



Na Mídia

07/12/2021 | [MIT Technology Review](#)

O uso de social bots em campanhas eleitorais e os desafios para a democracia

É preciso estruturar uma governança de algoritmos para viabilizar a transparência sobre esses sistemas e estabelecer políticas públicas de combate à desinformação para mitigar os efeitos nocivos do uso dessas tecnologias.

Eduardo Magrani | Paulo Rodrigo de Miranda

A rampa de lançamento da campanha de Donald Trump inicia com um fato falso: o suposto nascimento de Obama fora do território dos Estados Unidos. A partir desse contexto, as eleições de 2016 nos EUA foram marcadas pela viralização de *fake news*, sendo constatado que vinte e três dos cinquenta boatos de notícias falsas de melhor desempenho encontrados no *Facebook* envolviam o tema da propaganda eleitoral norte-americana, conforme análise realizada pela *BuzzFeed News*.

Por sua vez, nas eleições presidenciais que ocorreram no Brasil, pesquisas indicam que 98% dos eleitores do presidente eleito Jair Bolsonaro foram expostos a uma ou mais notícias falsas durante a eleição, sendo que 89% acreditaram que os fatos eram verdade, segundo estudo da *Avaaz*. Dentre as principais notícias falsas espalhadas entre os eleitores destacaram-se: a fraude nas urnas eletrônicas; a implementação de um suposto “kit gay” nas escolas por Fernando Haddad (candidato da oposição); e que o agressor de Bolsonaro (Adélio Bispo de Oliveira) era filiado ao PT.

Nessa perspectiva, diversos debates têm surgido em relação às implicações e consequências das notícias falsas implementadas através do uso de plataformas digitais e das ferramentas tecnológicas empregadas como estratégia política em campanhas eleitorais, tal como o uso de social *bots* e *microtargeting*. Em uma análise mais ampla, a desinformação pode ser vista como um fenômeno derivado da mudança na forma como as sociedades passaram a produzir e consumir informação política.

Os meios de comunicação de massa são instrumentos essenciais para a implementação e manutenção de uma democracia representativa e configuram um dos principais mecanismos de atuação dos partidos políticos em

campanhas eleitorais. Nesse viés, as plataformas digitais, em especial as redes sociais, passaram a assumir um papel central nas estratégias de publicidade e manipulação nas campanhas eleitorais.

Com a expansão da *big data* houve um crescimento do poder das plataformas, deslocando os algoritmos para o papel de *gatekeeper* dos fluxos informacionais, que passam a realizar os filtros de conteúdo personalizado para cada usuário. Esses novos mecanismos de modulação personalizados perturbam os processos já frágeis da formação da vontade democrática, minando o pluralismo da mídia e o diálogo deliberativo. Os fluxos informacionais percorrem verdadeiros jardins murados imperceptíveis aos usuários. Além disso, inexistem informações quanto aos mecanismos e critérios de distribuição empregados pelos algoritmos na disseminação de conteúdos geridos pelas grandes plataformas.

A personalização de conteúdo com a formação de bolhas de filtro é um dos principais elementos que conduzem à fragmentação e à polarização de opiniões. Contudo, ao mesmo tempo, é esse mesmo mecanismo de filtragem de informação que mantém a lógica econômica das plataformas, sendo sua chave de sobrevivência. A segregação ideológica promovida pelas plataformas e mídias sociais empobrece o debate na esfera pública virtual e desintegra o ambiente que é diversificado e necessário para o desenvolvimento de ideias e opiniões, fundamentais para a formação de um consenso.

Ademais, as plataformas digitais acabaram suprimindo a demanda por verdades políticas alternativas, por narrativas contendo “viés de confirmação”, intensificando informações que estejam alinhadas aos pontos de vista dos usuários dessas plataformas. Dentro desse novo ambiente tecnológico e vulnerável, novas estratégias de marketing político têm sido empregadas para a manipulação da opinião pública, em especial a utilização de *social bots* e de *microtargeting*.

Os usos de *social bots* servem como verdadeiras estratégias políticas no intuito de influenciar os conteúdos gerados, ao automatizarem as postagens, comentários e interações com outros usuários, visando influenciar e moldar as atitudes dos eleitores. Os perfis falsos na esfera digital exploram todas as vulnerabilidades desse ecossistema, se valendo da coleta de dados pessoais, dos preconceitos e das emoções, ao intensificar os sentimentos dos usuários na circulação das informações falsas e ao alavancar conteúdos e indivíduos de forma artificial.

