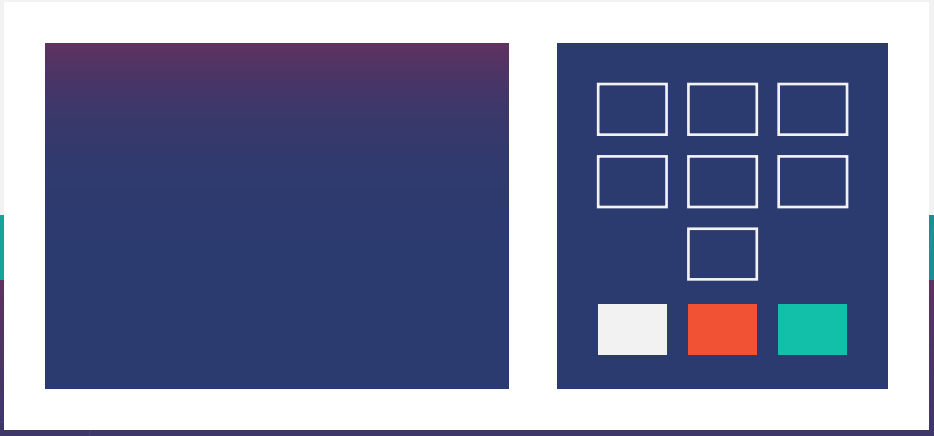
COMO COBRIR CRITICAMENTE A URNA ELETRÔNICA

SEM ALIMENTAR TEORIAS DA CONSPIRAÇÃO



@artigo19
@artigo19
@artigo19
@artigo19brasil
artigo19.org

ARTIGO 19

ARTIGO 19

DEFENDENDO A LIBERDADE DE EXPRESSÃO E INFORMAÇÃO

Dobrando a aposta: uma cobertura crítica da urna eletrônica pode ajudar a fortalecer a democracia 03

Uma pergunta pouco trivial: o que é "urna eletrônica"? 05

Independência de *software*, a urna brasileira e o "voto impresso" 06

Sistemas de votação eletrônicos com registro direto (DRE) 08

O voto eletrônico brasileiro na balança 09

Sistemas VVPAT: da (interessante) teoria à (complexa) prática 11

Auditoria de risco limitado 12

"Voto impresso" no Brasil 13

Dispositivos de preenchimento de cédulas (BMDs) e escâneres 14

Voto online 16

Sistemas com criptografia 17

Projeto Eleições do Futuro 18

Recomendações internacionais 19

Discordar e divergir, sim; afrontar, nunca! 20

DOBRANDO A APOSTA:

UMA COBERTURA CRÍTICA DA URNA ELETRÔNICA PODE AJUDAR A FORTALECER A DEMOCRACIA

Democracia pode ser muita coisa, mas é, acima de tudo, o reconhecimento da existência de desacordos em uma sociedade e, ao mesmo tempo, um acordo para que essas diferenças sejam administradas sem o uso da violência e por meio de um processo aberto à participação de toda a cidadania: as eleições. Esse método implica que derrotas e vitórias políticas são sempre temporárias, pois a cada novo ciclo eleitoral o jogo é disputado novamente. Essa é então a regra fundamental da democracia, ancorada em outro importante pacto social também baseado na mútua confiança: o acordo sobre os procedimentos de votação – principalmente quanto à maneira de registrar, coletar e contar votos.

No entanto, nos últimos anos, em várias partes do mundo, o método democrático tem sido ameaçado. Os roteiros são muito parecidos: candidatos populistas se aproveitam de uma onda inicial de descontentamento e oferecem soluções mágicas e radicais. Uma vez eleitos, tentam subverter o próprio método que os alçou ao poder, como se chutassem a escada pela qual subiram, para que só eles possam permanecer no topo.

Uma das maneiras de chutar a escada é atacar discursivamente o sistema de votação, independentemente de qual seja ele. Assim, se conseguirem emplacar a tese de que esse sistema está corrompido – de que as eleições não são justas, portanto –, populistas constroem um falso argumento para catalisar e justificar sua permanência no poder, corrompendo a democracia.

Mas o fenômeno não é tão simples. Ataques a instituições democráticas, como o processo eleitoral, muitas vezes se valem inicialmente de críticas e discussões pertinentes sobre essas instituições. Além disso, também é comum que um ceticismo e um descontentamento legítimos em relação a elas sejam explorados para que teorias da conspiração possam ser interpretadas como verdadeiras.

O exemplo brasileiro de ataques à urna eletrônica e à Justiça Eleitoral é ilustrativo. Há uma série de críticas sérias à tecnologia de votação usada no Brasil. Também é legítimo e compreensível que, além dessas críticas e de uma insatisfação difusa com a democracia, a arquitetura tecnológica da urna e a maneira como ela vem sendo administrada estejam gerando ceticismo e desconfiança. Mas nada disso exclui a possibilidade de que, ao mesmo tempo, essa situação seja levianamente usada como ingrediente de narrativas conspiratórias, abalando a confiança pública no método democrático e abrindo janelas de oportunidade para investidas autoritárias.

A defesa das instituições democráticas é normalmente a reação mais evidente e factível. Uma defesa empreendida de várias maneiras e por diversos atores e instâncias, mas raramente com o reconhecimento de eventuais falhas ou necessidade de melhorias ou reformas. No caso do jornalismo, muitas vezes essa empreitada é marcada por uma postura, consciente ou não, de alinhamento a versões e narrativas de instituições consideradas democráticas e pelo receio de produção de conteúdo crítico a elas.

