiança no sistema não dependa exclusivamente de uma relação vertical entre eleitor e autoridade eleitoral. A possibilidade de inspeção por terceiros introduz uma dimensão de confiança verificável. Não se trata de afirmar que qualquer cidadão individualmente consiga compreender todos os componentes do sistema. Trata-se de reconhecer que instituições qualificadas podem acessar os sistemas em condições regulamentadas, examinar seu funcionamento, formular questionamentos e acompanhar o processo. Em 2026, por exemplo, diferentes instituições realizaram inspeções nos códigos-fonte, incluindo o Senado Federal e outras entidades. O Ministério Público Federal também iniciou inspeção dos códigos destinados às eleições daquele ano.

5.2 O TESTE PÚBLICO DE SEGURANÇA COMO INSTRUMENTO DE MELHORIA CONTÍNUA

O Teste Público de Segurança dos Sistemas Eleitorais (TPS) constitui outro elemento central da arquitetura de segurança. A iniciativa foi realizada pela primeira vez em 2009 e passou a integrar uma política permanente de avaliação externa dos sistemas. Até 2025, o TSE realizou oito edições do teste, promovendo a participação de pesquisadores e especialistas na tentativa de identificar vulnerabilidades. A característica mais importante do TPS está justamente em sua lógica. Seu objetivo não deve ser interpretado como uma tentativa de provar que um sistema tecnológico é absolutamente invulnerável. Sistemas complexos não podem ser tratados dessa maneira. O teste procura criar condições para que pesquisadores tentem encontrar fragilidades. A existência de um achado, portanto, não representa automaticamente uma fraude eleitoral. Um achado técnico constitui uma informação sobre uma vulnerabilidade ou comportamento que precisa ser analisado, reproduzido, classificado e, quando pertinente, corrigido. O próprio TSE descreve o TPS como instrumento de fortalecimento da confiabilidade, transparência e segurança e registra que a identificação de falhas permite aperfeiçoar os sistemas (Brasil, 2025c). A edição de 2025, destinada às Eleições 2026, constituiu a oitava edição do procedimento. O teste ocorreu em dezembro de 2025, após a abertura dos códigos-fonte no âmbito do Ciclo de Transparência das Eleições 2026 (Brasil, 2025a). A importância do mecanismo pode ser resumida na seguinte lógica: testar, identificar, analisar, corrigir e testar novamente. Essa lógica aproxima a segurança eleitoral das práticas contemporâneas de segurança de sistemas críticos.

5.3 O QUE AS EDIÇÕES DO TESTE PÚBLICO DE SEGURANÇA REVELARAM

A afirmação de que o Teste Público de Segurança constitui instrumento de melhoria contínua ganha envergadura quando confrontada com seus resultados concretos. Em 2012, uma equipe de pesquisadores independentes demonstrou que o mecanismo de

embaralhamento do Registro Digital do Voto podia ser revertido a partir de produtos públicos da própria eleição, permitindo recompor a ordem cronológica dos votos de uma seção e, com isso, comprometer o sigilo do sufrágio. Em 2017, a mesma linha de investigação obteve execução de código arbitrário no equipamento a partir da adulteração da mídia de carga (Aranha et al., 2013; Marcacini; Barreto Junior, 2019, p. 136-139).

Esses achados não desmentem a tese aqui sustentada. Ao contrário, confirmam-na. Um sistema que jamais produzisse achados seria ou perfeito (hipótese que a engenharia de sistemas críticos não admite) ou submetido a testes incapazes de encontrar o que existe. A relevância dos episódios de 2012 e 2017 reside em outro ponto: eles desvelam que a verificabilidade se torna efetiva quando o exame é conduzido por terceiros com autonomia metodológica, tempo suficiente e liberdade de publicação. As correções que se seguiram a cada edição integram, nessa quadra, o próprio ciclo descrito acima.

6 VERIFICAÇÃO DOS SISTEMAS ANTES DA VOTAÇÃO

A auditoria ocorre também durante a preparação das urnas. A regulamentação prevê procedimentos de verificação da integridade e autenticidade dos sistemas instalados, inclusive mediante ferramentas desenvolvidas pelo TSE ou pelas próprias entidades fiscalizadoras. Entre os instrumentos previstos estão o AVPART, destinado à verificação da autenticidade dos programas da urna, e o VPP - Verificação Pré/Pós-Eleição, além de programas de verificação desenvolvidos por entidades fiscalizadoras (Brasil, 2021, arts. 4º, I e IV, 38 e 39). A Resolução estabelece ainda que as entidades fiscalizadoras podem acompanhar procedimentos de verificação e formular questionamentos. Esse modelo é importante porque estabelece uma conexão entre três momentos: 1. o sistema examinado durante o desenvolvimento; 2. o sistema compilado, assinado e lacrado; 3. o sistema efetivamente instalado na urna. A finalidade é reduzir o espaço entre aquilo que foi fiscalizado e aquilo que efetivamente será utilizado.

