OpiniÃ£o: Sem teoria da conspiraÃ§Ã£o: Ã© impossÃvel fraudar urnas

Há uma verdade evidente que muitos relutam em aceitar: o sistema de voto eletrônico brasileiro é o melhor e mais seguro existente. O sentimento de desconfiança que se procurou gerar nessas eleições não encontra apoio na realidade.

Mitos e *fake news* infestam as redes sociais. Desde acusações no sentido de que os equipamentos foram fabricados por uma empresa venezuelana, até malabarismos de estatística probabilística — que não funcionam em sistemas estimulados, como é o caso de uma eleição —, o que não falta são as mais bem elaboradas teorias conspiratórias. E os fatos são claros: todo o procedimento envolvido no sistema eletrônico de votação é extremamente seguro e possui barreiras de segurança insuscetíveis de violação.

É muito fácil afirmar que a urna eletrônica é um computador e, como tal, pode ser violado. É fácil argumentar que "até a NASA" já foi invadida, e que "basta um técnico" para que o resultado da apuração seja modificado.

Talvez não tenha sido realizado o esclarecimento suficiente à população sobre os sistemas de segurança existentes no processo de votação — que são dezenas. Isto, por certo, colaborou com a disseminação das inverdades e da histeria que tomou conta de muitos eleitores e de parte da sociedade.

A urna eletrônica em si não é o único elemento de todo o processo de voto eletrônico. É apenas o mais evidente. O sistema de voto "por máquinas" já era previsto no artigo 152 do Código Eleitoral de 1932. Desde 2004, prevê a legislação o registro de voto exclusivamente em meio digital, quando abandonado de vez o sistema de cédulas de papel. Falemos inicialmente sobre a urna eletrônica, que é a segunda maior vítima (a primeira são os milhares de servidores, magistrados e promotores de Justiça que trabalham na Justiça Eleitoral) das acusações falsas compartilhadas freneticamente nas redes sociais.

A urna é, fruto de um projeto do Tribunal Superior Eleitoral, exclusivamente adaptada às necessidades de segurança que envolvem o processo de votação. Trata-se de equipamento que não possui em seus circuitos nenhum sistema de comunicação remota. Não há sequer "portas" de conexão em rede (aquele cabinho azul), ou tampouco wi-fi, bluetooth ou qualquer espécie de radiofrequência e similares. Noutros termos, a urna não está e nem possui meios para que venha a estar conectada à internet.

Fosse possível superar essa barreira, que, por si só, já torna difícil e impraticável a tarefa de se buscar o comprometimento individual e pessoal de mais de meio milhão de urnas eletrônicas, é importante dizer também que qualquer tentativa de acesso direto também seria impossível. Todas as urnas eletrônicas contam com um "chip" criptográfico de segurança, que decide o que pode ou não se comunicar com a urna. Qualquer tentativa de se conectar dispositivos não autenticados e certificados pela Justiça Eleitoral resulta em falha, pois que o citado chip de segurança não permite que dispositivos externos tenham acesso sequer à BIOS da máquina, e, muito menos, à memória volátil, memória física e outros sistemas. Todo o barramento de comunicações passa, primeiro, pelo guardião criptográfico. Então, não há como conectar um modem externo, um pen drive, o que quer que seja às urnas eletrônicas. O resultado seria

sua violação e registro da tentativa em logs de sistema.

Vale lembrar ainda que todas as urnas eletrônicas possuem lacres invioláveis assinados individualmente pelos juízes eleitorais, promotores eleitorais de cada zona eleitoral. São nove lacres em cada urna, de modo que qualquer tentativa de acesso ao equipamento resultaria em sua violação e ficaria evidente para fiscais de partido, candidatos, mesários.

