Valor ECONÔMICO

Imprimir ()

25/08/2017 - 05:00

Eleições sob ataques digitais

Por **Virgilio Almeida**



O problema foi claramente identificado em vários países. Nos últimos dois anos, várias eleições foram alvos de ataques digitais, também chamados de ciber-ataques, que ocorrem na internet e nas plataformas online, como Facebook, Instagram, YouTube, Twitter, Whatsapp e Google. Os ataques digitais, isto é, disseminação de notícias falsas, 'sites' falsos, manipulação de opiniões, vazamento de dados pessoais, guerra de informações, propaganda automatizada e uso de robôs nas mídias sociais, são diferentes faces das estratégias utilizadas para influenciar processos eleitorais em países democráticos.

Cada vez mais, são nessas plataformas que os cidadãos consomem e compartilham notícias políticas, gastam tempo defendendo ou atacando posições partidárias e decidem o rumo de seus votos. No Reino Unido, por exemplo, uma pesquisa recente mostrou que 84% dos jovens entre 18 e 24 anos consideram a internet a principal fonte de informação. O mesmo ocorre para 62% da faixa da população que tem 25 e 34 anos e 53% para aqueles entre 35 e 44 anos.

Estados Unidos, Reino Unido, França, Holanda e Montenegro são países cujas eleições sofreram algum tipo de ataque digital, com maior ou menor interferência nos resultados finais. A Alemanha se preparou antecipadamente para se defender de ataques nas eleições que ocorrem no final de setembro. Em vários casos, a origem dos ataques estava fora do território do país, sendo a Rússia o país mais frequentemente responsabilizado pelos ataques. O que se percebe das análises dos ataques ocorridos é que a maioria das campanhas políticas não está preparada e não tem as ferramentas e a tecnologia necessárias para se defender de ataques cibernéticos.

Dentre as várias técnicas de disseminação de notícias falsas e manipulação de opinião na internet e nas mídias sociais estão os robôs, também conhecidos como 'bots'. São agentes de software (i.e, código de computador) que podem imitar o que os humanos fazem em várias situações. São usados para criar conteúdo nas mídias sociais e interagir com pessoas. Cada vez mais, os bots têm sido usados para finalidades políticas, como, por exemplo, automatizar propaganda eleitoral, inflar o número de seguidores que um político tem, gerar comentários negativos sobre adversários ou tentar distorcer e influenciar o discurso político.

O cenário político brasileiro é um terreno fértil para ataques digitais. Há vários alvos atraentes para ataques, dentre eles a avalanche de denúncias de corrupção, a descrença com os atuais políticos, o acirramento da polarização ideológica e partidária

Os bots podem operar sem intervenção humana e têm condições de adaptar ao contexto onde operam. Pesquisas publicadas pela Universidade de Oxford estimam que na semana anterior ao dia da eleição para presidente dos Estados Unidos, 19 milhões de contas operadas por bots geraram comentários no Twitter de apoio a Donald Trump ou Hillary Clinton. A preocupação com o uso de bots torna-se mais forte quando se percebe que apoios populares e opinião pública podem ser fabricados artificialmente ou manipulados pelos bots e com isso distorcer o debate de ideias e valores, tão essenciais numa eleição.

Ainda escaldados pela guerra de informações e ataques digitais que permearam a eleição do presidente Trump, instituições da sociedade americana buscam alternativas para proteger o processo democrático nos Estados Unidos. A Universidade de Harvard lançou recentemente um novo projeto chamado "Defendendo a Democracia Digital", que visa criar condições, conhecimentos e tecnologia capazes de mitigar os vários tipos de ataques online, que ameaçam a democracia americana. O grupo é formado por acadêmicos, ex-participantes das campanhas de Hillary Clinton e Mitt Romney, junto com especialistas em segurança e executivos das grandes empresas de tecnologia.

O cenário político brasileiro é um terreno fértil para ataques digitais. Dentre os fatos que se destacam no atual cenário político do país, vários deles mostram-se alvos atraentes para ataques. Dentre eles estão a avalanche de denúncias de corrupção, a descrença da população com os atuais políticos, o acirramento da polarização ideológica-partidária e as eleições de 2018. Esses fatos já têm forte ressonância nas mídias sociais, onde milhões de brasileiros postam frequentemente fatos, opiniões e notícias sobre suas paixões, frustrações e ódio com a situação política do país. Além disso, o tecido social do país é claramente propício aos ataques digitais, devido a diversos fatores.

Cerca de 84% da população, ou seja por volta de 185 milhões de brasileiros, vivem em zonas urbanas, onde o acesso a internet e às mídias sociais fazem parte do cotidiano de grande parcela dos brasileiros. Mais de 90 milhões de brasileiros assistem os canais do YouTube e mais de 102 milhões de brasileiros compartilham seus dados, opiniões e notícias no Facebook todos os meses. Um estudo recentemente publicado pela Universidade de Oxford apresenta detalhes do uso de bots em três momentos políticos recentes que foram a eleição da presidente Dilma em 2014, o impeachment da presidente em 2016 e as eleições municipais do Rio de Janeiro em 2016.

Face a esse cenário, resta então a pergunta: o que o governo e a sociedade estão fazendo para proteger as eleições de 2018? Como as lições dos outros países que sofreram ataques digitais podem e devem ser aproveitadas? Como obter mais transparência nas campanhas eleitorais quanto ao uso de bots e propaganda automatizada? Como minimizar os efeitos da invasão de bots nas mídias sociais, as propagandas eleitoriais automatizadas, as notícias falsas e a manipulação de informações por diferentes grupos de interesse nacionais ou internacionais? São perguntas chaves que requerem um posicionamento proativo do governo e da sociedade, para que tenhamos eleições democráticas e seguras em 2018.

Virgilio Almeida é professor Associado ao Berkman Klein Center na Universidade de Harvard e foi secretário de política de informática no Ministério da Ciência, Tecnologia e Inovação de 2011-2015.