



Às vésperas de mais 155 milhões de eleitores irem às urnas, elas são as estrelas pelo protagonismo do Brasil. O sistema é totalmente informatizado, permitindo que a votação ocorra em poucos minutos e o resultado revelado no mesmo dia

Eletrônica, segura e rápida

» IAGO MAC CORD
» RENATO SOUZA

Às vésperas das eleições, uma das estrelas chega à maturidade. Ao completar três décadas de existência em 2026, a urna eletrônica, legitimamente brasileira, consolidou-se como a espinha dorsal da soberania popular no país, transformando um sistema outrora vulnerável a manipulações em um dos processos eleitorais mais ágeis e seguros do mundo. O equipamento, que estreou nas eleições municipais de 1996, utilizado por cerca de 30% do eleitorado, alcançou a marca de 100% de informatização apenas quatro anos depois, culminando na realização do maior pleito informatizado do planeta.

Essa revolução tecnológica não apenas extinguiu fraudes manuais históricas, mas também posicionou o Brasil como uma referência global de ponta, com a tecnologia de votação eletrônica sendo utilizada ou inspirando sistemas em ao menos 33 outros países. As eleições são totalmente informatizadas. Em outubro, mais de 155 milhões de brasileiras e brasileiros irão às urnas para eleger presidente da República, governadores, senadores, deputados federais e deputados estaduais e distritais: o 1º turno será em 4 de outubro, enquanto eventual 2º turno vai ser no dia 25 do mesmo mês.

A elaboração da tecnologia é resultado de um esforço conjunto de engenharia e vontade política que ganhou forma em 1995, durante a gestão do ministro Carlos Velloso na presidência do Tribunal Superior Eleitoral (TSE). Executado por um grupo multidisciplinar de especialistas que ficou conhecido como “os ninjas”, o projeto reuniu talentos do Instituto Nacional de Pesquisas Espaciais (Inpe), Instituto Tecnológico de Aeronáutica (ITA) e do então Centro Técnico Aeroespacial (CTA) para projetar

um equipamento robusto, seguro e capaz de operar nos locais mais remotos do território nacional.

Modelo

Partindo do modelo da urna eletrônica de 1996 (UE96), que opera com modestos 2 megabytes de memória e utilizava disquetes, o sistema evoluiu para equipamentos altamente sofisticados, protegidos por camadas de criptografia, assinaturas digitais e sistemas de verificação constantes.

A urna tinha uma missão clara: encerrar a era das intervenções humanas desonestas no processo eleitoral. Antes da digitalização, as eleições eram marcadas por táticas fraudulentas como as “urnas grávidas” (preenchidas com votos antes do início do pleito), o roubo e a substituição de urnas de lona e a manipulação manual durante a contagem em que os apuradores preenchiam votos em branco com canetas de cores específicas.

A segurança do equipamento é garantida por um ecossistema de auditoria que atua antes, durante e após a votação. No ano anterior às eleições, o Ministério Público Eleitoral (MPE) e outras entidades fiscalizadoras acompanham desde a análise dos códigos-fonte até a cerimônia de lacração dos sistemas em setembro, quando os softwares são assinados digitalmente e tornam-se inalteráveis. Um fator crucial de isolamento é que as urnas não possuem conexão com a internet, o que as protege de ataques cibernéticos remotos.

Reconhecimento

Apesar do reconhecimento internacional e da robustez técnica, a urna eletrônica ocorre em um cenário de divisão na opinião pública brasileira. Dados de uma pesquisa da Genial/Quaest, divulgada em fevereiro, indicam que 53% dos brasileiros confiam no sistema,

Minervino Júnior/CB/D.A.Press



São realizados vários testes para verificar eventuais falhas e erros, buscando a correção imediata

enquanto uma fatia significativa de 43% manifesta desconfiança.

Esse ceticismo é atribuído por parlamentares, como a senadora Damare Alves (República-DF), a uma combinação de baixo letramento digital da população e ao reflexo de fraudes ocorridas em outras esferas digitais, como no Instituto Nacional do Seguro Social (INSS), que geram um receio infundado de vulnerabilidade no voto. No campo legislativo, esse debate se reflete em projetos que propõem o voto impresso como um mecanismo adicional de conferência.

Segurança

É nesse cenário de debate que as especificidades técnicas do sistema ganham relevância. O Brasil é alvo de bilhões de ataques cibernéticos todos os anos. São

investidas contra sites do governo, páginas de internet, sistema bancário ou fraudes mais simples, como o envio falso de boletos para que vítimas façam pagamentos pensando se tratar de uma dívida legítima. Esses alvos têm em comum os sistemas on-line. A principal vantagem da urna eletrônica é que os equipamentos não estão em rede, ou seja, não são conectados à internet. Os votos são capturados e processados por um software 100% nacional, desenvolvido pela própria Justiça Eleitoral.

