

Revista Eletrônica EJE

Ano IV – Número 6 – Outubro/Novembro 2014

ENTREVISTA

Ministro Tarcísio Vieira de Carvalho Neto fala sobre as ações eleitorais, que é o tema desta edição.

REPORTAGEM

Conheça um pouco mais sobre a atividade jurisdicional do TSE – Os processos submetidos ao Tribunal seguem tramitação própria, conforme as suas características é o título da reportagem produzida pela Assessoria de Imprensa e Comunicação Social do TSE.

ARTIGOS

Nesta edição, os artigos discorrem sobre: as doações de campanha oriundas de pessoas jurídicas; a ilegitimidade do comitê financeiro para interpor recurso eleitoral; os mecanismos de segurança da urna eletrônica; e as modificações na propaganda eleitoral e na propaganda partidária promovidas pela Minirreforma Eleitoral de 2013. Confira.



Por que a urna eletrônica é segura

*Rodrigo Carneiro Munhoz Coimbra**

Em todos os anos de eleições no Brasil, além dos acalorados debates entre os candidatos e suas propostas, sempre surge uma pergunta: a urna eletrônica é realmente segura? Essa questão mexe com o imaginário

das pessoas e acende discussões na imprensa e nas redes sociais. Toda sorte de supostas fraudes e teorias conspiratórias surge nessa época. O fato é que a Justiça Eleitoral trabalha duro para garantir que a votação ocorra de forma segura, transparente e eficiente. E o sucesso e a qualidade desse trabalho podem ser conferidos pela população ao final de cada eleição.



*Bacharel e mestre em Ciência da Computação pela Universidade de Brasília. Analista judiciário do Tribunal Superior Eleitoral lotado na Seção de Voto Informatizado.

A Justiça Eleitoral utiliza o que há de mais moderno em termos de segurança da informação para garantir a integridade, a autenticidade e, quando necessário, o sigilo. Esses mecanismos foram postos à prova durante os Testes Públicos de Segurança realizados em 2009 e 2012, nos quais nenhuma tentativa de adulteração dos sistemas ou dos resultados da votação obteve êxito. Além disso, há diversos mecanismos de auditoria e verificação dos resultados que podem ser efetuados por candidatos e coligações, pelo Ministério Público (MP), pela Ordem dos Advogados do Brasil (OAB) e pelo próprio eleitor.

Um dos procedimentos de segurança que pode ser acompanhado pelo eleitor é a Cerimônia de Votação Paralela. Na véspera da eleição, em audiência pública, são sorteadas urnas para verificação. Essas urnas, que já estavam instaladas nos locais de votação, são conduzidas ao Tribunal Regional Eleitoral (TRE) e substituídas por outras, preparadas com o mesmo procedimento das originais. No dia das eleições, também em cerimônia pública, as urnas sorteadas são submetidas à votação

nas mesmas condições em que ocorreria na seção eleitoral, mas com o registro, em paralelo, dos votos depositados na urna eletrônica. Cada voto é registrado numa cédula de papel e, em seguida, replicado na urna eletrônica, tudo isso registrado em vídeo. Ao final do dia, no mesmo horário em que se encerra a votação, é feita a apuração das cédulas de papel e comparado o resultado com o boletim de urna.

Outro mecanismo bastante simples de verificação é a conferência do boletim de urna. Ao final da votação, o boletim com a apuração dos votos de uma seção transforma-se em documento público. O resultado de cada boletim pode ser facilmente confrontado com aquele publicado pelo Tribunal Superior Eleitoral (TSE) na Internet, seja pela conferência do resultado de cada seção eleitoral, seja pela conferência do resultado da totalização final. Esse é um procedimento amplamente realizado pelos partidos políticos e coligações há muito tempo e que também pode ser feito pelo eleitor.

Tais procedimentos para a aferição da segurança do processo eleitoral não são os únicos mecanismos desenvolvidos pela Justiça Eleitoral. A urna eletrônica utiliza o que há de mais moderno quanto às tecnologias de criptografia, assinatura digital e resumo digital. Toda essa tecnologia é utilizada pelo *hardware* e pelo *software* da urna eletrônica para criar uma cadeia de confiança, garantindo que somente o *software* desenvolvido pelo TSE, gerado durante a Cerimônia de Lacração dos Sistemas Eleitorais, pode ser executado nas urnas eletrônicas devidamente certificadas pela Justiça Eleitoral. Qualquer tentativa de executar *software* não autorizado na urna eletrônica resulta no bloqueio do seu funcionamento. De igual modo, tentativas de executar o *software* oficial em um *hardware* não certificado resultam no cancelamento da execução do aplicativo.

