

EPISÓDIO 4

Urna eletrônica não é conectada a nenhuma rede e, por isso, invadi-la é inviável

Quando se fala na possibilidade de um “ataque hacker” à urna eletrônica, é preciso especificar em que momento do processo eleitoral essa tentativa poderia em tese ocorrer e de que forma isso seria feito. No [primeiro episódio](#) da série, a **ARTIGO 19** [demonstrou](#) por que é inviável tentar fraudar eleições manipulando, de alguma forma, a totalização que é feita pelo Tribunal Superior Eleitoral (TSE).

Outra possibilidade que poderia ser cogitada, então, seria invadir remotamente a urna eletrônica antes ou durante o período de votação. Mas isso também é impossível, já que ela não é conectada à internet ou a qualquer outra rede, seja por cabo, *wifi* ou *bluetooth*.

Por isso, restaria a alternativa de invadir a urna fisicamente. Mas essa hipótese tampouco é viável, por vários motivos. Primeiro, porque os pretensos fraudadores precisariam invadir milhares de equipamentos. Em uma eleição presidencial, por exemplo, a adulteração deveria ocorrer em mais de [50 mil urnas](#). A estimativa leva em conta que cada aparelho recebe em média cerca de 300 votos e que milhões deles precisariam ser adulterados. Além disso, é preciso considerar que não faria sentido adulterar todos os 300 votos, pois cada urna já teria um número razoável de votos para o candidato que seria favorecido. Tampouco seria estratégico fazer uma adulteração massiva, pois isso tornaria a fraude mais detectável.

Ou seja, nesse cenário de 50 mil urnas, os fraudadores teriam de contar com a conivência de quem é responsável pela guarda e supervisão de milhares de equipamentos. No dia da eleição, por exemplo, em cada seção eleitoral trabalham ao menos quatro pessoas. Ou seja, no mínimo 200 mil pessoas teriam que ser convencidas a participar do esquema. Se for considerado o período anterior ao dia da eleição, o número seria ainda maior, pois há os servidores e policiais que fazem a guarda das urnas nos tribunais regionais eleitorais.

Se esses obstáculos já não fossem suficientes, outra barreira teria de ser superada: os lacres físicos colados atrás de cada urna eletrônica (em todas as portas de acesso físico ao equipamento e às mídias nele inseridas). Os lacres são feitos pela Cada da Moeda, em material autoadesivo e com uma numeração sequencial de sete dígitos específica para cada aparelho. Caso alguém tente [retirá-los](#), eles ficarão com a inscrição “TSE”, indicando que a urna foi violada.

Mesmo que, ainda assim, o acesso físico às urnas fosse possível, os fraudadores não conseguiriam adulterar o programa instalado no equipamento, pois ele só opera depois de

verificar se o *software* é exatamente aquele que foi desenvolvido pela Justiça Eleitoral. É o que se chama de “cadeia de confiança baseada em *hardware*”. Trata-se de um chip resinado na placa-mãe que checa as assinaturas digitais do programa instalado, entre outros requisitos de segurança.

