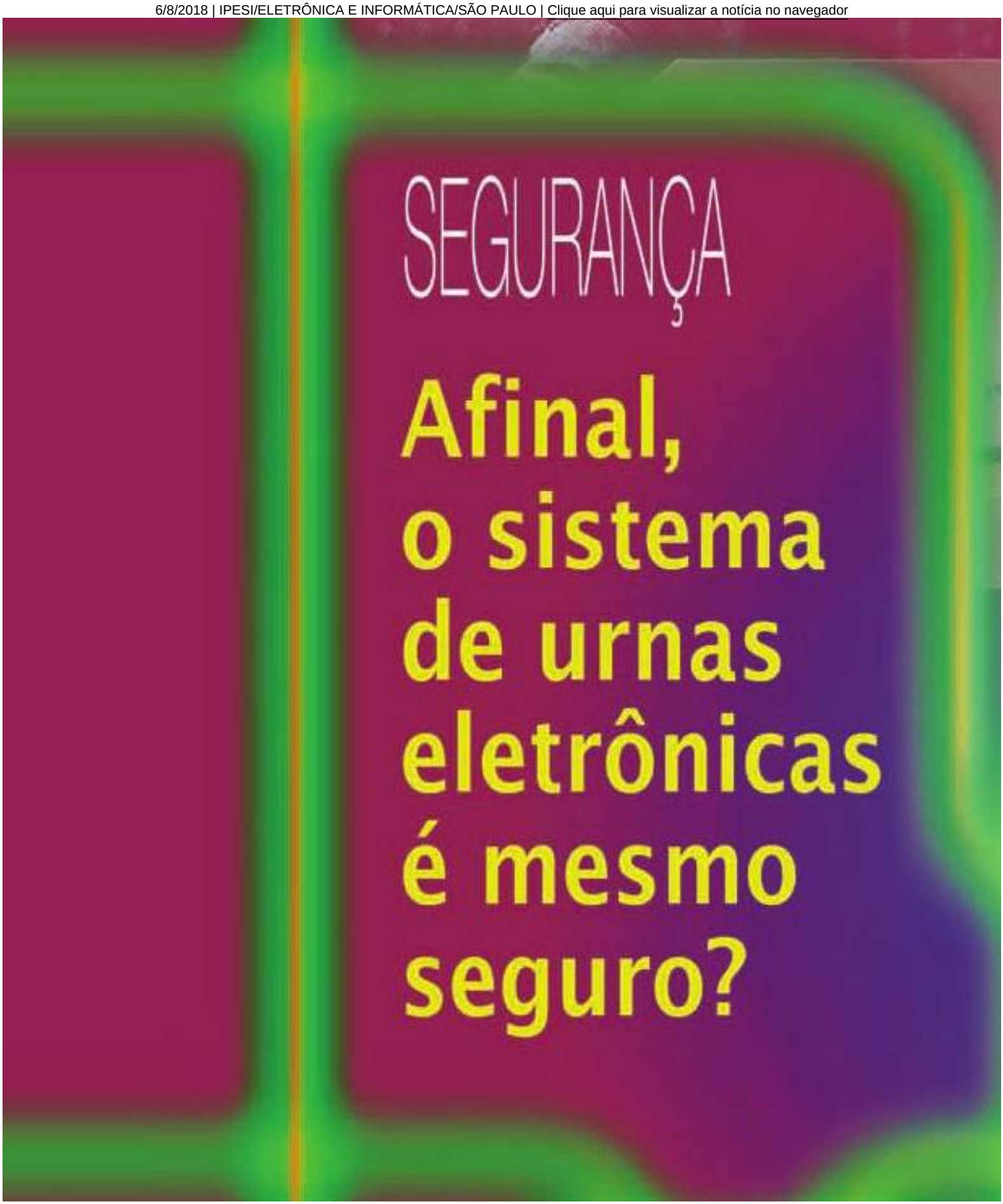
SEGURANÇA
Afinal,
o sistema
de urnas
eletrônicas
é mesmo
seguro?

Quanto o sistema eleitoral brasileiro é seguro?

Sistema de votação eletrônico necessita de proteção para evitar invasões, fraudes e manipulações

O escândalo de manipulação de milhões de dados do Facebook pela Cambridge Analytica soou um alerta: o eventual vazamento desse conteúdo ou seu uso por empresas de marketing pode influenciar eleições ou mesmo o comportamento de um grupo de usuários, com o efeito "manada".

André Gradvohl, membro sênior do Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) e professor da Faculdade de Tecnologia da Universidade de Campinas (Unicamp), reforça esse alerta. "O Facebook é o caso mais relevante no momento porque é uma das redes sociais mais populares no mundo e chamou bastante atenção da mídia, em função das consequências que pode ter causado às eleições presidenciais americanas de 2016. Dependendo das investigações e de novos fatos que podem surgir a partir desse escândalo, podemos testemunhar outros desdobramentos, com consequências no Brasil, inclusive", afirma.