Para todo o conjunto de *software* produzido durante a Cerimônia de Lacração dos Sistemas Eleitorais, são geradas assinaturas digitais e resumos digitais. Caso haja qualquer suspeição

quanto à autenticidade do *software* da urna eletrônica, as assinaturas digitais e os resumos digitais podem ser conferidos e validados por aplicativos desenvolvidos pelo TSE e por *software* desenvolvido por partidos políticos, pelo MP e pela OAB.

Todos os dados que alimentam a urna eletrônica, assim como todos os resultados produzidos, são protegidos por assinatura digital. Não é possível modificar os dados de candidatos e eleitores presentes na urna, por exemplo. Da mesma forma, não é possível modificar o resultado da votação contido no boletim de urna ou o registro das operações feitas pelo *software* (Log) ou mesmo o arquivo de Registro Digital do Voto (RDV), entre outros arquivos produzidos pela urna, uma vez que todos estão protegidos pela assinatura digital.

Muito se fala da possibilidade de *hackers* invadirem as urnas no dia da votação, mas a urna eletrônica não é vulnerável a ataques externos. Esse equipamento funciona de forma isolada, ou seja, não dispõe de qualquer mecanismo que possibilite sua conexão a redes de computadores, como

a Internet. Também não é equipado com o *hardware* necessário para se conectar a uma rede ou mesmo qualquer forma de conexão com ou sem fio. Vale destacar que o sistema operacional Linux contido na urna é preparado pela Justiça Eleitoral de forma a não incluir nenhum mecanismo de *software* que permita a conexão com redes ou o acesso remoto.

Além disso, as mídias utilizadas pela Justiça Eleitoral para a preparação das urnas e gravação dos resultados são protegidas por técnicas modernas de assinatura digital. Não é possível a um atacante modificar qualquer arquivo presente nessas mídias.

Também são tomadas medidas contra possíveis tentativas de violação que possam ser feitas por pessoas que trabalham diretamente no processo eleitoral. Para isso, a Justiça Eleitoral utiliza ferramentas modernas de controle de versão do código-fonte dos sistemas eleitorais. A partir dessas ferramentas, é possível acompanhar toda modificação feita sobre o código-fonte, o que foi

modificado e por quem. Somente um grupo restrito de servidores e colaboradores do TSE tem acesso ao repositório de código-fonte e está autorizado a fazer modificações no *software*. Uma consequência disso é que o *software* utilizado nas eleições é o mesmo em todo o Brasil e está sob o controle estrito do TSE.

O conhecimento sobre os sistemas eleitorais é segregado dentro do TSE. Isso significa que a equipe responsável pelo *software* da urna não é a mesma que cuida do sistema de totalização. Esse controle de acesso ocorre inclusive com relação ao sistema de controle de versões. A quantidade de sistemas eleitorais envolvidos na realização de uma eleição é tão grande que se torna impraticável a um agente interno ter um grau de conhecimento do todo que lhe permita realizar algum tipo de ataque.

Além disso, durante o período de desenvolvimento dos sistemas eleitorais, são realizados diversos testes tanto pelo TSE quanto pelos TREs com o objetivo de averiguar o correto funcionamento

de todo o conjunto de *software*. Os partidos políticos, o MP e a OAB podem acompanhar o desenvolvimento do *software* por meio de inspeção do código-fonte no próprio ambiente no qual serão gerados os aplicativos a serem utilizados nas eleições.

Durante o período eleitoral, além dos servidores da Justiça Eleitoral, são contratados colaboradores para a prestação de apoio às atividades de transporte, preparação e manutenção das urnas eletrônicas. Também são convocados milhões de mesários para o dia da votação. Em nenhum momento, esses colaboradores ou os mesários têm acesso ao código-fonte dos sistemas eleitorais. Embora essas pessoas tenham contato com as urnas eletrônicas, elas são incapazes de violar o *software* e o *hardware*. Isso é garantido pelos diversos mecanismos de segurança, baseados em assinatura digital e criptografia, que criam uma cadeia de confiança entre *hardware* e *software* e impedem qualquer violação da urna eletrônica.

A urna eletrônica brasileira é um projeto maduro, que já completou 18 anos de existência. Nos últimos anos, a Justiça Eleitoral tem organizado eleições seguras, transparentes e muito rápidas, que têm servido de modelo e inspiração para todo o mundo. As eleições e as urnas brasileiras são seguras e confiáveis, seja pelo trabalho árduo da Justiça Eleitoral, seja pelo efetivo acompanhamento de todo o processo pela sociedade.