O sistema eletrônico de votação conta ainda com intransponíveis proteções de software. O código-fonte de todos os sistemas eleitorais é disponibilizado publicamente a cada dois anos, durante seis meses, por força de previsão legal expressa (artigo 66 da Lei 9.504/97). Qualquer interessado pode destrinchar as milhares de linhas de código livremente. Ao término da auditoria pública obrigatória, os softwares são compilados em sessão pública, na presença de representantes da Justiça Eleitoral, Ministério Público, Polícia Federal, OAB, partidos políticos e quaisquer outros interessados. Os programas de computador resultantes são assinados digitalmente pelas autoridades mencionadas e integralmente criptografados com chaves de 4096 bits criadas com o auxílio da Abin, tecnologicamente impossíveis de serem desfeitas. Ademais, cada arquivo de computador geral é crivado por um *hash* individual, que é como se fosse a "impressão digital" de cada um deles, de modo que, acaso fossem adulterados posteriormente, seria facilmente constatada a alteração, porque se trata de cálculo matemático caracterizado por impossível "engenharia reversa". Noutros termos, os arquivos que chegam às zonas eleitorais e são inseridos nas urnas têm garantia de autenticidade. Qualquer violação implicaria alteração do *hash*, de facílima verificação por auditoria.

Ainda que houvesse (e não há) a possibilidade de comprometimento do hardware; ainda que houvesse a possibilidade de adulteração do software (e não há); ainda que houvesse o desejo claro e direto dos próprios membros da Justiça Eleitoral (e, por óbvio, não há) de adulterar o resultado do sufrágio popular, há pelo menos duas medidas adicionais de segurança que tornam impossível qualquer espécie de fraude.

A primeira delas, visando a proteger a apuração eletrônica posterior, é o boletim de urna. No início da votação é impressa a zerézima, um "extrato" de cada uma das urnas, demonstrando que há zero votos lançados em seu sistema. Ao término do dia da eleição, a urna é encerrada e automaticamente emite novo "extrato", que é o boletim de urna, no qual constam todos os votos que ela recebeu. Isto tudo muito antes de ser retirada a memória de resultado para transmissão de dados via rede VPN criptografada à Justiça Eleitoral para totalização. Ou seja, ainda que se quisesse alterar o resultado apurado nos tribunais, o valor não "bateria" com o impresso nos boletins de urna, que é a primeira garantia contra qualquer vício na apuração.

A segunda, e pouco conhecida, que visa a proteger a integridade de software e hardware, é o sistema de votação paralela. Através deste procedimento, no dia da eleição, quando já preparadas e posicionadas nas escolas e demais locais de votação, são sorteadas algumas urnas eletrônicas, por sistema manual. Os equipamentos, aleatoriamente selecionados dentre as dezenas de milhares em cada estado, são recolhidos, lacrados, substituídos por urnas de contingência e levados à sede dos cartórios eleitorais. Em procedimento público e filmado, tais urnas são objeto de eleição simulada. Sem que a urna possa saber que foi retirada do local de votação, ela passa a receber votos simulados, lançados pelos presentes à auditoria pública, com a diferença de que são votos declarados, filmados e anotados. Ou seja, é sabido de antemão quantos e quais votos foram inseridos na urna. Ao término da votação, imprime-se seu boletim

de urna, para comparação com os dados previamente conhecidos. Houvesse qualquer fraude no software, suprimindo ou adicionando votos a este ou àquele candidato, seria imediatamente detectada no procedimento de votação paralela.

Demonstrados aqui três ou quatro dos mais de noventa sistemas de segurança desenvolvidos pela Justiça Eleitoral, os fatos não podem mais ser vítimas das teorias conspiratórias divulgadas na internet. Colocar em dúvida nossos avanços com o sistema de votação eletrônica, infinitamente mais seguro que o sistema anterior, conhecido por suas falhas, é despropositado. Para além disso, o sistema avança para a biometria, mais uma idealização de segurança e modernidade, a colocar a Justiça Eleitoral brasileira em posição de destaque mundial, seja pela segurança seja pela organização e ainda pela rapidez, a revelar o esforço diário de juízes, promotores e servidores da Justiça Eleitoral na busca da excelência, no que contam, no dia da votação, com a participação de milhares de cidadãos chamados a contribuir no processo eleitoral.

A Justiça Eleitoral Brasileira está de parabéns pelos avanços obtidos e a responsabilidade com que trata a questão, especialmente por trazer segurança e confiança no sistema eleitoral.