Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

ELEIÇÕES ROBÓTICAS: O USO DE SOCIAL BOTS EM CAMPANHAS ELEITORAIS NOS ESTADOS UNIDOS E NO BRASIL

Jessica Araujo Silva Zanatta; **Julia Sanches Baptista**
jessica.zanatta@fatec.sp.gov.br; julia.baptista@fatec.sp.gov.br

Henri Alves de Godoy
Professor orientador
henri.godoy@fatec.sp.gov.br

Resumo

O artigo aborda um estudo de caso sobre uso deliberado de métodos de manipulação de informação, por meio de *social bots* e redes sociais. A partir das pesquisas e revisões bibliográficas demonstra-se como a aplicação de técnicas de manipulação pode influenciar em comportamentos e opiniões, podendo inclusive gerar riscos para a estabilidade Nacional. O estudo terá como foco ações de social bots nas eleições presidenciais dos Estados Unidos (2016) e Brasil (2018). Com base nos estudos, conclui-se que a utilização de social bots pode contribuir para a criação artificial de um ambiente informacional favorável para sustentar narrativas, influenciando a percepção dos usuários e radicalizando as discussões.

Palavras-chave: redes sociais; cibersegurança social; segurança da informação.

Abstract

The article deals with a case study on the deliberate use of information manipulation methods through social bots and social networks. Based on research and literature reviews, it is demonstrated how the application of manipulation techniques can influence behaviors and opinions and may even generate risks for National stability. The study will focus on the actions of social bots in the presidential elections of the United States (2016) and Brazil (2018). Based on the studies, it is concluded that using social bots can create a favorable informational environment to sustain narratives, influencing users' perceptions and radicalizing discussions.

Keywords*: social medias; social cybersecurity; information security.*

Jessica Araujo Silva Zanatta
Julia Sanches Baptista

ELEIÇÕES ROBÓTICAS: O USO DE SOCIAL BOTS EM CAMPANHAS ELEITORAIS NOS ESTADOS UNIDOS E NO BRASIL

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Segurança da Informação.

Americana, 02 de dezembro de 2022

Banca Examinadora:

Profº. Drº. Henri Alves de Godoy (Presidente)
Doutorado
FATEC Americana

Profº. Drº. Rodrigo Rosalis da Silva (Membro)
Doutorado
FATEC Americana

Profº. Esp. Evandro Santaclara
Especialista
FATEC Americana

1. Introdução

Se em sua criação, em 1969, as raízes do conceito de redes de computadores estavam no ambiente acadêmico e militar, ao longo das décadas e, especialmente com a intensificação do uso de tecnologias móveis, a Internet tornou-se parte do cotidiano do cidadão comum. Não é exagero afirmar que as atividades online romperam não somente barreiras geográficas, mas também comportamentais, uma vez que a vida online e offline são hoje uma só para grande parte dos usuários com o avanço das redes sociais e sua crescente adesão mundial. Estas mídias têm desempenhado papel fundamental para o sucesso de ações distintas, uma vez que ao longo dos anos passam a desempenhar novas funções antes pouco exploradas (KIMURAI et al., 2008), como, por exemplo, vendas e *marketing* digital. Neste contexto comercial a utilização de *bots* se mostrou uma grande aliada.

Bot é o nome atribuído para programas criados para automatizar tarefas, em geral, repetitivas, que podem ser roteirizadas. Surgido da palavra inglesa "*robot*", esse tipo de *software* tem ganhado popularidade ao longo dos últimos anos, acompanhando uma tendência de ampliação dos serviços e recursos baseados nas redes (ABOKHODAIR et al. 2015). Porém, a ferramenta não é necessariamente uma novidade para a computação. O primeiro *bot* de Internet foi desenvolvido no ano de 1993 como um agente de inteligência artificial voltado para tarefas de ftp, telnet e mensagem (e-mail), além de exercer atividades de manipulação de arquivo (ETZIONI e WELD, 1994 apud YADAV, 2022). Embora sua "inteligência" fosse limitada, algumas das características serviram como modelo, como a interface para a Internet e comportamento adaptativo em resposta a condições transitórias do sistema (YADAV, 2022).