7 AUDITORIA NO DIA DA VOTAÇÃO

7.1 TESTE DE AUTENTICIDADE E TESTE DE INTEGRIDADE

No dia da eleição, a auditoria alcança as próprias urnas que estão ou poderiam estar relacionadas ao processo de votação. O Teste de Autenticidade dos Sistemas Eleitorais tem por finalidade verificar a integridade e a autenticidade dos programas instalados na urna eletrônica. A regulamentação prevê exame dos procedimentos de verificação e conferência dos lacres antes do início da votação (Brasil, 2021, arts. 75 a 80). O Teste de Integridade, por sua vez, constitui uma simulação controlada da votação. Urnas são submetidas a procedimentos nos quais votos conhecidos são inseridos e posteriormente comparados com o resultado produzido pelo equipamento. A Resolução estabelece expressamente a conferência do resultado apresentado pela urna com os votos realizados durante o teste (Brasil, 2021, arts. 61 a 73). A lógica é simples, embora o sistema tecnológico seja complexo: voto conhecido, digitação na urna, apuração pela urna e comparação com o resultado conhecido. Se o resultado produzido pela urna não corresponder aos votos efetivamente inseridos, haverá uma inconsistência que deverá ser investigada.do pela urna não corresponder aos votos efetivamente inseridos, haverá uma inconsistência que deverá ser investigada.

7.2 OS LIMITES DO TESTE DE INTEGRIDADE

O raciocínio subjacente ao Teste de Integridade (voto conhecido, digitação, apuração e

comparação) é sólido, mas possui um pressuposto que precisa ser explicitado: o de que o equipamento testado não sabe que está sendo testado. A literatura de segurança computacional analisa precisamente esse pressuposto. Um programa malicioso implantado por adversário interno pode ser dotado de condições de disparo baseadas em data, horário, cadência de digitação ou ausência de habilitação de eleitores, comportando-se de modo íntegro sempre que identificar ambiente de auditoria e desviando-se apenas na seção real. Sob essa hipótese, para Marcacini e Barreto Junior (2019), a votação paralela não prova a integridade do *software*: prova a integridade do software quando observado.

Contudo, os pressupostos apontados pelos pesquisadores merecem ressalva. O fundamento central da crítica é o de que o teste de integridade é realizado em condições tão específicas que seria facilmente contornado por invasores internos. Afirmam, por exemplo, que o tempo entre a votação de eleitores no teste de integridade é "irreal, pois cada voto simulado precisa ser gravado em vídeo, ser inserido em um segundo computador [...], de modo que se passam vários minutos entre um voto e seu subsequente" (Marcacini; Barreto Junior, 2019, p. 129-130). Essa demora, para os autores, permitiria ao software malicioso identificar que aquela determinada urna estaria passando pelo teste de integridade, pois "em condições reais, três ou quatro eleitores teriam usado a urna eletrônica em um intervalo desses" (Marcacini; Barreto Junior, 2019, p. 130). A premissa, contudo, não se sustenta. As características das seções eleitorais variam de modo acentuado em razão da dimensão continental do eleitorado brasileiro. Nesse sentido, a votação constante com poucos segundos entre eleitores pode ser característica de algumas seções eleitorais, mas não constitui regra geral. Além disso, o volume de eleitores de cada seção interfere nesse fluxo, assim como a própria afluência do eleitorado, que se dá de forma não uniforme ao longo do dia, embora concentrada no período da manhã. Por certo, aperfeiçoamentos no procedimento podem reforçar as barreiras e mitigar esse tipo de vulnerabilidade.

Registrar esse limite não equivale a sustentar que ele tenha sido explorado. Vale a distinção assentada na seção 11.3 entre possibilidade teórica, vulnerabilidade concreta e exploração efetiva. Vale, porém, para compreender por que o Teste de Integridade com Biometria, examinado a seguir, representa avanço qualitativo e não mero refinamento procedimental: ao introduzir eleitores reais e habilitação biométrica, a simulação aproxima-se das condições da seção autêntica e estreita a margem de discriminação entre ambiente de teste e ambiente de votação. Estreita, sem eliminar. É essa constatação que conduz ao debate sobre independência de *software*.

7.3 O TESTE DE INTEGRIDADE COM BIOMETRIA

Uma evolução recente da arquitetura de auditoria foi a utilização do Teste de Integridade com Biometria, implementado nas eleições de 2022 e incorporado à regulamentação para as Eleições 2026. A Resolução TSE n. 23.758/2026 inseriu um conjunto específico de dispositivos na Resolução n. 23.673/2021 para disciplinar o procedimento. A norma estabelece, entre outros pontos, a participação de eleitoras e eleitores voluntários, a utilização da biometria para habilitação (Brasil, 2026c), o registro da presença e procedimentos específicos de documentação e acompanhamento (Brasil, 2026b). A inovação possui relevância porque responde a uma questão recorrente no debate público: a diferença entre uma simulação realizada sem eleitores e uma simulação que incorpora a etapa de habilitação biométrica. A existência da biometria no teste não substitui as demais camadas de auditoria. Ela acrescenta uma modalidade de verificação. A regulamentação também estabelece limites para o fornecimento de determinados arquivos produzidos pelas urnas submetidas ao teste e disciplina a documentação do procedimento, evidenciando que a auditabilidade deve coexistir com proteção de informações e preservação do sigilo eleitoral (Brasil, 2026b).