No entanto, ainda que essa estratégia possa conter momentaneamente ameaças autoritárias, a confiança nas instituições não é automaticamente restaurada; as críticas e discussões sobre elas tampouco desparecem magicamente. A questão de fundo subsiste, e a democracia que foi protegida pode até continuar intacta – para o bem e para o mal –, mas reproduzindo as condições que haviam gerado forças antidemocráticas.

A **ARTIGO 19 Brasil e América do Sul**, que desde 2020 vem conduzindo pesquisas e atividades sobre tecnologias de votação, acredita que esse é também o caso da urna eletrônica brasileira. Dificilmente a confiança nesse procedimento de votação será resgatada sem que as críticas e discussões sobre ele sejam superadas. Apenas "dobrando a aposta" na democracia é que a situação pode começar a mudar, com o enfrentamento direto e positivo dos principais pontos que têm gerado ceticismo e desconfiança.

A existência de uma imprensa livre e plural e de uma cobertura jornalística crítica podem desempenhar papel importantíssimo nesse processo; por exemplo, fornecendo informações que qualifiquem o debate público, revelando fatos e situações que podem ser o gatilho para aperfeiçoamentos, desmistificando narrativas oficiais.

No entanto, é no mínimo prudente reconhecer que "dobrar a aposta" tem seus riscos. Uma cobertura jornalística nesses termos pode acabar sendo subvertida para alimentar novas teorias conspiratórias, campanhas de desinformação e discursos golpistas. Por isso, o objetivo desta publicação é justamente fornecer informações que possam amparar e fomentar uma cobertura que seja a um só tempo crítica e ousada, mas também equilibrada e consciente da complexidade e delicadeza do tema.

UMA PERGUNTA
POUCO TRIVIAL:

O QUE É "URNA ELETRÔNICA"?

A questão aparentemente tola pode revelar que, no geral, não estamos acostumados com a ideia de que existe mais de um tipo de tecnologia de votação. Dizemos "urna eletrônica" para designar o sistema desenvolvido pela Justiça Eleitoral, usado há quase 30 anos em todas as eleições do país. Mas também empregamos a justaposição das duas palavras para fazer referência a tecnologias de votação adotadas em outros lugares. Conclusão: entre o sentido específico do termo e seu uso expandido, surge a confusão entre espécie – a tecnologia usada no Brasil – e o gênero "voto eletrônico", que compreende vários tipos de arquitetura tecnológica.

Há ainda outra dicotomia de sentidos que costumam ser confundidos: "urna eletrônica" enquanto a máquina na qual digitamos a tecla "confirma" ou como todo o sistema de votação no qual ela está inserida – desde o desenvolvimento do *software* até a totalização dos votos.

Essa multiplicidade de sentidos pode gerar entendimentos imprecisos sobre o assunto. Por exemplo, é comum a afirmação, feita pela própria **Justiça Eleitoral,** de que dezenas de países do mundo usam "urna eletrônica", dando a entender que se trata de apenas um tipo de tecnologia e que, portanto, o Brasil não é um caso isolado. E a clássica máxima de que a urna eletrônica "não é conectada à internet" – o que é incontestavelmente verdadeiro – dá a entender que apenas o equipamento é vulnerável a potenciais ataques, e não outras etapas que fazem parte de todo o processo eletrônico de votação.

Confusões parecidas ocorrem com a expressão "voto impresso", empregada com diferentes sentidos e que, por isso, pode gerar ruídos de comunicação e conclusões equivocadas.

Para que as especificidades de cada arquitetura tecnológica sejam bem compreendidas – portanto, para que análises críticas e ponderadas possam ser feitas a respeito –, é preciso estabelecer premissas comuns sobre os termos mais usados e as tecnologias a que se referem. É o que será feito a seguir. ■

INDEPENDÊNCIA DE *SOFTWARE*, A URNA ELETRÔNICA BRASILEIRA E O "VOTO IMPRESSO"

Antes de expor os principais tipos de voto eletrônico, é importante fixar o conceito de "independência de *software*", pois ele não apenas é útil para diferenciá-los, mas também está por trás das principais discussões sobre segurança de sistemas eletrônicos de votação.

Segundo a definição, "um sistema de votação é independente de *software* se uma modificação ou erro indetectável em seu *software* não puder causar uma modificação ou erro indetectável em um resultado eleitoral".

Em outras palavras, a validade dos resultados gerados por um sistema de votação que tem essa característica não depende do correto funcionamento de seu *software*, mesmo que ele contenha falhas ou adulterações impossíveis de serem descobertas.

Isso porque, se essas falhas ou adulterações não percebidas gerarem um resultado incorreto, necessariamente é possível constatar o problema. Como? Com dados independentes, que não foram gerados pelo próprio *software*. Por exemplo, registros físicos dos votos, que permitem a conferência do resultado por meio da contagem dessas cédulas. Essa arquitetura é chamada de *Voter-Verified Paper Audit Trail* (VVPAT), ou trilha de auditoria por voto verificado e registrado em papel, mais conhecido no Brasil como "voto impresso".

Já em um sistema dependente de *software*, uma modificação ou erro indetectável pode causar uma modificação ou erro também indetectável no resultado eleitoral. Por quê? Porque, de partida, no *software* não se pode confiar, já que erros ou fraudes ficam abaixo do radar, por definição. Restaria então a opção de investigar o resultado produzido por esse sistema. Mas, se não existirem informações que não tenham relação com o *software* – um segundo conjunto de registros criados de forma independente –, então conceitualmente será impossível saber se esse resultado está de fato correto. O principal sistema eletrônico com essas características é o de registro direto de votos, ou *Direct-Recording Electronic* (*DRE*) *voting system*. É o modelo usado no Brasil.