Ao direcionar este conceito para as redes sociais, os bots passaram a ser tratados como *social bots* ou "robôs sociais". Neste contexto, os *social bots* são utilizados para a automação e controle de perfis em redes sociais e podem, portanto, realizar atividades online (BOSHMAH et al., 2011; DAPP, 2017 apud LEITE, 2018). Esses robôs sociais, capazes de apresentar comportamentos parcialmente ou mesmo completamente autônomos, são arquitetados de maneira a imitar o comportamento de usuários humanos (CHEN et al., 2022). Na rede social Twitter, por exemplo, um *social bot* controlando uma conta pode tomar ações como dar *likes*, *retweet*, seguir, comentar e citar o conteúdo de outros usuários (BESKOW; CARLEY, 2019). Alguns desses *social bots* são utilizados para propagar conteúdos que vão desde *posts* comerciais (como no caso de *bots* de

marketing) até conteúdo adulto. Por outro lado, outros desses robôs estão usualmente envolvidos em ações de intimidação, infiltração e manipulação de redes, propaganda política e cerceamento de vozes dissidentes às suas próprias agendas (BESKOW; e CARLEY, 2019).

Outro exemplo expressivo da presença de *social bots* está dentro da rede social Facebook, onde a estimativa é de que mais de 83 milhões das contas existentes são contas falsas (CELLANJONES, 2016, apud LEITE, 2018). Dado os exemplos, e considerando a conta de um robô uma conta falsa, é possível inferir que parte dessas contas são utilizadas por esse mesmo tipo de programa.

Entretanto, para além das interações sociais mais usuais, é importante ter em mente que este mesmo ambiente digital recheado de atores "falsos" tem também sido notadamente utilizado para organização política. No Brasil, movimento nesta linha pôde ser acompanhado durante as manifestações de 2013, momento no qual as redes sociais foram usadas para convocar e expressar posicionamentos políticos e suporte para organização de atos, embora não tenham possibilitado o aprofundamento sobre as pautas levantadas (SCHERER-WARREN, 2014). Ainda assim, as movimentações sociais-políticas nas redes têm setornado cada vez mais evidentes, especialmente em períodos de eleições.

Neste cenário de alto e crescente trânsito de dados, por vezes de relevância nacional, observa-se o surgimento de ações sistemáticas visando direcionar e manipular opiniões e padrões de consumo de informação em massa com objetivos obscuros e que se apresentam como um risco iminente à estabilidade econômica, social e democrática. É necessário, portanto, tratar esta problemática como uma questão não somente de segurança da informação, como também de segurança nacional. Neste artigo será explorado a extensão da atuação de mecanismos cibernéticos, nominalmente social bots, em eleições norte americanas e brasileiras. Serão envolvidos as limitações e vulnerabilidades que as redes sociais e seus usuários possuem sob a ótica da cibersegurança social.

2. Referencial Teórico

Para aprofundar na temática, sobretudo como foram desempenhadas as ações de robôs nas redes sociais em períodos eleitorais recentes ao redor do mundo, é necessário

estabelecer dois conceitos marcantes que circulam esse universo: cibersegurança sob a ótica das interações sociais online e as ações de um *social bot*.

2.1. Guerra de Narrativa e Cibersegurança Social

As redes sociais são utilizadas por diversos atores diferentes, cada um deles desempenhando níveis também distintos de atividades. O controle e a manipulação de um conjunto de atores criam coletivamente um impacto nas redes, ainda que para mensurar o quão profundo esse impacto seja, se faça necessário considerar fatores como forma de organização desse grupo, seu tamanho, recursos dispostos e motivações (CHEN et al., 2022). É inegável, entretanto, que a tecnologia atualmente possibilita que atores no Estado e fora dele consigam rapidamente manipular ao nível global crenças e ideais, mudando inclusive rumos em campos de batalha (BESKOW e CARLEY, 2019). Segundo Beskow e Carley (2019), este é um conceito que foi recentemente observado através da lente da chamada "Guerra híbrida", mas ao observarem a colocação do coordenador da agência estatal russa para notícias internacionais, Dmitry Kiselev, apresentam a compreensão de que este tipo de guerra, ou seja, a guerra da informação/narrativa, é hoje o principal tipo de guerra.

