Nota de esclarecimento

A urna eletrônica é um dispositivo que coleta a intenção do eleitor, conta os votos designados pelo eleitor e, então, emite o resultado de uma votação ocorrida dentro de um intervalo de tempo. Tudo isso deve ocorrer de acordo com os requisitos constitucionais do caput do artigo 14 da Constituição Federal, entre eles, o sigilo do voto.

A votação tem um momento de início e de fim, além de ocorrer em um dado local.

Antes da votação, a urna é carregada com os dados dos eleitores e dos candidatos correspondentes, em um procedimento conhecido como "preparação".

Uma vez que as urnas estejam prontas, é estabelecida uma correspondência, na forma de tabela, entre o local em que a urna receberá votos (seção) e a sua identidade.

O início da votação é indicado pela emissão da zerésima, que atesta que a preparação daquela urna foi adequada, ou seja, que todos os eleitores e candidatos incluídos na preparação estão corretos e que não há nenhum voto contabilizado.

Enquanto a votação ocorre, os votos são registrados em uma estrutura de dados chamada Registro Digital do Voto (RDV). A cada voto adicionado a essa estrutura de dados, os votos são embaralhados e cifrados, impedindo que alguém interrompa e recupere alguma informação sigilosa. Porém, mesmo que uma interrupção ocorra, a urna é suficientemente resiliente para reiniciar do ponto que parou, mesmo que esteja substituindo outra urna como contingência.

Ao final da votação, essa coleta é finalizada, gravando-se as últimas versões do RDV e do Boletim de Urna (BU) – uma espécie de relatório – na Memória de Resultado, um pendrive conhecido pela sigla MR. Esses RDVs e BUs gravados na MR são assinados digitalmente com a identidade da urna.

Os resultados são, então, impressos no BU com as contagens dos votos para cada candidato/partido. Depois, o BU é afixado na seção eleitoral (no local de votação) para que todos possam conferir ou fazer uma contagem paralela à oficial. Perceba que, nesse ponto do processo, o resultado da urna é imutável, pois a integridade (garantia de que os resultados não estão corrompidos) e a autenticidade (garantia de que os resultados são provenientes de uma urna válida) de seu conteúdo podem ser verificadas a qualquer momento.

A Memória de Resultado é então utilizada para que seu RDV e seu BU sejam transmitidos para o TSE e, assim, os resultados de todo o país sejam totalizados, isto é, as contagens de todas as seções para cada candidato-cargo sejam agrupadas e aplicadas os quocientes eleitorais e partidários. Em resumo, a

totalização é a aplicação da legislação eleitoral ao resultado da contagem pura e simples.

Para que o resultado de uma urna seja considerado, ou seja, para que a totalização use o resultado de uma urna, existe uma lista de exigências a serem superadas. Uma delas, e talvez a mais importante, é que ela deve ter vindo de uma urna válida. Uma urna válida é aquela que tem uma identidade reconhecida pelo TSE por meio da verificação da assinatura digital do resultado (no RDV e no BU) e que esteja presente na tabela de correspondência de forma correta, isto é, a urna deve ter vindo da seção para a qual foi preparada.

Uma vez totalizada a eleição, ocorre a divulgação desses resultados, seja em site do próprio do TSE, quanto em veículos de mídia.

Em termos de dispositivo de hardware, a urna é um computador. Porém, não é um computador comum de mercado, mas sim projetado conforme exigências estabelecidas pelo TSE para garantir a segurança de seu hardware.

No vídeo apresentado pelo youtuber, é exposta, de forma didática, uma maneira de se fazer uma urna usando um kit simples, como é o caso de placas com processador Arduino. Porém, é uma oportunidade para esclarecer os motivos pelos quais uma urna eletrônica não é tão simples como apresentado.

Confira abaixo uma lista de esclarecimentos elaborados a partir de uma análise do que aparece no vídeo:

1) A urna eletrônica real não pode ser clonada, pois existe um perímetro criptográfico, que basicamente contém um computador exclusivo que atende a dois requisitos básicos: (a) identificá-la unicamente como um dispositivo da Justiça Eleitoral; (b) oferecer serviços criptográficos confiáveis aos aplicativos da urna. Esse computador exclusivo é protegido contra tentativas de invasão que, se forem tentadas, serão evidenciadas;

2) Para identificar a urna unicamente, são gerados parâmetros criptográficos pela própria urna, dentro do perímetro criptográfico, no momento de sua fabricação e que garantidamente nunca são expostos. Essa identidade é conferida na preparação da urna antes da votação e, depois, na totalização dos votos. Portanto, se uma urna não corresponder àquela que foi carregada, há meios para que ela não seja considerada válida, permitindo ainda que sejam verificadas as evidências, caso se confirme alguma tentativa de fraude;

3) O teclado do eleitor é um dispositivo bastante diferente daquele exibido no vídeo. Em primeiro lugar, ele não é de membrana e nem é matricial. O teclado do eleitor é um periférico com um microcontrolador próprio, que se conecta via USB com a placa-mãe (via canal de comunicação cifrado) e tem, ele mesmo, um perímetro criptográfico que o identifica como um teclado da urna, e não como um teclado qualquer. Esse teclado do eleitor tem as mesmas proteções para impedir tentativas físicas de invasão;

4) As urnas eletrônicas, como um computador comum, têm firmwares (softwares gravados em memórias residentes nas placas), que iniciam operacionalmente a urna, além de contar com softwares básicos que carregam o sistema operacional. Porém, de forma diferente dos computadores comuns, a urna eletrônica conta com uma cadeia de confiança iniciada pelo computador do perímetro criptográfico, que verifica as autenticidades e integridades de cada um dos componentes dessa cadeia. Resumindo, essa cadeia de confiança impede que softwares alheios à Justiça Eleitoral sejam carregados e executem na urna;

5) Além de impedir que softwares alheios à Justiça Eleitoral sejam carregados e executem na urna, a cadeia de confiança tem perfis operacionais. Há perfis exclusivos para os fabricantes, restringindo bastante seu uso. Há perfis de desenvolvedores e testadores, que permitem uma operação completa, mas não durante uma eleição oficial. E há o perfil oficial de um software que somente pode ser executado durante uma eleição real;

6) Os códigos-fonte dos softwares e dos firmwares são abertos à consulta durante seis meses antes das eleições, para qualquer pessoa que queira encontrar algum mecanismo malicioso e comunicar sua existência à Justiça Eleitoral. Além disso, antes das eleições, são realizados testes públicos de segurança, nos quais são submetidos planos de testes em que os participantes podem expor vulnerabilidades que alterem o resultado da votação ou revelem o voto, quebrando o seu sigilo. As contribuições dos participantes na exposição de eventuais vulnerabilidades são valiosas, pois, depois de encontradas, são corrigidas e testadas novamente com a ajuda do participante, para verificar se foram realmente corrigidas;

Como se percebe, uma urna eletrônica real não é tão simples e desprotegida como aquela apresentada no vídeo. Além disso, há meios de auditoria para se verificar se os softwares e firmwares executados na urna contêm algum mecanismo malicioso, como o exposto no vídeo. Além disso, há todo um conjunto de procedimentos, que impede a recepção de resultados ilegítimos provenientes de eventuais equipamentos clonados ou gerados por softwares ilegítimos.