Mas por que erros ou alterações no *software* de um sistema eletrônico de votação seriam indetectáveis? Por que essa premissa está embutida no conceito? Rivest e Wack, os autores que o criaram, explicam que os *softwares* usados em eleições são bastante complexos, inclusive porque a necessidade de equilibrar requisitos conflitantes, como sigilo do voto e precisão da contagem final, gera ainda mais complexidade. O código-fonte da tecnologia brasileira, por exemplo, tem dezenas de milhões de linhas. Mesmo um erro pequeno pode gerar uma vulnerabilidade que pode ser explorada por um invasor ou simplesmente produzir um resultado incorreto. "Encontrar todos os erros em um sistema grande é, em geral, considerado impossível ou uma tarefa bastante exigente e extremamente cara", afirmam.

É por esse motivo que parâmetros internacionais sobre sistemas de votação e especialistas em segurança não recomendam o uso de sistemas sem independência de *software* (leia mais a respeito na página 19).

A realidade, no entanto, é mais complexa. Na prática, sistemas VVPAT podem apresentar outras vulnerabilidades, e sistemas DRE podem contornar sua dependência de *software*. É o que veremos na sequência. ■

SISTEMAS DE **VOTAÇÃO ELETRÔNICOS COM REGISTRO DIRETO (DRE)**

Por ser a arquitetura tecnológica implementada no Brasil, as máquinas usadas nesse tipo de sistema também costumam ser chamadas de "urna eletrônica". Sua principal característica é que as escolhas de cada eleitor são registradas direta e eletronicamente na memória instalada em um computador – e apenas nela. Isso quer dizer que não há um suporte "intermediário", físico, no qual a preferência do eleitor é inscrita. Apenas uma interface por meio da qual o voto é composto, como um teclado e uma tela – ou uma tela sensível ao toque. Isso significa que o eleitor não pode ver como exatamente a máquina registrou seu voto, diferentemente de outras tecnologias.

Sistemas DRE são dependentes de *software*, já que não produzem um conjunto de registros autônomos, sem relação com o programa de computador instalado nas urnas, que poderiam ser usados para checagem do resultado.

Urnas eletrônicas não são conectadas à internet. A instalação do *software* é feita fisicamente, com uma mídia de carga. Mas as etapas que antecedem a votação, do desenvolvimento do *software* até a sua instalação, são consideradas por especialistas as mais sensíveis do ciclo eleitoral.

A tecnologia DRE começou a ser usada na década de 1970, nos Estados Unidos; sua disseminação pelo país, no entanto, demorou para acontecer. Em 1980, menos de 1% do eleitorado votou nesses equipamentos, percentual que subiu para 3% em 1988, 5% em 1992, 7% em 1996 e 13% em 2000.

Depois dos problemas na eleição presidencial de 2000 na Flórida envolvendo um sistema de cartões perfuráveis, o uso de máquinas DRE começou a ser incentivado: em 2004, 31% do eleitorado registraram votos usando essa tecnologia, com um pico em 2006 (38%). Mas, com a publicação de alguns estudos e recomendações e a pressão de organizações da sociedade civil e de líderes políticos, autoridades eleitorais têm abandonado esse tipo de sistema. Em 2020, 2,6% dos americanos votaram em jurisdições onde essa tecnologia estava disponível para todos os eleitores. Nas eleições deste ano, o percentual será de 1,4%.

No Brasil, a urna eletrônica foi introduzida nas eleições municipais de 1996, quando os votos de mais de 32 milhões de brasileiros – um terço do eleitorado da época – foram coletados por cerca de 70 mil equipamentos. Quatro anos depois, no pleito de 2000, 100% dos eleitores já votaram usando a nova tecnologia.

As máquinas de registro direto de votos também foram introduzidas na Europa, Ásia e outros países da América do Sul. Na Holanda, foram usadas de 1997 a 2006. A Índia começou a usar máquinas DRE em 1998, com total implementação em 2004. Um estudo publicado em 2010 por oito pesquisadores demonstrou algumas vulnerabilidades do sistema

indiano que poderiam ser exploradas para alterar resultados ou violar o sigilo do voto. Em 2013, uma **decisão** da Suprema Corte do país determinou que o sistema passasse a gradativamente ter o registro físico do voto (sistema VVPAT), processo concluído em 2019.

A Venezuela implementou urnas eletrônicas com registro impresso em 2004, que continua em operação.

Segundo a principal **base de dados** sobre o uso de voto eletrônico no mundo, elaborada pelo Idea (*International Institute for Democracy and Electoral Assistance*), atualmente 18 nações usam sistemas DRE[1]. Mas o Brasil é o único país que adota exclusivamente máquinas sem voto impresso. No demais casos, além de sistemas puramente DRE, também há seções com VVPAT ou outras tecnologias. Além disso, na maioria deles o sistema DRE não é usado em larga escala, como França e Estados Unidos.

1. Embora seja a principal referência no assunto, essa base de dados contém algumas imprecisões e informações desatualizadas.

O VOTO ELETRÔNICO BRASILEIRO NA BALANÇA

Por não ser independente de *software*, o sistema de votação eletrônico brasileiro não segue as principais recomendações internacionais (leia mais na página 19). Mas isso não significa que ele seja inerentemente inseguro ou que existam razões para acreditar que resultados eleitorais incorretos têm sido produzidos.

A validade dos resultados, aqui, tem sido perseguida com outra abordagem: a inspeção do próprio *software* e de seu correto funcionamento, já que não existe um segundo conjunto autônomo de resultados com o qual o resultado gerado eletronicamente possa ser comparado.

É verdade que essa empreitada não é simples, conforme já afirmado. Mas é preciso considerar que o conceito de independência de *software* foi proposto há quase vinte anos. Desde então, a Justiça Eleitoral vem criando novos mecanismos de fiscalização e auditoria, que se complementam mutuamente. Cada um foi concebido para abordar aspectos específicos do sistema. Portanto, isoladamente, não são autossuficientes. Mas, em conjunto, buscam uma blindagem completa. A maior parte desses mecanismos conta com a participação de instituições que fiscalizam as operações e atividades empreendidas pela Justiça Eleitoral, as chamadas "entidades fiscalizadoras[2]".