O conceito, entretanto, ganha contornos de complexidade ainda mais significativos uma vez que, ao utilizar do ambiente civil (as redes sociais), pessoas comuns passam a ser vistas como agentes de transformação. A partir de então, passa-se a pensar sobre uma nova abordagem de cibersegurança, a Cibersegurança Social, ou *Social Cybersecurity*. De acordo com Beskow e Carley (2019), a Cibersegurança Social é um subdomínio emergente da segurança nacional que busca caracterizar, compreender e prever mudanças comportamentais, seja ao nível cultural, político ou de resultados sociais, advindas do intermédio de ferramentas tecnológicas. Além disso, visa construir uma infraestrutura cibernética que consiga manter o que os autores entendem como 'caráter essencial' diante de ciber-ameaças.

Beskow e Carley (2019) ainda complementam que os alvos de hackers usuais são os sistemas de informação, mas que a Cibersegurança Social envolve ações de humanos por meio de tecnologia tentando "hackear" outros humanos. Nesse sentido, aqui os alvos são humanos e as sociedades que nos unem. O meio cibernético, para Beskow e Carley (2019) é usado para a máxima entrega e impulsiona avanços em *marketing* direcionado, exploração

de lacunas políticas deixadas por instituições governamentais, psicologia e manipulação, unida a compreensão e uso de conceitos de ciência sociais para operações estratégicas.

As redes sociais são espaços amplos para a consolidação de tais técnicas, uma vez que a guerra de narrativa é uma superação do espaço físico para o avanço ao espaço psicológico e cognitivo, alimentando o imaginário coletivo. O uso de técnicas de manipulação é feito por vezes como um suplemento à guerra psicológica ao espalhar tensão e informação falsa a respeito de adversários (CHEN et al., 2022).

2.2. Social Bots

Como estabelecido anteriormente, a disputa da opinião pública enquanto questão de segurança nacional ganha novos contornos no ambiente online, sobretudo nas redes sociais, meio de comunicação crítico para reconhecimento de eventos e emergências. (CASSA et al. 2013). De acordo com análises de postagens na rede social *Twitter* realizadas após o atentado na maratona de Boston, no ano de 2013, a mídia foi importante para o reconhecimento e caracterização da emergência. Por outro lado, acusações falsas foram propagadas por ações de *bots*, que compartilharam postagens sem prévia verificação de fatos ou mesmo a credibilidade dos autores originais (CASSA et al. 2013). Segundo Chen et al. (2022), o desenvolvimento de tecnologias para esse tipo de ação obscura caminha na direção do que chamam de intervenção cognitiva e controle de audiências. Para os autores, os social bots encontram-se hoje como a ‘principal arma no arsenal’.

Um *social bot* considerado malicioso é aquele que tem como objetivos a exploração e manipulação de discursos nas redes, podendo influenciar na instabilidade de diversos setores da sociedade. Exemplo significativo é abordado por Ferrara et al. (2014, apud LEITE, 2018) ao explorarem um caso no qual uma campanha utilizando *social bots* resultou no aumento ‘inorgânico’ de 200 vezes do valor de mercado da empresa de tecnologia Cynk.No evento, os robôs conseguiram orquestrar uma discussão sobre a empresa a ponto de serem ‘notados’ por sistemas automatizados de *trading*, que iniciaram uma compra em massa de ações da companhia (FERRARA et al., 2016). Tais sistemas automatizados de compra e venda de ações exploram justamente as informações provenientes de redes sociaispara suas atividades. Entretanto, sem mecanismos robustos de checagem de fatos, asoperações foram suspensas somente quando analistas de mercado perceberam o ocorrido, mas não antes de gerar perdas significativas (FERRARA et al., 2016).