Porém, isso não impediu que uma batalha política fosse travada nos últimos anos em relação à segurança da urna. O sistema eletrônico de votação não é perfeito. A cada eleição, são identificados problemas isolados no hardware e no software da urna, gerando a troca de equipamentos.

Nas últimas eleições gerais,

em 2022, de acordo com o Tribunal Superior Eleitoral (TSE), foram substituídas 3,2 mil urnas, que apresentaram defeitos irreparáveis durante a votação no primeiro turno. Apenas em Marabá, no Pará, foi necessária a adoção de votação manual, em urna de pano com a coleta de voto em cédula de papel. Como não existe conexão com a internet, um ataque que gere danos em massa ao sistema de coleta dos votos é improvável.

Outra hipótese é uma tentativa de ataque ocorrer contra o sistema de totalização dos votos, que conta com diversas camadas de segurança, e usa servidores da Justiça Eleitoral para receber e processar os dados. Em 2018, uma ameaça gerou um inquérito da Polícia Federal, que concluiu que não houve nenhum tipo de alteração nem ameaça à segurança e ao sigilo.

Revolução tecnológica sem igual

» CAETANO YAMAMOTO*
» PEDRO JOSÉ*

A revolução causada pela urna eletrônica é celebrada por especialistas que acompanham o processo eleitoral em todas suas nuances. De acordo com eles, a informatização das eleições é um avanço sem igual, eliminando ameaças, riscos e suspeitas de fraudes. Também contribuiu para a agilidade no momento da votação e no resultado final, além de evitar perdas e prejuízos.

Para o advogado Luiz Gustavo Cunha, especialista em direito eleitoral, a introdução da urna eletrônica representou um dos maiores avanços institucionais da Justiça Eleitoral brasileira.

“Além da celeridade, a informatização fortaleceu a segurança do processo eleitoral ao incorporar mecanismos de auditoria, assinaturas digitais, boletins de urna, registro digital do voto e testes públicos de segurança, permitindo que partidos políticos, Ministério Público, Ordem dos Advogados do Brasil (OAB), Polícia Federal, universidades e entidades fiscalizadoras acompanhem diferentes etapas do processo”, afirma.

Jéfferson Campos Nobre, membro senior do Instituto de Engenharia Elétrica e Eletrônica (IEEE), reitera os aspectos técnicos operacionais da urna, que tornou o processo de votação mais rápido, padronizado, acessível e seguro.

“Muito além do equipamento utilizado nas seções eleitorais, a engenharia está presente em toda a estrutura do sistema brasileiro de votação: do desenvolvimento e da atualização contínua do hardware à criptografia dos dados, passando pelo armazenamento seguro, pela transmissão das informações e pela auditoria pública”, ressalta

Luiz Roberto/TSE



Recentemente, o Tribunal Superior Eleitoral (TSE) firmou parceria com plataformas digitais para combate à divulgação das fake news

Sistema próprio

O avanço tecnológico atingiu o ponto em que a urna tem um próprio sistema operacional — o Uenux, baseado em Linux —, que permite modernizações constantes, tornando o equipamento cada vez mais seguro.

Segundo Nobre, a urna eletrônica possui um chip físico de segurança singular que atua em conjunto com o sistema interno para criar chaves criptográficas capazes de impedir ataques ou fraudes.

“A urna eletrônica brasileira é resultado da integração entre engenharia eletrônica, computação, telecomunicações e segurança da informação. Trata-se de uma tecnologia desenvolvida especificamente para o Tribunal Superior Eleitoral e constantemente atualizada”, afirma Nobre.

O sistema da urna assegura, por exemplo, o sigilo do voto. Os votos são armazenados de forma embaralhada, impedindo qualquer associação entre o eleitor e a escolha registrada. “O transmitido não são votos individuais, mas os totais

consolidados do boletim de urna, somados automaticamente. Isso garante tanto a agilidade da apuração quanto a preservação do sigilo”, explica Nobre.

Além da segurança tecnológica, a Constituição assegura que, no dia da eleição, ao votar, é proibido o ingresso na cabine de votação portando aparelho celular ou qualquer outro equipamento que possa registrar o voto. Essa proibição foi incluída na Lei das Eleições em 2009 e se encontra em vigor desde então.

Voto ser sigiloso e liberdade de expressão não estão dissociados. No dia da votação, o cidadão pode manifestar apoio a partidos e candidatos. Contudo, o voto é um direito de cada pessoa e deve ser exercido de forma secreta para a escolha dos representantes políticos.