Os usuários dentro do ambiente virtual, muitas vezes, possuem dificuldade em identificar as narrativas políticas dentro de uma análise racional, porquanto os filtros algoritmos reduzem a capacidade dos usuários de se proteger da manipulação de interesses escusos de políticos, agentes privados ou governos. Isso revela o potencial das plataformas em influenciar as crenças e os comportamentos políticos dos usuários.

Além do uso de *social bots*, a publicidade personalizada ou comportamental (*microtargeting*) tem sido listada como um mecanismo importante para a ampliação do alcance do conteúdo patrocinado. A segmentação e a adaptação são usadas há muito tempo para aumentar o impacto das mensagens políticas, contudo, a segmentação online e as novas técnicas de adaptação estão sendo empregadas de maneiras novas, sutis e poderosas, com grande potencial para influenciar o comportamento e as escolhas dos eleitores.

A utilização de *microtargeting* demonstra a facilidade e a precisão que as empresas e os partidos políticos encontram para direcionar suas mensagens a determinados eleitores, transformando grupos heterogêneos em vários subgrupos homogêneos no intuito de obter maior eficiência da publicidade política direcionada. Atualmente, é possível desenvolver perfis de eleitores de forma detalhada, correlacionando diversos dados, tais como informações demográficas (idade, sexo filiação partidária), sobre atividades econômicas, sociais e políticas do público-alvo em potencial, além de informações do comportamento desses usuários que permite uma visão adicional sobre pensamentos, crenças e características psicológicas.

O uso abusivo de *social bots* e do *microtargeting* é um problema relacionado a uma das camadas da estrutura da desinformação, porquanto as referidas ferramentas tecnológicas serviriam de instrumentos para a ampliação do alcance da desinformação. Desse modo, o combate à desinformação está intrinsecamente relacionado à resolução dos problemas oriundos do uso abusivo de *social bots* e *microtargeting*.

Diante da erosão da confiança nas instituições públicas e de rupturas políticas apoiadas em redes de desinformação, esse novo modelo de campanha orientada por dados apresenta um desafio sistêmico e institucional, que demanda uma combinação de abordagens políticas e regulamentares. Desse modo, exige-se uma atuação multisetorial, na qual os centros de pesquisa, entidades da sociedade civil e jornalistas assumam um papel fundamental para monitorar o potencial impacto da desinformação na sociedade.

Desde 2018, a União Europeia tem adotado diversas medidas preventivas buscando maior responsabilidade algorítmica e transparência. Através do relatório elaborado pelo Grupo de Especialistas de Alto Nível (*High-Level Expert Group – HLEG*), criado pela Comissão Europeia, promoveu-se a implementação de um Código de Boas Práticas firmado com o Facebook, Twitter, Microsoft, Google, Mozilla e TikTok, no qual houve a instituição de uma política voltada ao bloqueio de *bots* e perfis falsos quando utilizados para fins de desinformação.

Ademais, o HLEG elencou diversas medidas no intuito de aumentar a transparência em torno da desinformação, tais como: i) ações para aumentar a transparência da origem do financiamento, identificando o conteúdo patrocinado, especialmente quando envolver publicidade política; ii) indicadores de transparência que permitam sinalizar fontes confiáveis e identificáveis tanto nos resultados dos mecanismos de busca quanto nos *feeds* de notícias das mídias sociais; iii) fornecimento de informações básicas sobre o funcionamento dos algoritmos que selecionem e exibem informações.

A identificação de conteúdo patrocinado e o fornecimento de informações básicas sobre o funcionamento dos algoritmos que selecionam e exibem informações é fundamental para viabilizar a análise dos pagamentos sobre influenciadores humanos e uso de *social bots* para promover determinadas mensagens na esfera pública virtual. A abertura, nesse sentido, permitiria a colaboração com organizações independentes que possuem atividades de verificação de fatos, bem como permitiria maior compreensão sobre a aparente popularidade de um influenciador ou de uma determinada informação online, que muitas vezes pode estar sendo impulsionada com investimentos direcionados ou ser resultado de uma manipulação artificial.

Com efeito, a busca de soluções alternativas ao combate da desinformação nas redes sociais demanda a construção de novos modelos que devem ter como norte o papel sociopolítico que as plataformas digitais possuem no processo democrático, especialmente porque estão em uma posição privilegiada para agir dentro da esfera pública automatizada. Nesse viés, atrair a responsabilidade das plataformas para o enfrentamento à desinformação é essencial quando se busca conter os incentivos econômicos que premiam notícias sensacionalistas.