Ao tratar de *social bots* é necessário ter em conta que esta é uma ferramenta cibernética que explora o comportamento humano. Para além do problema de verificação de informação, um obstáculo este anterior aos próprios bots, esta nova configuração de interação humano versus máquina evidencia uma tendência conhecida: independentemente de sua veracidade ou rigor, um conteúdo muito popular e endossado tem um poder de influência excessivamente poderoso (FERRARA et al., 2016). Esse aspecto pode ser facilmente explorado por social bots estruturados em redes, em uma espécie de *botnet* de robôs sociais. Ainda que o termo *botnet* seja comumente usado na Segurança da Informação como uma rede de computadores comprometidos, a noção de *social botnets* caracteriza-se como um conjunto de identidades ou perfis online que mimetizam comportamentos humanos e socializam com eles (YADAV, 2022).

De acordo com Yadav (2022), um estudo sobre engajamento em comunidades online relacionadas a momentos de crise descobriu que aproximadamente 10% das contas nessas conversas eram de robôs sociais. Alguns dos grupos nas comunidades, inclusive, eram constituídos inteiramente por *bots* (NIED et al., 2017 apud YADAV, 2022). Isso é especialmente relevante porque do ponto de vista de campanhas políticas, por exemplo, há como descrever dois fatores estratégicos que se utilizam desses "bolsões de robôs": vantagem do pioneirismo e quantidade como qualidade (BONDY, 2017 apud YADAV, 2022). A vantagem daquele que inicia utilizando redes de social bots de maneira maliciosa para espalhar desinformação é que ele consegue criar um meio informacional favorável para sua narrativa, já que desmentir um boato é mais difícil que apenas criá-lo. Além disso, as ações de uma *social botnet* ganham força a partir da sua escala, espalhando informações falsas como se fossem verdadeiras, mas ganhando credibilidade a partir da ilusão da 'maioria' (BONDY, 2017 apud YADAV, 2022).

3. Materiais e Métodos (ou Metodologia)

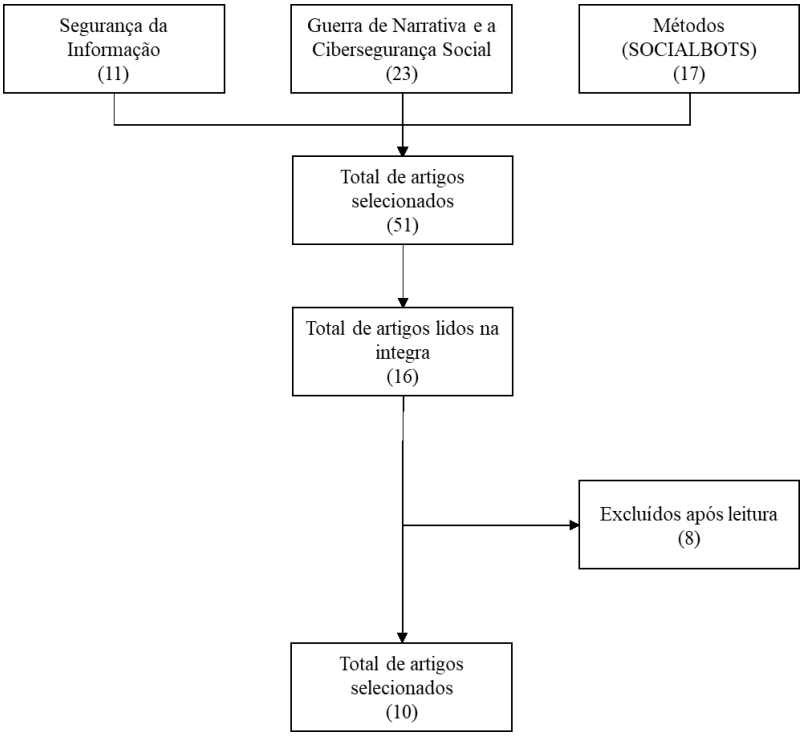
Este artigo foi baseado na metodologia de pesquisas bibliográficas, onde promovemos a revisão da literatura acadêmica relacionada à temática abordada. Para isso, utilizamos livros, artigos acadêmicos, sites da Internet, entre outras fontes.