E, com a proximidade das eleições gerais de outubro, o Brasil chama especial atenção pelo fato de utilizar um sistema de votação totalmente eletrônico, que necessita de proteção para evitar invasões, fraudes e manipulações. Do ponto de vista tecnológico, o que é possível utilizar para proteger os votos e garantir um resultado honesto? "Atualmente, há diversas tecnologias que podem melhorar a segurança dos votos e garantir que o resultado da eleição representa fielmente a vontade do povo", afirma Gradvohl. "Para ter um sistema de eleição eletrônica confiável, são necessárias que algumas propriedades sejam satisfeitas. As principais são o sigilo e a integridade. Outras são a elegibilidade (apenas eleitores habilitados poderão votar), a equidade (resultados não devem ser antecipados para evitar influenciar eleitores que ainda não votaram), a resistência à coação (o comprovante do voto não deve identificar a escolha do eleitor), as verificabilidades individual e universal (respectivamente, a possibilidade de o eleitor verificar que seu voto foi contabilizado e que o resultado da eleição considerou todos os votos)."

Em relação às tecnologias, o membro do IEEE destaca que a criptografia é a mais usada atualmente, pois garante as propriedades referentes ao sigilo e a integridade dos dados. Porém, ressalva ele, outras propriedades precisam ser reforçadas com tecnologias mais atuais. "Blockchain tem potencial para ser uma das tecnologias utilizadas para garantir as propriedades necessárias para a votação eletrônica. No entanto, para um país do tamanho do Brasil, é necessário mais estudos e adaptações antes da tecnologia Blockchain ser colocada em prática", observa.

Auditoria necessária - Apesar de todos os avanços tecnológicos, ainda é alto o grau de ceticismo em relação à urna eletrônica no Brasil, sobretudo por causa da dificuldade de se auditar, de forma independente, tanto a eleição em si, quanto o software embutido na urna eletrônica. "Nesse sentido, o Princípio de Kerckhoffs diz que um sistema deve ser seguro, mesmo que tudo sobre o sistema seja conhecido publicamente, exceto a sua chave (criptográfica). Portanto, um sistema que mantenha sua segurança por obscuridade, isto é, porque as pessoas desconhecem seu funcionamento, é no mínimo classificado como inseguro", explica o professor Gradvohl.

Além disso, a auditoria de qualquer software é necessária para atestar sua segurança, incluindo a inspeção do código fonte, testes de software, testes de invasão e outras ações que buscariam fragilidades na segurança do software, tudo isso seguindo uma metodologia rigorosa e específica. Porém, conforme observa o membro do IEEE, auditorias dessa magnitude demandam um tempo razoável. "O último teste público de segurança (TPS) da urna eletrônica no Brasil, promovido pelo TSE, utilizou apenas cinco dias (de 27 de novembro a 1º de dezembro de 2017), incluindo a preparação do ambiente de testes e a produção do relatório parcial. Esse período é curtíssimo, mesmo considerando que várias equipes bem capacitadas participaram do teste público", avalia.

Antes terceirizado, hoje o software eleitoral brasileiro é majoritariamente desenvolvido por equipe do Tribunal Superior Eleitoral (TSE). "O problema não é a equipe de desenvolvimento (interna ou externa ao TSE), pois, caso seja bem qualificada e atenta ao estado-da-arte, então isso basta para desenvolver um software com a segurança necessária", explica Gradvohl. Porém, citando a chamada Lei de Linus (segundo a qual "dados olhos suficientes, todos os erros são evidentes"), o professor acrescenta que "ter um software que possa ser auditado e esmiuçado por pessoas que não pertençam à equipe de desenvolvimento pode expor as falhas de segurança mais rapidamente. Após sua exposição, essas falhas podem ser corrigidas antes de se colocar o software em uso."

Portanto, alerta Gradvohl, o que aumenta o risco é o desconhecimento das vulnerabilidades do software e do hardware. "Nesse sentido, equipes de auditoria externa, que utilizem uma metodologia rigorosa, podem encontrar essas vulnerabilidades e repassar as informações para correção pela equipe de desenvolvimento", sugere.

Proteção - Mecanismos que protegem o software eleitoral brasileiro contra manipulações sofrem de falhas de projeto fundamentais, segundo apuraram alguns especialistas que a ele tiveram acesso. Todas as urnas compartilham o mesmo "segredo" para proteger o software e isso está diretamente inserido no código-fonte do equipamento, gerando ao menos 500 mil cópias dessa informação às

claras em cartões de memória, o que põe em dúvida confidencialidade, um dos pilares de qualquer sistema seguro. "A população sabe que um segredo compartilhado com mais do que duas pessoas não é mais um segredo. Além disso, a obtenção de uma chave criptográfica compartilhada desvendaria o segredo de todas as urnas usadas e comprometeria toda a eleição. O potencial para invasão ao usar essa política de chave única para todas as urnas é imenso", adverte o membro do IEEE. Solução? "Se cada urna possuísse uma chave própria, dificilmente um atacante envidaria esforços para quebrar esse segredo. A possibilidade de um ataque em massa seria bem menor nesse caso."