8 REGISTROS DA VOTAÇÃO E AUDITORIA APÓS A TOTALIZAÇÃO

8.1 ZERÉSIMA, BOLETIM DE URNA E REGISTRO DIGITAL DO VOTO

A auditabilidade não se limita aos testes realizados pela Justiça Eleitoral. A própria votação produz documentos e registros que permitem conferência. A zerésima é emitida antes do início da votação e permite demonstrar a situação inicial da urna (Brasil, 2021, art. 67). Ao final da votação, é produzido o Boletim de Urna, documento que apresenta os resultados daquela seção eleitoral. O Boletim de Urna possui importância especial porque permite comparar o resultado produzido localmente com o resultado posteriormente divulgado na totalização. O TSE informa que o BU contém dados como identificação do município, zona, local, seção, votos por partido e candidato, votos em brancos e nulos, além de elementos de validação. O documento contém QR Code e suas vias são destinadas a diferentes formas de conferência e fiscalização (Brasil, 2024a). O QR Code amplia a possibilidade de conferência porque permite a leitura digital do conteúdo do BU. A documentação técnica do TSE também disponibiliza especificações relacionadas aos arquivos de BU, RDV, assinaturas digitais e logs, bem como informações para leitura e verificação desses arquivos (Brasil, 2022). O Registro Digital do Voto constitui outro mecanismo relevante. Introduzido em 2004, o RDV registra os votos de forma embaralhada e separada por cargo, preservando o sigilo da escolha individual enquanto permite procedimentos de verificação e auditoria (Brasil, 2025b). A combinação entre zerésima, BU, QR Code, RDV, assinaturas digitais, *hashes* e *logs* forma uma rede de registros que permite confrontar diferentes etapas do processo.

8.2 AUDITORIA APÓS A VOTAÇÃO E A TOTALIZAÇÃO

A auditabilidade continua após o encerramento da votação. A Resolução TSE n. 23.673/2021 prevê a verificação de relatórios e cópias de arquivos dos sistemas e a verificação da correção da contabilização dos votos por meio da comparação com os Boletins de Urna impressos (BRASIL, 2021, art. 5º, VIII, 'b' e arts. 51 e 52). Também existe previsão de preservação da integridade dos arquivos de log relacionados ao envio, recebimento e processamento dos Boletins de Urna (Brasil, 2021, art. 83). Essa característica é importante para compreender o sistema como um processo completo. Não basta analisar apenas a urna. É necessário considerar: preparação, votação, encerramento, geração do BU, transmissão, recebimento, totalização, conferência. A segurança do processo eleitoral deve acompanhar todo esse fluxo. A possibilidade de confrontar o resultado local produzido pelo BU com o resultado posteriormente disponibilizado constitui uma das principais características de verificabilidade do modelo.

9 MATRIZ DE AUDITABILIDADE E TIPOLOGIA DOS MECANISMOS DE VERIFICAÇÃO

A partir da documentação analisada, pode-se propor uma matriz para representar as diferentes etapas da auditabilidade:

Quadro 2 – Matriz de auditabilidade do sistema eletrônico de votação

Momento	Mecanismo	Principal objeto de verificação
Desenvolvimento	Inspeção do código-fonte	Lógica e funcionamento dos sistemas
	Acompanhamento por entidades fiscalizadoras	Processo de especificação e desenvolvimento

Pré-eleição	Teste Público de Segurança	Vulnerabilidades e resiliência
Compilação	*Hash*	Integridade
	Assinatura digital	Autenticidade
Lacração	Mídias e lacres	Preservação dos sistemas
Preparação	AVPART	Autenticidade dos programas
	VPP	Verificações pré e pós-eleição
	Tabelas de correspondência	Associação entre seção e urna
Dia da eleição	Teste de Autenticidade	Integridade e autenticidade dos programas
	Zerésima (no início da votação)	Situação inicial da urna
	Teste de Integridade	Correspondência entre votos conhecidos e resultado
	Teste com Biometria	Funcionamento da urna com habilitação biométrica
	Boletim de Urna (no fim da votação)	Resultado da seção
	QR Code (no fim da votação)	Conferência digital do Boletim de Urna
Pós-eleição	RDV	Registro digital dos votos
	Logs	Rastreabilidade de eventos e operações
Totalização	Comparação BU/resultado	Correspondência entre o resultado local e totalização

Fonte: elaboração própria a partir de BRASIL (2021).

Essa matriz permite visualizar uma característica central do modelo brasileiro: não existe uma única auditoria da urna eletrônica. Existe uma cadeia de procedimentos de fiscalização distribuídos por diferentes fases do processo.

A matriz autoriza, ainda, um segundo movimento analítico. Os mecanismos nela arrolados não possuem todos a mesma natureza, e a distinção importa para delimitar o que cada um efetivamente demonstra.

Um primeiro conjunto verifica a autenticidade do programa. O resumo digital, a assinatura digital, a lacração, o AVPART e o Teste de Autenticidade atestam que o executável em uso corresponde àquele que foi inspecionado, compilado e lacrado. Demonstram identidade entre o programa fiscalizado e o programa instalado, o que é condição necessária de toda a cadeia subsequente.

Um segundo conjunto opera verificação intrassistêmica. A zerésima, o boletim de urna, o QR Code, o Registro Digital do Voto, os *logs* e o cotejo entre boletim e totalização confrontam registros gerados pelo próprio sistema. Sua contribuição é substancial e com frequência subestimada: fecham a superfície de ataque relativa à transmissão e à totalização, etapas em que historicamente se concentraram as fraudes do período das cédulas de papel. A asserção que autorizam é de consistência entre registros.