2. Vide artigo 6º da **Resolução 23.673/2021.**

Em sistemas sem independência de *software*, a transparência é ainda mais importante. Quanto maior, menor a necessidade de que a confiança no resultado dependa exclusivamente da fé depositada na tecnologia e no organismo eleitoral responsável por ela.

Embora avanços ainda sejam importantes, nos últimos anos a Justiça Eleitoral tem aprimorado seu nível de transparência. Por exemplo, o período durante o qual o *software* pode ser inspecionado pelas entidades fiscalizadoras, nas dependências do TSE, passou de seis meses a um ano. E no ciclo eleitoral de 2022, pela primeira vez três instituições passaram a ter acesso aos códigos-fonte fora da sede do tribunal.

Mas não se pode dizer que o código-fonte da tecnologia brasileira é totalmente aberto. O princípio inicial que norteou a concepção do sistema foi o de **"segurança por obscuridade"** – segundo o qual o sigilo evita o comprometimento da segurança –, o que dificulta a divulgação repentina e irrestrita desse código.

Ainda que o código-fonte fosse integralmente aberto, a arquitetura tecnológica usada no Brasil não permite que um eleitor sem conhecimentos altamente especializados consiga fiscalizar o processo eleitoral. Ele precisaria continuar acreditando na *expertise* e idoneidade de terceiros. Mais que isso, esse modelo não permite que o eleitor sequer consiga visualizar diretamente se o seu voto foi corretamente registrado. Esse foi um dos principais motivos que levaram o Tribunal Constitucional da Alemanha a **considerar inconstitucional** o sistema DRE, em 2009. Mesmo que empiricamente um sistema assim tenha níveis de segurança elevadíssimo, é preciso avaliar se a ausência desse tipo de verificabilidade não pode comprometer a confiança dos eleitores nessa tecnologia.

Por outro lado, sistemas puramente DRE impossibilitam o cometimento de fraudes que só podem ser realizadas se houver impressão dos votos, muitas delas associadas a dificuldades em garantir a custódia das urnas físicas, a brechas nos procedimentos analógicos e a condições de segurança pública. Em um país com as características do Brasil e com uma história marcada por inventivas estratégias de fraude eleitoral nos tempos em que não havia voto eletrônico, isso não é nada trivial. ■

SISTEMAS VVPAT: DA **(INTERESSANTE)** TEORIA À **(COMPLEXA)** PRÁTICA

Nesse sistema são utilizadas urnas eletrônicas DRE, mas as escolhas dos eleitores também são impressas em papel, pela própria urna ou por uma impressora acoplada a ela. O objetivo é que, antes de serem depositadas em receptáculos invioláveis, as cédulas preenchidas sejam verificadas pelos votantes. Isso garante, em tese, que os votos impressos contidos em cada urna física estão corretos. Caso seja preciso verificar o resultado gerado pelo sistema eletrônico, é possível compará-lo com o resultado de uma contagem dos votos físicos. Por isso, os sistemas VVPAT são independentes de *software*.

Para além de uma arquitetura tecnológica que, em tese, confere segurança às eleições, sistemas de votação baseados em cédulas físicas, também maximizam outros requisitos eleitorais e democráticos importantes, como a transparência e a verificabilidade.

Mas há nós a serem desatados. Um dos principais diz respeito à possibilidade de que surja uma divergência entre a totalização dos votos eletrônicos e a contagem dos votos em papel. Se isso ocorrer, qual deve prevalecer? Rebecca Mercuri, uma conhecida defensora do "voto impresso" nos Estados Unidos, entende que as vias físicas é que devem gerar o resultado definitivo.

A resposta não é simples, mesmo porque a existência da divergência apenas apontará que ao menos um dos sistemas falhou (ou os dois), mas não revelará qual. Também é preciso considerar que, em lugares onde a garantia da custódia de votos físicos é cronicamente problemática, a totalização resultante dessa contagem dificilmente será confiável.

Sistemas eletrônicos com "voto impresso" também devem conter uma diretriz clara sobre o que deve ocorrer caso algum eleitor afirme que o teor da cédula impressa não coincide com o voto que aparece na tela da urna eletrônica. Em democracias em que segmentos importantes da sociedade e das lideranças políticas parecem dispostos a empreender quaisquer estratégias para ganhar uma eleição, deve-se avaliar o risco de eleitores alegarem uma **falsa divergência,** a fim de deslegitimar o pleito e até justificar golpes.

Outro desafio se refere à maneira pela qual os votos impressos serão contados: normalmente, isso é feito por meio de escâneres ópticos (leia mais a respeito na página 14), que leem as cédulas em papel. Portanto, é um processo que também é realizado por meio de um *software*, ainda que diferente. De algum modo, então, será preciso confiar na tecnologia. Uma maneira para contornar essa questão é a chamada auditoria de risco limitado (veja mais detalhes na página seguinte).

Relacionada a esse ponto está a avaliação sobre a necessidade, ou não, de as vias impressas terem algum código de autenticação para evitar que cédulas inautênticas inseridas nas urnas físicas sejam validadas durante a contagem eletrônica. Mas, considerando que esse código será criado pelo mesmo sistema que registra eletronicamente os votos, a independência de *software* deixa de fazer sentido. Esse é **um dos principais argumentos** usados pelo TSE para refutar a arquitetura VVPAT.

