EPISÓDIO 5

Fraudar *software* da urna durante fase de desenvolvimento é praticamente impossível

Nos episódios 1 e 4, a **ARTIGO 19** demonstrou por que é inviável tentar fraudar o sistema eletrônico de votação invadindo a urna eletrônica ou adulterando dados durante a totalização dos votos. Portanto, o único momento em que em tese poderia ocorrer alguma forma de fraude é durante a fase de desenvolvimento dos programas que são instalados na urna, que ocorre na sede do Tribunal Superior Eleitoral, em Brasília. Essa hipótese, contudo, também é inviável, pois existem vários procedimentos de fiscalização e auditoria durante essa fase do ciclo eleitoral.

Um dos mais importantes é a chamada inspeção dos códigos-fontes, quando as entidades fiscalizadoras, como partidos políticos, Polícia Federal e Forças Armadas, têm acesso à programação dos *softwares* e podem acompanhar os trabalhos dos técnicos do tribunal. Nas eleições de 2022, o período dessa inspeção começou um ano antes do primeiro turno; nos pleitos precedentes, esse período era de seis meses.

Os testes públicos de segurança compõem outro mecanismo importantíssimo de fiscalização, quando especialistas em informática tentam atacar o sistema eletrônico de votação. O objetivo é que os ataques encontrem fragilidades nos sistemas e que os técnicos do TSE possam corrigi-las. Essas alterações são então verificadas novamente, nos chamados testes de confirmação, oportunidade em que os investigadores são convocados para verificar as correções implementadas e executar novamente os seus planos de ataque, a fim de comprovar que as falhas foram de fato tratadas.

Há ainda a lacração e assinatura digital dos sistemas, que ocorrem em uma cerimônia pública durante a qual é feito o “congelamento” de todos os *softwares* que serão instalados nas urnas. A lacração é um procedimento matemático que confere uma blindagem a todo o conjunto de sistemas, assegurando-lhes dois atributos: a autoria do TSE e a integridade.

Nessa cerimônia, os programas de verificação desenvolvidos pelo TSE e pelas entidades fiscalizadoras checam a integridade das aplicações que compõem o sistema da urna eletrônica, que são então compiladas e assinadas digitalmente por servidores do organismo eleitoral e por representantes das entidades que fiscalizam o processo eleitoral. A assinatura digital é um mecanismo análogo à assinatura de punho e permite confirmar a origem e autenticidade de um documento ou programa. A lacração também permite posterior auditoria do código-fonte dos sistemas – isto é, caso haja alguma dúvida sobre o

resultado eleitoral, é possível comparar o programa efetivamente instalado nas urnas com aquele “congelado” durante essa cerimônia.

Há ainda várias outras etapas de auditoria/fiscalização. Por exemplo, cerimônias de preparação das urnas e de verificação da afixação do lacre físico, testes de integridade, possibilidade de conferência da totalização de votos divulgada pelo TSE (por meio do uso de QR COdes impressos nos boletins de urna) e disponibilização aos partidos dos registros digitais do voto (para que façam de forma independente uma verificação dos resultados eleitorais e consigam checar se as informações constantes do boletim de urna estão corretas). Nenhum desses mecanismos de auditoria é autocontido ou autossuficiente; eles são complementares e, juntos, integram uma cadeia de segurança robusta, que torna inviável qualquer tentativa de fraude.