Um terceiro conjunto introduz elemento externo ao sistema. O Teste de Integridade compara o resultado apurado com votos conhecidos fora do equipamento, registrados em vídeo e em computador apartado; a inspeção do código-fonte e o Teste Público de Segurança submetem o artefato a exame conduzido por terceiros qualificados. São os mecanismos de

maior alcance demonstrativo e operam, no caso do Teste de Integridade, por amostragem.

A tipologia não estabelece hierarquia de importância. Mecanismos das três categorias são necessários, e a arquitetura extrai sua força precisamente da combinação entre eles: a verificação intrassistêmica só é significativa porque precedida da verificação de autenticidade, e esta só é significativa porque o artefato autenticado foi submetido a exame externo. O que a tipologia permite é enunciar com exatidão o que cada camada demonstra, de modo que a soma dos mecanismos não seja tomada por garantia de natureza diversa daquela que cada um deles produz.

10 DA SEGURANÇA À CONFIANÇA VERIFICÁVEL

A evolução descrita permite propor uma mudança conceitual na compreensão da confiança eleitoral. Em uma concepção tradicional, a confiança poderia ser representada como uma relação vertical: a instituição afirma que o processo é seguro e a sociedade confia. No modelo contemporâneo de auditabilidade, a relação pode ser representada de outra forma: a segurança técnica abre possibilidade de fiscalização, que produz evidências, as quais admitem verificação por terceiros e, só então, sustentam a confiança. Não se trata de eliminar a confiança institucional. A Justiça Eleitoral continua exercendo função central na organização das eleições. A diferença está em permitir que a confiança seja apoiada por mecanismos verificáveis. Essa mudança é especialmente relevante para sistemas tecnológicos complexos. A sociedade não precisa compreender integralmente o funcionamento de cada componente criptográfico para reconhecer que existem mecanismos de verificação. Da mesma forma, um cidadão não precisa ser especialista em tecnologia para compreender que o resultado de uma seção pode ser registrado no Boletim de Urna e posteriormente comparado com o resultado da totalização. A legitimidade democrática é fortalecida quando o cidadão dispõe de meios para conferir, direta ou indiretamente, evidências produzidas pelo próprio processo eleitoral.

11 COMPLEXIDADE, COMUNICABILIDADE E DESINFORMAÇÃO

11.1 O PARADOXO DA SEGURANÇA: MAIS TECNOLOGIA, MAIS COMPLEXIDADE

Existe, contudo, um problema fundamental. A evolução tecnológica aumenta a segurança, mas também aumenta a complexidade. Conceitos como criptografia assimétrica, assinatura digital, *hash*, cadeia de confiança, compilação, autenticação de *software*, *logs* e mecanismos de verificação não são intuitivos para grande parte da população. Surge, assim, um paradoxo: a segurança pode ser tecnicamente verificável e, simultaneamente, socialmente pouco compreendida. Essa diferença ajuda a explicar por que a existência de mecanismos de auditoria não elimina automaticamente questionamentos sobre o sistema. Uma instituição pode demonstrar tecnicamente determinado procedimento e, ainda assim, encontrar dificuldades para convencer grupos que já não reconhecem aquela instituição como fonte legítima de informação. A questão deixa de ser exclusivamente tecnológica. Torna-se comunicacional e política.

11.2 A DIMENSÃO INTERACIONAL DO PARADOXO

O paradoxo não se esgota no plano do discurso. Ele se materializa no ponto exato em que o sistema encontra o eleitor: a interface. A área de Interação Humano-Computador oferece, nessa ordem de ideias, um arcabouço teórico que o debate jurídico-eleitoral brasileiro ainda não incorporou de modo sistemático, embora a preocupação não seja nova entre nós, con-

forme apontam Edoardo Leitão Nogueira e Ingrid Teixeira Monteiro (2025) ao assinalarem os estudos de ergonomia cognitiva conduzidos por Cybis e Michel no final da década de 1990, que já analisavam a adequação do equipamento ao repertório do eleitor.

Em investigação sobre o modelo UE2022, conduzida com o Método de Inspeção Semiótica e o Método de Avaliação da Comunicabilidade, ambos oriundos da Engenharia Semiótica, os autores identificaram atritos de interface e rupturas comunicativas capazes de induzir erro de votação e de alimentar desconfiança subjetiva no instante mesmo do exercício do sufrágio. Um exemplo é ilustrativo: o eleitor que digita número inexistente com o propósito deliberado de anular o voto recebe a mensagem de teor culpabilizante "NÚMERO ERRADO", que atribui falha a quem exerceu escolha legítima. O desconforto cognitivo produzido não decorre de defeito de segurança, mas de decisão de projeto comunicacional.

As propostas de redesenho sistematizadas naquele estudo têm baixo custo e alto retorno em legitimidade percebida: barra de progresso que situe o eleitor na sequência de cargos, retorno sonoro diferenciado em todas as teclas e permanência do intérprete de Libras nas telas críticas. Nenhuma delas altera a arquitetura de segurança descrita nas seções 4 a 9. Todas alteram a experiência a partir da qual o eleitor formará seu juízo sobre o sistema.

Espraia-se daí uma consequência para a agenda comunicacional referida ao final deste estudo. Ela não se resume à divulgação institucional de mecanismos já existentes. Começa no desenho da interface, porque é ali (e não no sítio eletrônico do Tribunal) que a maioria absoluta dos eleitores efetivamente interage com o sistema eletrônico de votação.