Em relação à verificação feita pelos eleitores, centro gravitacional da confiabilidade do funcionamento do sistema, algumas pesquisas têm apontado que boa parte dos votantes não checa se de fato o voto impresso está correto. Assim, o modelo seria baseado apenas em um voto verificável, mas não necessariamente verificado, mitigando a vantagem teórica da independência de *software*.

Em uma **carta** endereçada em fevereiro de 2022 à Comissão Eleitoral do Senado de Indiana, onde tramita uma proposição para migrar as urnas eletrônicas do estado para o sistema VVPAT, especialistas da organização *Verified Voting* apontaram que a proposta compromete o sigilo do voto[3] e que a comunicação visual das vias impressas dificultaria sua verificação (principalmente por eleitores com deficiência visual). Também sinalizaram que o papel térmico previsto é pouco durável e propenso a desbotar e manchar.

3. Esse foi o principal argumento do STF para declarar a inconstitucionalidade do "voto impresso". Para mais detalhes sobre esse assunto, vá até a página seguinte.

AUDITORIA DE RISCO LIMITADO

Apontado como o método mais confiável para verificação de resultados produzidos por sistemas eletrônicos e registrados em papel, consiste na recontagem manual de apenas uma parte das cédulas físicas. Diferentemente de outras auditorias, que se baseiam em porcentagens fixas, nessa modalidade a amostra é estabelecida a partir de um "limite de risco" pré-estabelecido. Entre outras variáveis, esse limite considera a diferença do número de votos entre os candidatos obtida pelo resultado eletrônico. Em uma eleição em que a vitória aconteceu com folga, o número de cédulas a serem revisadas pode ser muito pequeno. Em uma eleição apertada, esse número será maior, mas muito menor do que a totalidade dos votos.

Em auditorias que se baseiam em percentuais fixos, corre-se o risco de que a amostra seja desnecessariamente grande (caso a vitória tenha ocorrido por larga margem) ou pouco representativa (caso o resultado eletrônico esteja apontando para uma vitória apertada).

Na auditoria de risco limitado, a contagem é manual porque a leitura feita eletronicamente, por escâneres, também é suscetível de fraude ou erro. Isso porque as partes da cédula lidas eletronicamente, como código de barras, podem não corresponder aos caracteres alfanuméricos impressos nela. Ou seja, um humano lerá uma coisa – o voto correto – e a máquina pode ler outra, em caso de erro ou fraude.

“VOTO IMPRESSO” NO BRASIL

O chamado sistema VVPAT chegou a ser aprovado duas vezes pelo Congresso Nacional, em **2009** e **2015.** Mas o Supremo Tribunal Federal (STF) declarou que as leis que os instituíram eram inconstitucionais, em 2013 e **2020,** respectivamente. Nas duas ocasiões, a Corte entendeu que o desenho tecnológico do sistema de “voto impresso” previsto pelos legisladores colocava em risco o sigilo do voto e, portanto, a livre manifestação do eleitor.

Em 2002, uma **lei** instituindo o sistema VVPAT no país já havia sido aprovada, mas o próprio Parlamento **revogou** o dispositivo após o **fracasso** de alguns testes feitos no pleito daquele ano. Como forma de emular o papel que seria desempenhado pelo “voto impresso”, em **2003** foi instituído o “registro digital do voto”.

Uma quarta tentativa de instituir o voto impresso no Brasil ocorreu em 2019, mas por meio de uma proposta de emenda à Constituição **(PEC 135/2019),** numa tentativa parlamentar de superar o entendimento do STF. Mas a proposta acabou sendo **rejeitada** pela própria Câmara dos Deputados. O **último substitutivo** apresentado pelo relator, deputado Filipe Barros (PSL-PR), previa que todos os votos impressos deviam ser contados manualmente, deturpando a arquitetura VVPAT.

Além disso, o assunto foi abordado em um ambiente polarizado, dentro e fora do Parlamento, e de maneira açodada e pouco rigorosa, sem detalhamentos e contextualizações importantes. Pode-se dizer que a pauta foi instrumentalizada pelo Executivo da época e seus aliados para gerar desconfiança sobre o sistema vigente. ■

DISPOSITIVOS DE **PREENCHIMENTO DE CÉDULAS (BMDs) E ESCÂNERES**

Segundo o glossário da última versão das Diretrizes Voluntárias para Sistemas de Votação[4] **(VVSG 2.0),** de 2021, dispositivos de preenchimento de cédulas (ou BMDs, do inglês *Ballot Marking Devices*) são equipamentos que permitem aos eleitores, por meio de uma interface eletrônica, selecionar e rever suas preferências. Os aparelhos imprimem essas escolhas em uma cédula de papel legível por humanos. Esse documento é o único registro de voto produzido pela máquina. **Portanto, o voto não é armazenado eletronicamente – principal diferença entre o sistema DRE e os BMDs.**

A cédula gerada pode mostrar todas as opções daquele pleito, mas com marcações gráficas feitas pela impressora nos espaços correspondentes aos candidatos ou partidos selecionados pelo eleitor. Outros modelos imprimem em uma cédula em branco apenas a lista dos nomes escolhidos. Nos dois casos, as preferências do eleitor também podem ser impressas pelos BMDs acompanhadas de um código de barras ou de um QR Code. Em seguida, as cédulas são lidas e tabuladas por escâneres ópticos.

Atualmente, na maior parte das vezes, essa leitura ocorre na seção eleitoral, quando o próprio eleitor escaneia o seu voto. Em alguns lugares, essas operações são feitas em centrais.

Os escâneres são previamente carregados com informações sobre o pleito (como a lista dos candidatos e o formato das cédulas) e, desse modo, conseguem "interpretar" as cédulas. Assim, quando elas são inseridas, esses equipamentos "leem" os votos, seja escaneando um registro que só as máquinas compreendem (como códigos de barra ou *QR Code*), seja usando a configuração da cédula para identificar como as marcas no papel correspondem às opções feitas pelo eleitor.