A criação de indicadores de transparência nos algoritmos das plataformas garantiria que notícias de qualidade e confiáveis estivessem substancialmente disponíveis e pudessem ser facilmente encontradas no ambiente digital. Tal medida, além de significar uma relevante melhoria da transparência, reforçaria o desenvolvimento do pensamento crítico por parte dos usuários, que é essencial no combate à desinformação.

Com efeito, o primeiro passo para o Brasil seria que as autoridades públicas se conscientizassem da importância do apoio de uma rede independente de centros de pesquisa e entidades da sociedade civil, sobre a desinformação, criando-se um canal aberto para jornalistas e pesquisadores de diferentes áreas relevantes, incluindo das próprias plataformas. Nesse sentido, embora não existam propostas das autoridades públicas, similares às da União Europeia,

voltadas especificamente ao estabelecimento de diretrizes preventivas ao combate a desinformação, o TSE tem adotado diversas medidas comprometidas com a democracia.

A Suprema Corte eleitoral tem se destacado ao desenvolver campanhas contra a desinformação, realizar acordos com entidades civis para fins de verificação das notícias falsas e adotar parcerias com as plataformas no combate à desinformação. Mais recentemente, em novembro de 2021, o TSE firmou parceria com a Autoridade Nacional de Proteção de Dados (ANPD), por meio do acordo de cooperação técnica nº 4/2021, com o objetivo de adoção de ações conjuntas e coordenadas visando promover e zelar pela adequada aplicação da legislação de proteção de dados pessoais no âmbito eleitoral, tendo como uma de suas premissas a conciliação entre os princípios relacionados à proteção de dados pessoais e o interesse público intrínseco à atividade político-partidária e ao contexto eleitoral.

Essa medida revela-se como uma das partes necessárias para a “construção de uma ponte” entre a ANPD e a Justiça Eleitoral defendida em diversas oportunidades por Francisco Brito Cruz e Heloisa Massaro. Ademais, ainda que existam alguns dilemas para equacionar a atividade de fiscalização envolvendo as funções da ANPD e do TSE, a parceria firmada entre as instituições, relacionada ao compartilhamento de estudos, pesquisas, informações e orientações técnicas quanto ao conteúdo e à interpretação da LGPD, torna-se um passo importante para auxiliar o TSE na sua competência de regulamentação da propaganda eleitoral na internet (prevista no art. 57-J da Lei 9º.504/97), especialmente diante do atual cenário envolvendo novas estruturas e ferramentas de marketing digital baseadas na coleta e tratamento de dados pessoais.

Por sua vez, existem diversos projetos de lei propostos a fim de enfrentar os problemas relacionados à desinformação no Brasil. Contudo, a maioria deles visa criminalizar o ato de disseminação de notícias falsas, havendo pouca preocupação com o estabelecimento de políticas públicas e diretrizes voltadas ao combate preventivo da desinformação, bem como a realização de estudos que permitam a implementação de uma forma contínua de avaliação e monitoramento dos impactos da desinformação na sociedade.

Em maio de 2020, foi apresentado no Senado Federal o Projeto de Lei nº 2630/2020 (apelidado de “PL da *fake news*”). O referido projeto tem sofrido duras críticas de parlamentares e entidades da sociedade civil, especialmente porque seu trâmite legislativo tem ocorrido sem um debate prévio com a sociedade civil e sem o embasamento de estudos aprofundados sobre o tema.

No PL 2630/2020, há a definição de conta inautêntica e rede de distribuição artificial (art. 5º, II), que praticamente envolveriam a utilização de *social bots* e *botnets*. Ademais, o artigo 6º do referido projeto determina que os provedores de redes sociais e serviços de mensageria privada, no âmbito e nos limites técnicos de seu serviço, devem adotar medidas para vedar o funcionamento de contas inautênticas e contas automatizadas não identificadas.

Além disso, há a previsão que os provedores de aplicação de internet disponibilizem mecanismos de recurso e devido processo quando realizarem a indisponibilização de conteúdos e contas (art. 12, caput e §3º), bem como que os provedores de redes sociais produzam relatórios de transparências, contendo diversas informações, dentre as quais o “número total de contas automatizadas e de redes de distribuição artificial detectadas pelo provedor” (art. 13, caput e §1º, V).