11.3 DESINFORMAÇÃO, CONTESTAÇÃO ELEITORAL E AMBIENTE DIGITAL

Quanto mais sofisticada é a arquitetura técnica de segurança, maior pode ser a dificuldade de traduzi-la em uma linguagem socialmente compreensível. A expansão das plataformas digitais modificou profundamente a circulação de informações eleitorais. Pesquisas empíricas identificaram conteúdos de contestação eleitoral disseminados em diferentes plataformas, incluindo Facebook, Twitter e YouTube, com presença de argumentos conspiratórios e questionamentos sobre a segurança e a transparência das eleições (Dourado; Almeida; Piaia, 2024). A literatura recente também demonstra que a desinformação eleitoral passou a constituir objeto relevante de investigação acadêmica no Brasil, especialmente após as eleições de 2018, 2020 e 2022 (Alencar; Jesus-Silva; Teixeira, 2025). O fenômeno apresenta uma característica particularmente importante para o debate sobre a urna eletrônica. A contestação nem sempre se estrutura em torno de uma demonstração empírica de fraude. Em determinadas situações, a narrativa desloca a discussão para a possibilidade abstrata de que uma fraude poderia ocorrer. Essa diferença é fundamental. Há uma distinção entre: a) possibilidade teórica de uma vulnerabilidade; b) existência concreta de uma vulnerabilidade; c) possibilidade prática de exploração; d) capacidade de alteração do resultado; e) evidência de que a vulnerabilidade foi efetivamente explorada. A confusão entre essas categorias pode transformar uma possibilidade hipotética em uma afirmação factual de fraude. Em sistemas complexos, a pergunta cientificamente adequada não é se existe alguma possibilidade teórica de falha, mas quais riscos existem, quais barreiras foram construídas, quais mecanismos permitem detectar problemas e quais evidências existem sobre eventual exploração.

11.4 A DESINFORMAÇÃO E A INVERSÃO DO ÔNUS DA PROVA

Um dos desafios contemporâneos consiste na mudança da natureza da contestação. Em vez de apresentar evidências de que uma fraude ocorreu, determinadas narrativas podem partir da afirmação de que o sistema precisa provar ser absolutamente impossível de fraudar. Essa exigência é problemática do ponto de vista epistemológico. Nenhum sistema

tecnológico complexo pode ser apresentado como absolutamente imune a qualquer hipótese teórica de ataque. A segurança é uma questão de risco, controles, barreiras, detecção, resposta e capacidade de recuperação. Por isso, uma discussão racional sobre o sistema eletrônico de votação deve considerar evidências concretas e procedimentos verificáveis. A distinção entre vulnerabilidade, exploração e fraude efetiva é, portanto, essencial para qualificar o debate público.

12 VOTO IMPRESSO, INDEPENDÊNCIA DE SOFTWARE E VERIFICABILIDADE FIM A FIM

12.1 O COMPROVANTE IMPRESSO DE VOTAÇÃO: UMA HIPÓTESE E SEUS CUSTOS TÉCNICOS

A inversão do ônus da prova examinada na seção anterior encontrou tradução legislativa recorrente na proposta de comprovante impresso conferível pelo eleitor. A trajetória normativa é conhecida: o art. 59-A da Lei n. 9.504/1997, incluído pela Lei n. 13.165/2015, teve a eficácia suspensa por medida cautelar em 06.06.2018 e foi declarado inconstitucional pelo Supremo Tribunal Federal no julgamento de mérito da ADI 5889, concluído em setembro de 2020, por risco ao sigilo e à liberdade do voto. Em agosto de 2021, proposta de emenda constitucional com objeto equivalente não alcançou, na Câmara dos Deputados, o quórum de três quintos. A literatura de comunicação política demonstra que o tema operou menos como controvérsia técnica e mais como significante de desconfiança eleitoral mobilizado no debate parlamentar e nas redes (Oliveira, 2023; 2025).

Convém, ainda assim, verticalizar o exame técnico, que não se resume ao custo orçamentário. São quatro as ordens de limitação apontadas por Larissa Fontenelle Barbosa (2025).

A primeira é um paradoxo de dependência. Confiar na cédula impressa exige confiar que a urna a imprimiu fielmente. A auditoria continua, portanto, dependente do mesmo *software* cuja integridade se pretendia dispensar. O papel desloca o problema; não o elimina.

A segunda é a reconciliação. Havendo divergência entre o resultado eletrônico e a contagem das cédulas, uma das duas fontes há de prevalecer. Se prevalecer o registro digital, a impressão é ineficaz. Se prevalecer o papel, abre-se janela para fraude de varejo: subtração ou inserção de cédulas em seções determinadas, com potencial de anular urnas em locais selecionados por critério político. A regra de precedência precisa ser definida *ex ante* e, em qualquer das hipóteses, produz efeito indesejado.

A terceira é o sigilo. Falhas mecânicas de impressão e atolamento de papel térmico expõem a escolha do eleitor: precisamente a ratio *decidendi* acolhida na ADI 5889.

A quarta é a judicialização. A duplicidade de registros multiplica hipóteses de impugnação e tende a prolongar a proclamação de resultados apertados, com custo direto para a estabilidade do ciclo eleitoral. Trata-se de experiência já vivida, por exemplo, pelos Estados Unidos da América, onde a controvérsia sobre recontagem de votos na eleição na Flórida, nas eleições presidenciais de 2000, foi levada à Suprema Corte1.