Nas eleições americanas deste ano (2024), **23%** dos eleitores votarão em jurisdições onde BMDs constituem o único método de votação.

Sistemas com BMDs oferecem muitos recursos de acessibilidade, como permitir a alteração do idioma e do tamanho da fonte exibida na tela, além do uso de interfaces auditivas para pessoas com problemas motores.

4. As diretrizes VVSG são elaboradas e adotadas pela Comissão de Assistência Eleitoral dos Estados Unidos (*Election Assistance Commission*) e constituem um conjunto de padrões para sistemas de votação que os estados podem voluntariamente adotar.

Por causa dessas características e por constituírem sistemas independentes de *software*, os dispositivos de preenchimento de cédulas têm sido recomendados por especialistas e organizações que lidam com tecnologias do voto – muitas vezes em combinação com a velha cédula preenchida à mão –, em detrimento de sistemas eletrônicos VVPAT, que não podem prescindir de urnas DRE e de seus complexos programas de computador.

No entanto, estudos recentes têm apontado que o uso de BMDs também pode implicar uma série de riscos à integridade dos pleitos. Embora não existam evidências de que ataques reais tenham impactado resultados eleitorais, especialistas em segurança do voto têm demonstrado que eles são teoricamente exequíveis.

Os principais constam de um **relatório** elaborado pelo Centro para Democracia & Tecnologia (CDT). Um deles é o "ataque por código de barras inconsistente": o dispositivo imprime corretamente as informações legíveis por humanos, mas gera um código de barras corrompido, que não corresponde às escolhas do eleitor. ■

VOTO ONLINE

Com a evolução das tecnologias de informação e comunicação e, em especial, com o desenvolvimento, popularização e alcance da internet, a votação online parecia ser o próximo passo a ser dado pelos organismos eleitorais, a fim de tornar as eleições mais eficientes, acessíveis, participativas e baratas.

No entanto, apenas alguns países conseguiram implementar esse sistema de forma relativamente exitosa. O caso mais emblemático é o da Estônia, onde desde 2005 todos os seus cidadãos podem votar pela internet, em qualquer lugar do país. Segundo a base de dados do Idea (*International Institute for Democracy and Electoral Assistance*), Armênia, Austrália, Canadá, Panamá e Suíça são alguns dos países que têm eleições online, mas apenas em algumas regiões ou exclusivamente para parcelas específicas do eleitorado, como diplomatas e militares em missão no exterior, pessoas com deficiência e eleitores que moram fora do país.

Alguns países preferiram abandonar ou não adotar o voto online, depois de realizarem estudos de viabilidade ou experiências piloto, como França, Holanda e Noruega. Os principais desafios encontrados se referem a segurança, sigilo, transparência e confiabilidade, questões ainda não totalmente superadas. Por causa disso, sistemas de votação pela internet são provavelmente a solução tecnológica de mais difícil implementação, já que mexem em pontos centrais de todo o processo eleitoral, além de gerarem as discussões mais acaloradas quando o assunto é a implementação de tecnologias do voto. ■

SISTEMAS COM CRIPTOGRAFIA

Os sistemas eletrônicos que contam com registros físicos dos votos – seja os que se baseiam em urnas eletrônicas que imprimem cédulas (sistema VVPAT), seja os que usam escâneres ópticos – têm constituído a forma mais comum de concretizar o conceito de independência de *software*. Mas existe outra arquitetura tecnológica que também tem essa característica, mas pode prescindir de cédulas impressas: são os **sistemas de votação criptográficos verificáveis de ponta a ponta,** ou *cryptographic end-to-end (E2E) verifiable voting systems*, considerados o estado da arte em tecnologias de votação.

Nesse modelo, são empregadas técnicas de criptografia para armazenar uma cópia criptografada do voto, mantendo o sigilo e permitindo que os resultados finais sejam verificados de forma independente e universal, dispensando auditorias ou recontagens de cédulas em papel. Para isso, é fornecido aos eleitores um recibo que lhes permite checar se o voto foi incluído no resultado, mas sem revelar a ninguém seu teor.

Entre outras vantagens, a verificabilidade criptográfica de ponta a ponta elimina a necessidade de garantir a integridade da cadeia de custódia dos votos físicos, além de permitir que cada eleitor fiscalize individualmente o destino de seu próprio voto.

Sistemas com verificabilidade E2E devem permitir que o eleitor participe de três etapas do ciclo de votação: I) certificando-se de que seu voto foi constituído como ele queria; II) registrado como tal; III) contabilizado exatamente como foi registrado.

Um dos principais desafios no desenvolvimento de sistemas com essa característica diz respeito à preservação do sigilo do voto. Isso porque, em hipótese alguma o recibo pode ser usado como evidência para demonstrar em quem o eleitor votou. Somado a isso, esse recibo também deve ser delegável, isto é, o eleitor pode transferir a tarefa de verificação a qualquer parte interessada, como uma organização independente que fiscalize a eleição.

É aí que entram em cena as técnicas de criptografia, que geram recibos "criptograficamente mascarados". Na primeira etapa, há várias maneiras de garantir ao eleitor a possibilidade de verificar que esses recibos – nos quais estão inscritos códigos incompreensíveis – de fato correspondem a suas escolhas. A mais conhecida é o **"desafio de Benaloh"**: o eleitor pode usar o dispositivo de votação para produzir quantas cédulas criptografadas quiser, mas escolher apenas uma para ser depositada oficialmente. As demais têm suas "máscaras criptográficas" retiradas, revelando o teor do voto em linguagem compreensível. É como se a integridade da máquina fosse "desafiada": se seu *software* contiver um

erro ou adulteração capaz de gerar resultados incorretos, tais resultados muito provavelmente aparecerão nesses votos usados como desafio, já que as chances de o sistema prever se e como será desafiado por cada eleitor são praticamente nulas.

Em seguida, após o encerramento da votação, é publicada uma lista oficial eletrônica com cópias de todos os recibos de votação criptografados, permitindo aos eleitores confirmar que seus votos foram devidamente registrados. Se o comprovante de um eleitor não tiver sido postado, ele poderá reportar o fato e usar o recibo como prova para corrigir o erro.

Por fim, na terceira etapa de verificação, todos os recibos são processados usando uma série de cálculos criptográficos que geram os resultados eleitorais finais. Os algoritmos e parâmetros dessas operações criptográficas devem ser publicados para permitir que os eleitores verifiquem se os seus votos foram computados conforme registrados e para permitir que outros observadores verifiquem se a contagem está correta.

O principal desafio das verificações nessa terceira etapa é a necessidade de usar programas de computador, o que levanta uma outra questão: como podemos confiar neles? A resposta é que, como os algoritmos e parâmetros dessas operações criptográficas são públicos, qualquer pessoa ou instituição pode criar um programa para realizar uma verificação independente. Ao eleitor leigo, restaria a opção de escolher uma ou mais fontes de informação nas quais tenha confiança (um partido político, um veículo de comunicação, uma universidade etc.). Assim, se for criada a cultura de verificações independentes, eventuais erros do sistema de votação muito provavelmente serão detectados.

Os principais sistemas de votação criptográficos já desenvolvidos ainda não são usados em eleições estatais de larga escala. A primeira e principal experiência ocorreu em eleições locais na cidade de Takoma Park, nos Estados Unidos, em 2009 e 2011. **No geral, essa tecnologia tem sido usada em outros tipos de processos de participação, como eleições em conselhos universitários[5].**

5. "A Universidade de São Paulo, por exemplo, usa o sistema **Helios**".

PROJETO "ELEIÇÕES DO FUTURO"

Pesquisadores do Laboratório de Arquitetura e Redes de Computadores, da Universidade de São Paulo (Larc-USP), em convênio com o Tribunal Superior Eleitoral (TSE), estão estudando o desenvolvimento de um modelo de criptografia de ponta a ponta que poderia ser inserido no atual sistema eletrônico de votação usado no Brasil. É possível que no médio prazo essa tecnologia seja efetivamente implementada no país. ■

RECOMENDAÇÕES INTERNACIONAIS

As principais recomendações emitidas por organizações internacionais prescrevem que sistemas eletrônicos de votação devem de algum modo ter independência de *software*.

O Conselho da Europa até o momento é a única organização internacional que estipulou padrões para implementação de voto eletrônico dirigidos a países. Por isso, seu conjunto de recomendações é considerado um dos marcos mais importantes na área. Trata-se da **Recomendação CM/Rec(2017)5,** que atualizou uma compilação anterior, de 2004.

O compilado prevê 49 padrões a serem seguidos pelos Estados-membros que quiserem implementar votações eletrônicas. Eles têm como objetivo assegurar que as novas tecnologias garantam o sufrágio universal, igualitário, livre e secreto. Também se reportam a requisitos regulatórios e organizacionais e de transparência, *accountability*, confiabilidade e segurança dos sistemas.

O padrão 15 da Recomendação é expresso no sentido de que o sistema deve permitir ao eleitor a possibilidade de "verificar que a sua intenção está devidamente representada no voto" e que o voto "entrou na urna eletrônica sem ser alterado". Além disso, "qualquer influência indevida que tenha modificado o voto deve ser detectável".

Na mesma toada, os padrões 17 e 18 estabelecem que os sistemas devem fornecer evidências sólidas de que cada voto válido foi incluído corretamente no resultado e de que apenas votos de eleitores aptos a votar foram incluídos na totalização. Essas evidências devem ser verificáveis por meios que sejam independentes do sistema de votação eletrônico.

As Diretrizes Voluntárias para Sistemas de Votação **(VVSG 2.0),** de 2021, elaboradas e adotadas pela Comissão de Assistência Eleitoral dos Estados Unidos, além de estipularem que o público deve poder entender e verificar todas as operações do sistema eletrônico (recomendação 3.3.), também preveem explicitamente a independência de *software* (recomendação 9.1) e a pronta produção de registros do voto "que forneçam a capacidade de verificar se o resultado da eleição está correto e, na medida do possível, identificar a causa de quaisquer irregularidades" (recomendação 9.2.). ■

DISCORDAR E DIVERGIR, SIM; AFRONTAR, NUNCA!

A engenhosidade humana tem sido capaz de conceber dispositivos e sistemas tecnológicos cada vez mais avançados e para as mais diversas aplicações. Seriam eles capazes de produzir "eleições perfeitas", imunes a erros ou fraudes?

A História tem nos ensinado que a resposta não é tão simples, pois não depende apenas dos aspectos técnicos das próprias tecnologias. Também é preciso considerar como e por quem as eleições são realizadas e como cada sociedade tem estabelecido o seu pacto social em torno dos procedimentos por meio dos quais os seus representantes são eleitos.

Especialistas em segurança da informação entendem que não existem sistemas de votação invioláveis ou completamente seguros, sejam eles eletrônicos ou não. A avaliação meramente técnica das arquiteturas tecnológicas de sistemas de votação pode indicar que algumas apresentam maior risco teórico de vulnerabilidades. Mas é preciso considerar que fragilidades também são resultado da interação entre a tecnologia e o seu entorno.

Portanto, as vantagens e desvantagens de cada modelo devem ser estimadas a partir de uma série de variáveis específicas, como características culturais, geográficas, sociais, econômicas e demográficas de cada sociedade.