Como boa notícia, o professor destaca que parte das urnas do TSE já tem um módulo de segurança em hardware, certificado e testado, o que melhora os níveis de segurança, pois um atacante precisaria ter acesso físico ao equipamento e isso deixa rastros mais evidentes. "Esse módulo de segurança em hardware armazena e protege a chave criptográfica de cifração (chave privada)", explica. "No entanto, se for utilizado um software para manter a mesma chave criptográfica em todas as urnas, ter esse módulo implementado em hardware não traz nenhum benefício."

Nas eleições de outubro o TSE adotará o voto impresso em 6% das urnas eletrônicas, o que acrescentará ao pleito a propriedade de verificabilidade individual, ainda que parcialmente. "Isso é muito pouco, mas é um primeiro passo", avalia Gradvohl. "Para tornar o processo eleitoral mais transparente, outras propriedades também precisam ser implementadas para todos os eleitores, como, por exemplo, as propriedades à equidade, resistência à coação e a verificabilidade universal. Além disso, questões referentes ao sigilo e à integridade dos dados precisam ser aprimoradas, com técnicas mais tolerantes aos ataques e políticas mais transparentes que facilitem as auditorias."

Redes sociais - A recente intervenção russa nas redes americanas, que muitos consideram significativa para influenciar eleitores e eleger Donald Trump, acarreta novos questionamentos do mundo digital. "Redes sociais já são parte da rotina de muita gente, através das quais muitos dados pessoais são coletados, frequentemente sem que o usuário perceba. Em alguns casos, o usuário não precisa nem mesmo fazer parte daquela rede social. O simples acesso para verificar informações sobre alguém que está na rede social já é suficiente para coletar algumas informações básicas sobre quem está consultando a rede", avalia Gradvohl. "Na última audiência de Mark Zuckerberg no Congresso Americano, um dos congressistas - Ben Luján - denominou de perfil sombra as informações desse usuário que não pertence à rede social, mas que tem alguns dos seus dados coletados."

"Com essas informações, é possível traçar perfis dos grupos de usuários e campanhas podem ser feitas especificamente para esses públicos, cooptando as pessoas a partir do que elas anseiam ou das características que elas julgam ser importantes numa candidatura. Um candidato pode - caso conheça bem o público ao qual está se dirigindo - apresentar um discurso que o aproxima daquele público e construir uma imagem que atraia eleitores para a causa que defende, mesmo que não seja tão importante para o candidato", afirma o pesquisador membro do IEEE.

"De forma análoga, a imagem de um candidato adversário também pode ser corrompida ao apresentar, para um público ainda indeciso, por exemplo, características ou mesmo notícias falsas (fake news) que descredenciam aquele candidato ou o distanciam do anseio popular", acrescenta. "Ferramentas que utilizam a tecnologia Big Data são bastante adequadas para esses fins, pois conseguem extrair informações nem sempre muito evidentes de grandes volumes de dados. Além disso, essas ferramentas podem classificar os conjuntos de eleitores de acordo com suas características, tornando mais fácil a criação de campanhas ou narrativas direcionadas para esses grupos", conclui o professor.

Facebook - O acesso e a manipulação de dados de usuários do Facebook ganharam bastante atenção da mídia, por causa das consequências que podem ter causado às eleições presidenciais americanas de 2016. Porém, Gradvohl ressalva que o Facebook não é a única rede social utilizada pelas pessoas. Outras redes como o Youtube, o Instagram, o Twitter e o próprio Google também contêm muitos dados de usuários. "O eventual vazamento desses dados ou o uso deles por empresas de marketing pode influenciar eleições ou mesmo o comportamento de um grupo de usuários, com o efeito 'manada'", alerta o especialista, propondo que sociedade e governos estabeleçam regras para o uso desses dados.

"A comunidade europeia já deu passos na direção dessa regulamentação com a Lei de Proteção de Dados - GDPR (General Data Protection Regulation), aprovada em 2016 e que deve ser amplamente aplicada em 25 de maio deste ano, após um período de 2 anos de transição", destaca. No entanto, a GDPR protege apenas cidadãos europeus. Outros países, em especial o Brasil, ainda estão distantes de uma legislação adequada. "Embora o Marco Civil da Internet tenha sido regulamentado em 2016 no Brasil, essa lei não tratou efetivamente das questões referentes à proteção dos dados pessoais", avalia o membro do IEEE.