Segundo o advogado Luiz Gustavo Cunha, o sigilo do voto não existe apenas para proteger a privacidade individual do eleitor, mas é uma garantia constitucional “destinada a assegurar a liberdade de escolha e impedir qualquer forma

de coação”, como compra de votos ou intimidação.

Desafios

O avanço acelerado das tecnologias digitais traz novos desafios, entre eles o uso crescente de deepfakes e campanhas de desinformação nas redes sociais, como a disseminação de conteúdos manipulados por inteligência artificial tornou-se um dos principais riscos contemporâneos aos processos democráticos. Esse movimento é uma ameaça, pois a velocidade de propagação nas mídias sociais e a dificuldade de identificar os responsáveis tornam esse cenário extremamente complexo. “Mas a própria tecnologia também é uma aliada no combate à desinformação”, afirma Nobre. As ferramentas baseadas em inteligência artificial conseguem detectar comportamentos suspeitos, identificar campanhas coordenadas e auxiliar equipes técnicas na resposta a incidentes cibernéticos.

O especialista em crimes cibernéticos, Rodrigo Fragola, diz que a desinformação hoje não é apenas um

problema de tecnologia, mas também de comportamento humano.

“O combate passa por uma estratégia em camadas: plataformas mais ágeis para identificar campanhas coordenadas, uso de IA para detectar conteúdos sintéticos, rastreabilidade da origem do conteúdo, atuação rápida da Justiça Eleitoral quando houver abuso e, principalmente, educação digital para que o eleitor aprenda a verificar a procedência da informação antes de compartilhá-la.”

O especialista frisa que a desinformação é um componente que deve ser considerado, sobretudo porque tenta influenciar a percepção das pessoas antes mesmo de o voto ser registrado.

“O mais correto é dizer que o sistema eleitoral brasileiro possui múltiplas camadas de proteção, auditoria e melhoria contínua, enquanto a desinformação se tornou um desafio crescente porque explora vulnerabilidades humanas e sociais, e não necessariamente tecnológicas.”

*Estagiários sob supervisão de Rosana Hessel

Fiscalização contínua

Antes de cada pleito, a urna e seus sistemas passam por testes públicos de segurança, que podem ser acompanhados por partidos e entes públicos, assim como pela imprensa. Especialistas testam uma série de ataques, para avaliar a segurança do equipamento. Das vulnerabilidades identificadas nos testes de 2025, todas foram corrigidas para a votação deste ano, de acordo com o Tribunal Superior Eleitoral (TSE).

O advogado e especialista em direito eleitoral Renato Ribeiro, doutor em direito do Estado pela Faculdade de Direito da Universidade de São Paulo (USP), destaca que há uma diferença entre problemas técnicos e ataques. Segundo ele, questões técnicas não comprometem o resultado da votação.

“Problema técnico na urna, por si só, não significa fraude nem anula automaticamente a eleição. Troca-se a urna, preservam-se os votos nela já contidos se a votação já tiver sido iniciada. No limite, adota-se a votação em papel”, destaca o especialista.

Preservação

De acordo com Ribeiro, a legislação eleitoral tem mecanismos de contingência para preservar o exercício do voto: a ocorrência deve ser imediatamente comunicada à mesa receptora, registrada em ata, levada ao juiz eleitoral e tratada segundo as providências técnicas disciplinadas pela Justiça Eleitoral.

“Se houver ataque, coação, tumulto, impedimento de acesso ao local de votação ou qualquer forma de constrangimento ao eleitor, o caso deixa de ser apenas operacional e passa a exigir atuação imediata do juiz eleitoral, das forças de segurança e, se necessário, da própria Justiça Eleitoral em grau regional ou superior”, reitera. “Se ficar demonstrado que a irregularidade afeta a liberdade do voto, o sigilo, a fiscalização ou a normalidade da votação, a Justiça Eleitoral pode determinar a apuração das responsabilidades, anular a votação atingida e, nos casos mais graves, convocar nova votação ou nova eleição.”

Um ano antes dessas eleições, houve teste público para verificação da segurança das urnas. Após a avaliação, o TSE foi categórico: “A segunda etapa do Teste Público de Segurança dos Sistemas Eleitorais (Teste da Urna) de 2025, comprovou, mais uma vez, a segurança do sistema eleitoral brasileiro. No Teste de Confirmação, realizado na sede do Tribunal Superior Eleitoral (TSE), em Brasília, ficou constatado que nenhum dos achados fragilizou o sigilo ou a integridade do voto, que são os pilares do processo eleitoral do país”. (IMC e RS)