Esta pesquisa considerou artigos publicados entre os anos de 2010 e 2022, excluindo artigos após a análise de seus títulos e resumos, e, após a leitura na íntegra, foram excluídos artigos que não atingiram a expectativa inicial da temática proposta. Foram revisados 51

artigos, e destes selecionados 12 que foram base para a linha de argumentação. Foram escolhidos dois estudos de casos principais referentes às eleições presidenciais dos Estados Unidos em 2016 e às eleições presidenciais do Brasil em 2018.

As pesquisas foram inicialmente realizadas a partir do Google Acadêmico. Ao longo do aprofundamento temático, foram utilizadas mais as seguintes bases acadêmicas: Scielo; Association for Computer Machinery; Cornell University arXiv; Lumina (Universidade Federal do Rio de Janeiro); Laboratório de Pesquisa Cibernética do Instituto Militar de Engenharia; Journal of Information Security and Applications.

Figura 1 - Fluxograma (PRISMA) do processo de seleção dos artigos pesquisados.



Fonte: Próprios Autores

4. Resultados e Discussões

As redes sociais ganharam grande importância na comunicação política ao longo da década de 2010. Seja como espaço de debate entre eleitores ou como plataforma decampanha política, as redes com mecanismos de compartilhamento, como o *Twitter* e o *Facebook*, são redutos que difundem rapidamente qualquer informação levantada. Justamente por essas características que fazem parte de sua natureza, as redes sociais são terrenos férteis para espalhar mensagens arquitetadas para manipular a opinião pública. Os

social bots são ferramentas eficientes para garantir a massificação dessas ações e tem sido evidenciado em casos de eleições, apresentando uma dissonância no processo democrático e consequentemente um risco para a segurança nacional.

Em um estudo conduzido em 2016, analisando artigos e notícias em inglês, foi apontado que governos e outros atores utilizavam robôs sociais durante o período de eleições, discussões públicas e crises com o intuito de garantir o que consideravam uma 'segurança online preventiva'. Uma estratégia definida para os *bots* era a divulgação pró-governo ou candidato específico da localidade para cumprir o objetivo de influenciar a opinião pública a seu favor (WOOLLEY, 2016 apud BRACHTEN et al., 2017). Esta não é uma ação isolada, entretanto. Nas eleições presidenciais dos Estados Unidos no ano de 2012, segundo Woolley (2016, apud BRACHTEN et al., 2017) a candidatura de Mitt Romney adquiriu aproximadamente 117.000 seguidores gerais em cerca de 24 horas, por atividades presumidamente ligadas à social bots.

Brachten et al. (2017) abordam essas ações de *social bots* no *Twitter* sob a lente do que chamam de *astroturfing*, que seria a prática de tuitar ou retuitar uma opinião política de modo a implicar um consenso sobre a opinião em questão. Um bom indicador do uso dessa ação é a presença de muitos tweets automáticos sobre um assunto ou *hashtag*.

De modo geral, o uso de *social bots* no contexto político é usado para aumentar o número de seguidores, influenciar a opinião pública ou mesmo romper comunicação (WOOLLEY, 2016 apud BRACHTEN et al., 2017), consumindo o espaço de discussão com conteúdo similar, mas não relacionado ou desviando a atenção dos usuários legítimos para outros temas (ABOKHODAIR et al., 2015 apud BRACHTEN et al., 2017).

Além dos processos citados, as eleições presidenciais dos Estados Unidos no ano de 2016 foram marcadas pelo uso de robôs e disputa de narrativa. Bessi e Ferrara (2016) se propuseram a entender o ocorrido em seu artigo "*Social bots distort the 2016 U.S. Presidential election online discussion*", no qual utilizaram como método de pesquisa a coleta de *tweets* postados durante o período entre 16 de setembro e 21 de outubro de 2016, relacionados às eleições presidenciais. Com o uso da API de pesquisa do *Twitter*, uma lista foi compilada de modo a monitorar o mesmo número de palavras-chave e hashtags relacionadas aos dois principais candidatos no período, Hillary Clinton (quatro termos exclusivos) e Donald Trump (cinco termos exclusivos), além de outras relacionados aos

debates ocorridos no período. Com o estudo, