ELEIÇÕES

Urna eletrônica: quais são os itens de segurança contra fraude?

Entenda como funcionam os principais mecanismos de proteção dos equipamentos contra mudança de voto e quebra de sigilo

Brenda Zacharias

23 OUT **2020** **12h06** *atualizado às 12h17*

2 COMENTÁRIOS

Diversos **mitos** rondam a utilização de urnas eletrônicas no processo eleitoral brasileiro, do projeto e desenvolvimento dos aparelhos ao registro e a contagem dos votos. Contudo, não passam de desconfiança, de acordo com o Tribunal Superior Eleitoral (TSE), órgão responsável pela condução das eleições no País. **Não existe registro comprovado de fraude** desde a primeira vez em que foram usadas, em 1996. Isso porque existem cerca de 30 mecanismos de segurança para impedir tentativas de adulteração ou de quebra de sigilo dos resultados.

SAIBA MAIS

Arthur do Val e Orlando Silva trocam alfinetadas em "debate"

Candidata a vice-prefeita em Belém é alvo de ataques a tiros

PT cobra candidatos que não usam campanha para defender Lula

"O importante é ir para o segundo turno", afirma Russomanno

O secretário de tecnologia da informação do Tribunal, **Giuseppe Janino**, destaca os seguintes mitos entre os mais recorrentes:

- As urnas são compradas de empresas de tecnologia particulares e, por isso, podem ser reproduzidas;
- Vírus podem contaminar as urnas e roubar ou alterar os resultados;
- Não é possível auditar o programa de uma urna ou fazer a recontagem de votos.

Nenhuma dessas afirmações é verdadeira, de acordo com Janino. Para ele, a descrença no sistema surge primeiro por uma questão cultural: "O brasileiro tende a achar que não pode ser bom em alguma coisa. (*Neste caso,*) somos referência mundial para muitos países", afirma ele. O outro motivo deriva de questões políticas. "Fica mais fácil falar que perdeu por causa de fraude. Isso se propaga com muita intensidade com as redes sociais, infelizmente, desqualificando um processo que é uma conquista do brasileiro."

Entenda, a seguir, quais são os itens de segurança das urnas eletrônicas brasileiras.

Projeto brasileiro

O projeto das urnas foi totalmente desenvolvido por **técnicos da Justiça Eleitoral** com contribuição de consultores de órgãos federais como as Forças Armadas, o **Instituto Nacional de Tecnologia**, o **Instituto de Tecnologia da Aeronáutica**, o **Instituto Nacional de Pesquisas Aeroespaciais** e o Ministério das Comunicações.

Segundo Janino, o TSE acompanha e controla todo o processo fabril. "Isso fica tão evidente que, quando a empresa termina de fabricar, ela nem consegue testar (*as urnas*) se não tiver uma intervenção nossa", diz ele. Além do projeto físico, todos os **softwares** usados no processo eleitoral - ao todo, são **94 sistemas**, contando do cadastro do eleitor à divulgação dos resultados - são de uso exclusivo do tribunal.

Veja, nesta reportagem, as especificidades técnicas de uma urna eletrônica brasileira.

Softwares

Antes de cada eleição, todos os softwares ficam abertos por 180 dias para que partidos políticos, o Ministério Público, a Controladoria-Geral da União e outras entidades possam verificar a integridade dos programas que serão instalados nas urnas. A abertura também pode ser requerida após o pleito, em caso de suspeita de fraude: em **2014**, por exemplo, o PSDB auditou os códigos após suspeitar de irregularidades nas eleições presidenciais.

Depois deste período, os programas passam por um processo chamado **Cerimônia de Lacração**. O deste ano foi encerrado na última sexta-feira, 16. Todos os programas passam por um processo de blindagem: primeiro, são formados *hashes*, ou **resumo digital**, a partir dos códigos binários deles. Os *hashes* são como uma espécie de **dígito verificador**, explica Janino, que podem atestar a autenticidade do programa. "É como se eu pegasse uma folha com vários caracteres em uma folha e fizesse uma conta com eles. Se eu alterar um 'a' por 'b', o número não vai bater mais", diz.

Além disso, os programas recebem uma camada de **assinaturas digitais**, registradas por autoridades como o ministro e presidente do TSE, Luís Roberto Barroso, e o procurador-geral da República e eleitoral, Augusto Aras, e o próprio Janino. Todos os blocos de programação ficam amarrados por este conjunto de assinaturas e, caso seja necessário modificar algum trecho, todas as pessoas devem assiná-los de novo. Uma cópia dos programas fica armazenada na sala-cofre do tribunal e outras 27 são enviadas para os Tribunais Regionais para serem instaladas nas urnas.

MM_AG_PT_ASSET_928213

Equipamentos isolados

As urnas eletrônicas são equipamentos totalmente **isolados**, de acordo com o TSE. Ou seja: elas não estão conectadas à internet por cabos ou por conexão wi-fi, nem sequer aceitam conexão bluetooth. Caso algum hacker queira invadir uma urna, ele teria que fazer o processo na própria seção eleitoral, in loco.

Para se ter acesso à memória de uma urna, o hacker deveria, em primeiro lugar, romper um lacre físico que impede a abertura do aparelho. Este lacre é desenvolvido pela Casa da Moeda e, caso seja manipulado, muda de cor.

Ao ser iniciada, a urna ativa um dispositivo chamado **hardware de segurança**, uma espécie de computador dentro da urna. É nele onde ficam armazenados os certificados que garantem a autenticidade dos programas instalados nela e das informações geradas. Quando acionado, ele também confere se todos os programas e o sistema operacional são autênticos e estão em pleno funcionamento para, então, ativar a urna eletrônica para a votação. "Isso significa que não é possível rodar na urna qualquer software que não seja de autoria do TSE ou esteja adulterado", reforça Janino.

'Caixa-preta' da urna

As urnas eletrônicas contêm uma espécie de **"caixa-preta"**, como a encontrada nos aviões. Trata-se de um dispositivo chamado **log** que registra todas as suas atividades - ele anota todas as vezes em que a urna é ligada e desligada, o momento em que é habilitada para o primeiro eleitor votar, a hora em que emitiu o resultado e todas as outras ocorrências possíveis. Por meio dele, dá saber exatamente o que aconteceu com a urna e confirmar possíveis tentativas de fraudes, explica Janino.

Registro do voto

O **registro digital** é o arquivo com os votos de todos os eleitores naquela urna. De acordo com Janino, é como se existisse uma tabela dentro da urna com uma coluna para o voto para prefeito e outro para vereador. Os votos registrados na urna são gravados de maneira aleatória nessa tabela e contabilizados. No final, a planilha recebe uma assinatura digital da urna, que certifica a procedência dos dados. Com essa tabela, é possível realizar a **recontagem eletrônica** dos votos, se necessário.

Logo após a votação ser encerrada, a urna automaticamente faz a apuração dos votos e imprime os resultados daquela seção eleitoral. Este **boletim de urna** traz informações como total de votos por partido e por candidato, total de votos nulos e em branco e a hora do encerramento da eleição, e é fixado na frente da seção eleitoral. Isso é importante pois garante que, no encerramento da votação, o resultado já é de conhecimento público.

Depois de impresso o boletim, começa o processo de consolidação dos resultados. Eles são gravados em uma mídia digital removível e criptografados. A mídia vai para um ponto de transmissão em cartório eleitoral e é encaminhada até o totalizador por meio de uma rede interna do tribunal. Os dados são computados e, então, publicados. É um processo muito rápido: de acordo com Janino, na última eleição foram processados **150 mil votos por segundo**.

Testes públicos de segurança

O TSE promove um evento chamado **Teste Público de Segurança**, para a qual são convidados hackers cuja missão é tentar quebrar o sigilo das urnas ou produzir alguma fraude nos resultados. O tribunal dá aos participantes as urnas com algumas das barreiras já desativadas, de acordo com Janino, e permite que apliquem os seus planos de ataque. Nenhum deles, porém, já funcionou em qualquer uma das cinco edições do teste; a última foi realizada em novembro do ano passado.