Nesse ponto, torna-se relevante registrar que mesmo diante de lacunas regulatórias para lidar com os avanços tecnológicos oriundos da esfera pública virtual, em especial o impacto ocasionado pela nova forma de marketing político com a utilização de *social bots* e *microtargeting*, existem alguns mecanismos normativos aplicáveis ao uso de *social bots* no Brasil.

Com efeito, quando se trata do direito à liberdade de expressão previsto na Constituição Federal, encontra-se no lado oposto a previsão constitucional da vedação ao anonimato (CF, art. 5º, IV). O aparente conflito entre as duas

disposições constitucionais demanda, na contemporaneidade, uma acomodação hermenêutica da estrutura normativa.

A proteção da privacidade, dos dados pessoais e da liberdade de expressão, além de expressamente previstas no Marco Civil da Internet (Lei nº 12.965/2014), são fundamentais para um ambiente virtual saudável e seguro. Desse modo, ainda que o emprego abusivo de *social bots* e *botnets* implique na criação de um simulacro quanto ao legítimo exercício da liberdade de expressão, a vedação ao anonimato, por si só, não seria suficiente para combater de forma eficaz os efeitos nocivos da manipulação do debate público, além de colocar em risco outros direitos fundamentais que também merecem resguarda constitucional, em especial a garantia do acesso à internet como uma ferramenta imprescindível ao exercício da cidadania, que demanda, para tanto, a proteção da privacidade em suas mais diferentes facetas.

Dentro desse contexto, exige-se uma interpretação temperada da vedação ao anonimato quando se trata do embate dentro da esfera virtual envolvendo o entrelaçamento entre o emprego de mecanismos fraudulentos no exercício abusivo do direito à liberdade de expressão e a proteção da privacidade (em especial a intimidade dos usuários na internet sob o viés da proteção do sigilo constitucional) e dos dados pessoais (recentemente enquadrado como um direito fundamental pelo STF). De igual modo, o art. 22 da Lei nº 12.965/2014 (Lei do Marco Civil da Internet) aborda vários requisitos que devem conter o pedido para o fornecimento de registros de conexão ou de registros de acesso a aplicações da internet, servindo como parâmetros legais para o caso de eventual quebra de sigilo de dados que envolvam perfis automatizados empregados de forma irregular no âmbito da internet.

Em um segundo momento, com o advento da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018), o princípio da boa-fé e da privacidade contextual devem ser observados pelos partidos políticos e empresas de marketing digital, de modo que o emprego de *social bots* tendentes a manipular o debate político configura conduta abusiva e em desconformidade com as diretrizes da LGPD.

Por fim, a legislação eleitoral veda a veiculação de conteúdos de cunho eleitoral por meio de cadastro de perfis falsos ou anônimos, bem como a utilização de técnicas que ampliem artificialmente a repercussão de determinado conteúdo eleitoral (Lei nº 9.504/97, art. 58-B, §2º e §3º). Desse modo, além de configurar violação da legislação eleitoral, a utilização de perfis falsos automatizados (*social bots* e *botnets*) se enquadraria na hipótese de abuso de poder político diante da utilização indevida dos meios de comunicação social (art. 30-A da Lei nº 9.504/97 e art. 22 da LC 64/90).

A realização de campanhas eleitorais depende da confiança das instituições públicas e do acesso transparente e verossímil de informações, até porque os partidos políticos são entidades essenciais à estruturação da democracia representativa. Por essa razão, a utilização de *social bots* e *microtargeting* em campanhas políticas demanda a estruturação de uma governança de algoritmos de forma a viabilizar a transparência sobre a funcionalidade desses sistemas, sendo essencial o estabelecimento de novas políticas públicas na formulação de diretrizes de combate à desinformação e parcerias com o setor privado na busca de mitigar os efeitos nocivos do uso abusivo dessas novas ferramentas tecnológicas.

A realização de campanhas eleitorais depende da confiança das instituições públicas e de uma esfera de debate política que respeite os valores básicos de uma democracia.

Este artigo foi produzido por Eduardo Magrani, Presidente do Instituto Nacional de Proteção de Dados no Brasil e Sócio das áreas de “Privacidade, Tecnologia e Cibersegurança” e “Propriedade Intelectual e Inovação” do Demarest Advogados, em parceria com Paulo Rodrigo de Miranda, Analista do Ministério Público Federal do Rio

Grande do Sul (MPF/RS), Especialista em Direito Público e Integrante do projeto de pesquisa: a ressignificação do constitucionalismo