Nada disso significa que a demanda por verificação independente seja ilegítima. Ela é, ao contrário, tecnicamente pertinente, e a subseção seguinte examina os caminhos que a literatura especializada oferece para atendê-la. O que a análise afasta é a equação direta entre papel e confiabilidade.

12.2 VERIFICABILIDADE FIM A FIM E OS LIMITES DO *BLOCKCHAIN*

O debate público brasileiro consolidou-se em torno de um binômio redutor: registro puramente digital ou comprovante impresso. A literatura internacional trabalha com uma latitude bem mais ampla.

A via mais desenvolvida é a verificabilidade fim a fim (*end-to-end verifiability*), que emprega criptografia homomórfica e comprovantes cifrados para permitir que o eleitor confira se seu voto foi registrado e computado, sem revelar em quem votou e sem poder demonstrar a terceiros o conteúdo da escolha (propriedade essencial contra coação e compra de votos). O sistema STAR-Vote, concebido por pesquisadores e pela administração eleitoral do condado de Travis, no Texas, é um dos desenhos acadêmicos de maior circulação (Bell *et al*., 2013). Registre-se, contra leituras apressadas, que o STAR-Vote não dispensa o papel: combina interface de registro direto, trilha física e auditoria de risco limitado. Não se trata, pois, de alternativa ao voto impresso, mas de arquitetura em que o papel cumpre função estatisticamente definida.

Outrossim, propostas de votação sobre *blockchain* ganharam circulação no Brasil sob a promessa de descentralizar o registro e dispensar a confiança em qualquer autoridade central. Uma das avaliações técnicas de maior circulação é restritiva: pesquisadores do *Massachusetts Institute of Technology* demonstram que o *blockchain* não resolve nenhuma das vulnerabilidades estruturais do voto remoto e agrega outras. Coação doméstica e compra de voto permanecem intactas fora do ambiente controlado da seção; o dispositivo do eleitor continua exposto a comprometimento anterior ao registro na cadeia; a perda ou o furto de chaves privadas produz desabilitação ou personificação indetectáveis; e falhas de escala assumem, nesse arranjo, dimensão nacional (PARK *et al*., 2021).

Há, por fim, uma advertência que reconduz ao paradoxo examinado na seção 11. Nenhum desses desenhos produz confiança social por si. A verificabilidade matemática que o eleitor não compreende, não exerce e não sabe que existe permanece, do ponto de vista da legitimidade, indistinguível da confiança vertical que se pretendia substituir. O ganho criptográfico não dispensa o trabalho comunicacional; torna-o mais exigente.

12.3 UMA DIVERGÊNCIA DE AVALIAÇÃO

Convém registrar, ao fim desta seção, que a suficiência dos mecanismos atualmente disponíveis constitui objeto de divergência. Parcela da produção em segurança computacional sustenta que apenas arranjos dotados de independência de *software* ofereceriam garantia estrutural quanto à correspondência entre o resultado apurado e a vontade manifestada, razão pela qual Appel, DeMillo e Stark (2020) defendem o registro conferível pelo eleitor associado a auditoria de risco limitado, e não a simples impressão do voto depositada em urna de lona.

O presente estudo adota posição diversa. Entende que o conjunto de barreiras, registros e procedimentos descritos nas seções 4 a 9, operando de modo articulado e distribuído ao longo de todo o ciclo eleitoral, produz patamar de verificabilidade suficiente para sustentar a legitimidade do resultado, sem prejuízo do aperfeiçoamento contínuo que a própria arquitetura comporta e que sua trajetória de três décadas documenta.

A divergência é de avaliação, não de descrição. Há convergência quanto aos mecanismos existentes e quanto ao que cada um demonstra, nos termos da tipologia proposta na seção 10; o dissenso recai sobre o patamar de garantia que deles decorre e sobre o que se deve exigir de um sistema eleitoral em democracia de dimensões continentais. Explicitar o ponto exato do desacordo afigura-se preferível a dissimulá-lo, e a isso se presta o registro ora consignado.

13 AUDITABILIDADE E LEGITIMIDADE DEMOCRÁTICA

A legitimidade democrática não decorre exclusivamente da vitória eleitoral. Ela depende também da percepção de que a competição ocorreu segundo regras previamente conhecidas, que os votos foram contabilizados de maneira íntegra e que os resultados podem ser submetidos a mecanismos de fiscalização. Por essa razão, segurança e auditabilidade possuem dimensão política. Um sistema tecnicamente seguro, mas inacessível à fiscalização, poderia enfrentar problemas de legitimidade. Da mesma forma, um sistema amplamente auditável pode enfrentar uma crise de confiança caso suas evidências sejam desconhecidas, mal compreendidas ou deliberadamente descontextualizadas. A legitimidade exige, portanto, uma combinação de: integridade técnica + fiscalização + transparência + comunicação + confiança institucional. A experiência brasileira demonstra que a auditoria não é uma atividade concentrada em determinado momento. Ela começa antes da eleição, com a especificação e inspeção dos sistemas; passa pelo Teste Público de Segurança; continua na compilação, assinatura digital e lacração; prossegue na preparação das urnas; alcança o dia da votação, com os Testes de Autenticidade e Integridade; e continua depois da votação, com a conferência dos boletins, registros e resultados. É essa continuidade que permite caracterizar o sistema como uma arquitetura de auditabilidade.