Também é importante que, antes da implementação de um sistema, as reais necessidades sejam identificadas, pois tecnologias do voto não são um fim em si mesmo. Elas devem ser concebidas para eliminar ou mitigar problemas concretos ou para aperfeiçoar o sistema existente. E, seja qual for o modelo escolhido, sua implementação deve necessariamente ser progressiva e controlada.

Isso não quer dizer que inexistam parâmetros para avaliar abstratamente as tecnologias de votação. Organismos internacionais e entidades que lidam com o assunto têm emitido uma série de recomendações endereçadas a estados, organismos eleitorais, legisladores, juízes, tribunais e desenvolvedores de sistemas. Esses enunciados convertem os princípios democráticos que devem reger eleições em postulados aplicáveis aos sistemas eletrônicos (leia mais na página 19).

Sigilo do voto e sufrágio universal, por exemplo, devem ser assegurados, assim como procedimentos eleitorais justos e precisos – o que implica as garantias de que todo eleitor deve conseguir compor seu voto de acordo com sua intenção, de que esse voto será registrado da maneira como foi composto e de que será contado da maneira como foi registrado.

Segundo as recomendações internacionais, essas garantias são concretizadas por meio de outro importante requisito. Trata-se da verificabilidade, que permite que as principais atividades e operações eleitorais sejam controladas e fiscalizadas pelo eleitor e pela sociedade, tornando o sistema mais democrático. Além disso, essa característica contribui para a contínua renovação da confiança pública no processo eleitoral, pois sua transparência e o fornecimento de evidências sólidas de que tudo correu bem ajudam a convencer o público leigo de que a tecnologia não está corrompida.

Atualmente, sistemas eletrônicos que geram registros físicos dos votos são a principal maneira de assegurar a verificabilidade (mais detalhes sobre os sistemas VVPAT e de dispositivos de preenchimento de cédulas estão nas páginas 11 e 14, respectivamente).

A premissa por trás desses sistemas é que eles devem ter independência de *software* (vide página 6). O modelo implementado no Brasil não tem essa característica e, portanto, não segue integralmente as recomendações internacionais.

Do ponto de vista estritamente técnico e teórico, a ausência dessa característica poderia ser um problema grave. No entanto, a Justiça Eleitoral brasileira tem procurado garantir a segurança do sistema com outra abordagem. Considerando que não existe um segundo conjunto autônomo de resultados com o qual o resultado gerado eletronicamente possa ser comparado, a validade dos resultados é buscada por meio da inspeção do próprio *software* e de seu correto funcionamento (conforme exposto na página 9).

Certamente há a possibilidade de avanços e aprimoramentos, principalmente em relação à transparência do sistema. Mas, ainda que isso ocorra, um eleitor sem conhecimentos altamente especializados não conseguiria fiscalizar o processo eleitoral. Nem mesmo um *expert*, aliás, conseguiria testemunhar empiricamente que seu próprio voto "entrou" na urna eletrônica corretamente.

Por outro lado, caso a independência de *software* fosse assegurada por meio de um sistema que produz registros físicos dos votos, surgiria uma série de outros problemas de magnitude considerável, inexistentes atualmente. O eleitor até poderia "ver com os próprios olhos" que o voto físico de fato contém as suas escolhas. Mas, dependendo da maneira como a complexa cadeia de procedimentos analógicos fosse administrada, essa segurança poderia ter pouca validade.

Portanto, é importante ter em conta que as recomendações que prescrevem o uso de dispositivos independentes de *software* muitas vezes não consideram a realidade concreta de cada país e reportam-se apenas aos aspectos estritamente tecnológicos dos sistemas de votação, deixando de observar todo o conjunto de operações que constituem uma eleição.

Debates sobre o melhor modelo de tecnologia do voto para uma determinada sociedade devem considerar uma abordagem holística, que incorpore, sim, o espírito das recomendações internacionais, mas que também se reporte às especificidades locais e às diferentes escolhas políticas por trás de cada arquitetura.

Em uma sociedade democrática, participativa e plural, é natural e salutar que discussões sobre o sistema eletrônico de votação sejam travadas. Elas podem gerar críticas construtivas à tecnologia do voto implementada, traçando o caminho para aperfeiçoamentos, revisões de rota, adoção de novos sistemas ou mesmo a ratificação da confiança pública na tecnologia empregada.

Esse debate também precisaria contemplar as demais arquiteturas tecnológicas existentes, incluindo aquelas que ainda estão sendo desenvolvidas, como o sistema de votação criptográfico em estudo pela Justiça Eleitoral (veja mais detalhes na página 18). Sem a participação da sociedade nesse debate, é pouco provável que melhorias ou novas tecnologias, por mais seguras que sejam, consigam conquistar confiança pública.

Apesar de a conjuntura política ser um elemento desafiador, o exercício das liberdades de expressão, de imprensa e acadêmica, além da garantia do direito de acesso à informação, é a única forma de restabelecer o pacto social brasileiro em torno de seu sistema de votação. Um jornalismo crítico e responsável tem um papel importantíssimo nesse processo.

Coordenação da Publicação
André Boselli
Patrícia de Matos

Pesquisa e Texto
André Boselli

Revisão Textual
André Boselli
Patrícia de Matos

Design e Diagramação
Roberta Giotto

COMO COBRIR **CRITICAMENTE A URNA ELETRÔNICA**

SEM ALIMENTAR TEORIAS
DA CONSPIRAÇÃO

ARTIGO19

DEFENDENDO A LIBERDADE DE EXPRESSÃO E INFORMAÇÃO

@artigo19
@artigo19
@artigo19
@artigo19brasil
artigo19.org

ARTIGO19