TECNOLOGIA

Representante da organização internacional Instituto de Engenheiros Eletricistas e Eletrônicos alerta para risco de não haver auditoria externa do sistema de segurança das urnas eletrônicas

Ciberataques podem ameaçar as eleições

PAULA PACHECO

São Paulo – O escândalo revelado recentemente sobre o uso de dados de usuários do Facebook pela empresa Cambridge Analytica e como a sua manipulação influenciou nas eleições presidenciais dos Estados Unidos tem colocado pesquisadores em alerta sobre os efeitos da falta de segurança não apenas nas empresas, mas também no processo eleitoral de outros países. Um deles é o Brasil.

André Gradvohl, integrante sênior do Instituto de Engenheiros Eletricistas e Eletrônicos (a organização internacional sem fins lucrativos IEEE) e professor da Faculdade de Tecnologia da Universidade de Campinas (Unicamp), alerta para o fato de o sistema eleitoral brasileiro não contar com nenhum tipo de auditoria de entidades externas. "Isso mostra o risco que existe de algum tipo de quebra de segurança", avalia o especialista. Segundo dados do Tribunal Superior Eleitoral (TSE), neste ano serão usadas 550 mil urnas eletrônicas para cerca de 147 milhões de eleitores.

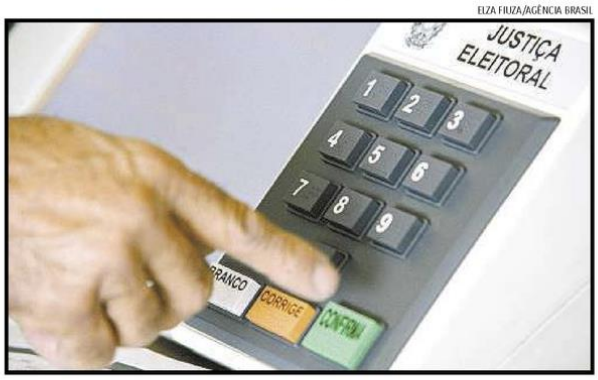
Gradvohl explica que sempre que há um software crítico, como no caso do sistema brasileiro de urnas eletrônicas, a auditoria externa pode garantir a rigidez no controle de segurança. Hoje, explica o professor, o TSE faz um workshop com pesquisadores um ano antes das eleições, durante cerca de uma semana, para testar aspectos de vulnerabilidade. Para o integrante do IEEE, esse teste deveria ser feito por mais tempo e mais vezes, não apenas um ano antes do pleito. "Nesse período é preciso entender o software e procurar erros. Não é um prazo suficiente para fazer os estudos necessários. Além disso, o sistema tem de ser avaliado regularmente", critica.

A proposta de Gradvohl é que o Brasil adote o conceito de software aberto para as urnas eletrônicas. Apesar de parecer ruim, já que ampliaria o acesso, seria uma forma de os pesquisadores buscarem brechas no sistema. "Hoje, a opção é pela segurança por obscuridade. O sistema é trancado para que ninguém tenha acesso, mas isso não impede que seja descoberta uma porta de entrada por meio de alguma falha existente", explica.

O especialista aponta outro problema de segurança nas urnas eletrônicas brasileiras. A chave de segurança, ou chave criptográfica, é a mesma para todas. Ou seja, se um invasor conseguir quebrar a segurança de uma urna, terá acesso a todas elas. Para Gradvohl, a solução seria que cada urna tivesse a sua chave, o que diminuiria os impactos no caso de ataque cibernético. "Imagine que cada urna é um cadeado. Se você tem a mesma chave, ou criptografia, para abrir todos os cadeados é claro que o risco é bem maior do que ter uma chave para cada um deles", exemplifica.

O representante do IEEE não tem um valor exato de quanto seria necessário investir para individualizar as chaves de segurança das urnas eletrônicas brasileiras. Por alto, ele calcula que seria necessário desembolsar alguns milhões de reais. Segundo o professor, o TSE tem equipe técnica qualificada para fazer esse tipo de desenvolvimento. Já no caso da autoria externa, proposta por Gradvohl, o tribunal poderia fazer uma convocação por meio de editais e contar com a participação de universidades.

ELZA FIUZA/AGÊNCIA BRASIL



Segundo o TSE, serão usadas 550 mil urnas eletrônicas para cerca de 147 milhões de eleitores neste ano

FRAGILIDADE Gradvohl lembra que outra forma de manipular os resultados das eleições é por meio de ações nas redes sociais, como aconteceu nos Estados Unidos. Para o especialista, o Marco Civil da Internet brasileiro trata com pouca profundidade da questão da privacidade de dados. Se essas informações são manipuladas, como fez a Cambridge Analytica, é possível disparar o chamado "efeito manada", levando eleitores a acompanharem tendências criadas por softwares e inteligência artificial.

"O Brasil tem muito a evoluir no que diz respeito à proteção de dados pessoais. Hoje, é possível monitorar todo o comportamento das pessoas tanto nas redes sociais quanto fora delas, como hábitos de consumo, tipo de pagamento preferido, e com isso direcionar propagandas que muitas vezes não temos a menor consciência. Simplesmente, extraem dados sobre o nosso comportamento e os usam da forma que querem. Da mesma forma podem fazer isso para direcionar a preferência por esse ou aquele candidato nas eleições", adverte.

COMPROVANTE

O Tribunal Superior Eleitoral (TSE) aprovou resolução que estabelece o registro impresso do voto nas eleições deste ano. Ao todo, 30 mil das 550 mil urnas eletrônicas, o equivalente a cerca de 5%, terão um módulo de impressão acoplado. Para que o mecanismo não sirva como uma espécie de comprovante de compra de voto, o eleitor não terá acesso ao registro em papel. Com a novidade, assim que o eleitor votar será impresso um comprovante, que irá para uma urna plástica lacrada e descartável, o que impedirá o seu contato com o papel. Esse voto impresso terá, além de mecanismos de controle, um código usado como forma de atestar a autenticidade das informações. No entanto, não haverá nenhum dado que permita identificar o eleitor. Ao final da votação, a Comissão de Auditoria da Votação Eletrônica será responsável por organizar os trabalhos de verificação dos registros.