Uma contribuição possível desta análise consiste em compreender a segurança eleitoral não como atributo isolado da urna, mas como resultado da interação entre diferentes mecanismos, distribuídos pelas três categorias delineadas na seção 9. Esse conjunto não elimina o risco tecnológico. O que ele faz é distribuir o risco, ampliar as possibilidades de detecção e multiplicar as oportunidades de fiscalização, característica que aproxima a segurança eleitoral da estabilidade democrática.

CONSIDERAÇÕES FINAIS

Ao completar três décadas, o sistema eletrônico de votação brasileiro apresenta uma arquitetura de segurança significativamente mais complexa do que aquela existente na primeira geração da urna eletrônica. A evolução ocorreu em diferentes dimensões: *hardware*, *software*, criptografia, autenticação, biometria, fiscalização, auditoria, transparência e produção de evidências. O desenvolvimento dos mecanismos de segurança foi acompanhado por uma progressiva institucionalização da auditabilidade. O código-fonte passou a ser disponibilizado para fiscalização; entidades externas passaram a participar do processo; testes públicos passaram a procurar vulnerabilidades; sistemas passaram a ser assinados e lacrados; urnas passaram a ser submetidas a testes de integridade e autenticidade; e documentos como a zerésima, o Boletim de Urna e o Registro Digital do Voto passaram a produzir elementos adicionais de conferência. A principal conclusão deste estudo é que o sistema eletrônico de votação brasileiro não deve ser compreendido apenas como uma tecnologia destinada à coleta e contabilização de votos. Ele constitui uma arquitetura institucional de segurança, fiscalização e verificabilidade. Essa conclusão permite estabelecer uma distinção importante entre segurança e confiança. A segurança pode ser construída por mecanismos técnicos. A auditoria pode produzir evidências. A transparência pode permitir acesso e fiscalização. Entretanto, a confiança social depende também da capacidade de essas evidências serem compreendidas e reconhecidas. É nesse ponto que se encontra o principal desafio para as próximas décadas. A desinformação digital pode não depender da demonstração de uma fraude concreta. Em determinadas circunstâncias, sua eficácia política está relacionada à produção permanente de dúvida sobre a possibilidade de fraude. A resposta institucional, portanto, não pode limitar-se à afirmação de que o sistema é seguro. É necessário demonstrar como a segurança é construída, quais mecanismos podem ser fiscalizados, quais evidências são produzidas e como terceiros podem verificar os resultados. A experiência dos 30 anos do sistema eletrônico de votação brasileiro indica, assim, uma transição da confian-

ça baseada predominantemente na autoridade institucional para uma confiança apoiada na verificabilidade. Essa transformação não significa que a confiança institucional perdeu importância. Ao contrário, instituições eleitorais independentes permanecem indispensáveis. O que se modifica é a natureza da relação entre instituição e sociedade: a autoridade passa a ser acompanhada por mecanismos de fiscalização e produção de evidências. Nesse sentido, a auditabilidade constitui uma ponte entre a segurança tecnológica e a legitimidade democrática. Reconhecer limites não é enfraquecer o sistema. É condição do próprio discurso de verificabilidade. Uma instituição que apresenta seus mecanismos como imunes a qualquer objeção adota, no plano retórico, a mesma estrutura de autoridade que a arquitetura de auditabilidade veio superar. A preservação dessa legitimidade para as próximas décadas dependerá, portanto, de duas agendas complementares. A primeira é tecnológica: continuar aperfeiçoando *hardware*, *software*, criptografia, testes e mecanismos de auditoria. A segunda é comunicacional: tornar esses mecanismos compreensíveis, acessíveis e verificáveis pela sociedade. A democracia não depende apenas de que o processo eleitoral seja seguro. Depende também de que a sociedade consiga reconhecer as razões pelas quais pode confiar em sua integridade.

REFERÊNCIAS

ALENCAR, Marta Thaís; JESUS-SILVA, Thiago Henrique de; TEIXEIRA, Juliana Fernandes. Desinformação na comunicação: a Rede Nacional de Combate à Desinformação. Intercom – **Revista Brasileira de Ciências da Comunicação**, São Paulo, v. 48, e2025111, 2025. DOI: 10.1590/1809-58442025111pt. Disponível em: https://www.revistas.intercom.org.br/index.php/revistaintercom/article/view/5071. Acesso em: 20 out. 2026.

APPEL, Andrew W.; DeMILLO, Richard A.; STARK, Philip B. Ballot-marking devices cannot ensure the will of the voters. **Election Law Journal: Rules, Politics, and Policy**, v. 19, n. 3, p. 432-450, 2020. DOI: 10.1089/elj.2019.0619.

ARANHA, Diego F.; KARAM, Marcelo Monte; MIRANDA, André de; SCAREL, Felipe. **Vulnerabilidades no software da urna eletrônica brasileira**. Brasília, DF: [s. n.], 2013. Disponível em: https://archive.org/details/vulnerabilidades_urna_eletronica_brasileira. Acesso em: 20 out. 2026.

BARBOSA, Larissa Fontenelle de Mendonça. O voto impresso no Brasil: limitações técnicas e práticas. **Justiça Eleitoral em Debate**, v. 15, n. 2, 2025. Disponível em: https://revista.tre-rj.jus.br/rjed/article/view/211. Acesso em: 8 set. 2026.

BELL, Susan et al. STAR-Vote: a secure, transparent, auditable, and reliable voting system. **USENIX Journal of Election Technology and Systems (JETS)**, v. 1, n. 1, p. 18-37, ago. 2013.

BRASIL. **Lei n. 4.737, de 15 de julho de 1965**. Institui o Código Eleitoral. Diário Oficial da União, Brasília, DF, 19 jul. 1965.

BRASIL. **Lei n. 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Diário Oficial da União, Brasília, DF, 1 out. 1997.

BRASIL. **Lei n. 13.165, de 29 de setembro de 2015**. Altera as Leis n. 9.504, de 30 de setembro de 1997, n. 9.096, de 19 de setembro de 1995, e n. 4.737, de 15 de julho de 1965. Diário Oficial da União, Brasília, DF, 29 set. 2015.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 5889/DF**. Relator: Min. Gilmar Mendes. Tribunal Pleno. Julgado em 14 set. 2020. Diário da Justiça Eletrônico, Brasília, DF, n. 238, 28 set. 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5346547. Acesso em: 20 out. 2026.

BRASIL. Tribunal Superior Eleitoral. **Auditoria: entenda o que é e como conduzir**. Brasília, DF: Tribunal Superior Eleitoral, [s.d.].

BRASIL. Tribunal Superior Eleitoral. **Códigos-fonte: do Ciclo de Transparência ao Teste Público da Urna**. Brasília, DF: Tribunal Superior Eleitoral, 2025a.

BRASIL. Tribunal Superior Eleitoral. **Conheça a evolução da urna eletrônica: de 1996 a 2024**. Brasília, DF: Tribunal Superior Eleitoral, 2025b.

BRASIL. Tribunal Superior Eleitoral. **Conheça as principais etapas de transparência e segurança da urna no dia da eleição**. Brasília, DF: Tribunal Superior Eleitoral, 2024a.

BRASIL. Tribunal Superior Eleitoral. **Documentação técnica do software da urna eletrônica - Eleições 2022**. Brasília, DF: Tribunal Superior Eleitoral, 2022.

BRASIL. Tribunal Superior Eleitoral. **Resolução n. 23.673**, de 14 de dezembro de 2021. Dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação. Brasília, DF: Tribunal Superior Eleitoral, 2021. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021. Acesso em: 20 out. 2026.

BRASIL. Tribunal Superior Eleitoral. **Resolução n. 23.758**, de 2 de março de 2026. Altera a Resolução n. 23.673, de 14 de dezembro de 2021, que dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação. Brasília, DF: Tribunal Superior Eleitoral, 2026b. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2026/resolucao-no-23-758-de-2-de-marco-de-2026. Acesso em: 20 out. 2026.

BRASIL. Tribunal Superior Eleitoral. **Resolução n. 23.759**, de 2 de março de 2026. Dispõe sobre a participação das eleitoras e dos eleitores no processo eleitoral. Brasília, DF: Tribunal Superior Eleitoral, 2026c. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2026/resolucao-no-23-759-de-26-de-fevereiro-de-2026. Acesso em: 20 out. 2026.

BRASIL. Tribunal Superior Eleitoral. **Teste Público de Segurança dos Sistemas Eleitorais**. Brasília, DF: Tribunal Superior Eleitoral, 2025c.

DOURADO, Tatiana; ALMEIDA, Sabrina; PIAIA, Victor. Fraude nas urnas e contestação eleitoral no Brasil: análise multiplataforma de atores políticos, viés conspiratório e moderação de conteúdo. **Opinião Pública**, Campinas, v. 30, 2024.

MARCACINI, Augusto Tavares Rosa; BARRETO JUNIOR, Irineu Francisco. Aspectos jurídicos, políticos e técnicos sobre sistemas eletrônicos de votação e a urna eletrônica. **Revista Brasileira de Estudos Políticos**, Belo Horizonte, n. 118, p. 97-149, jan./jun. 2019.

NOGUEIRA, Edoardo Leitão; MONTEIRO, Ingrid Teixeira. Uma avaliação da comunicabilidade da Urna Eletrônica brasileira. In: **XXIV Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais (IHC 2025)**, Belo Horizonte, Minas Gerais. Trilha: ideias inovadoras e resultados Emergentes.

OLIVEIRA, Ana Carolina Nunes de. Democracia, populismo e discurso do voto impresso no Brasil. **Dados – Revista de Ciências Sociais**, 2023.

OLIVEIRA, Ana Carolina Nunes de. A PEC do voto impresso nos discursos parlamentares e nas redes sociais: comunicação política e desconfiança eleitoral. **Opinião Pública**, 2025.

PARK, Sunoo; SPECTER, Michael; NARULA, Neha; RIVEST, Ronald L. Going from bad to worse: from Internet voting to blockchain voting. **Journal of Cybersecurity**, v. 7, n. 1, tyaa025, 2021.

RIVEST, Ronald L. On the notion of “software independence” in voting systems. **Philosophical Transactions of the Royal Society A**, v. 366, n. 1881, p. 3759-3767, 2008. DOI: 10.1098/rsta.2008.0149.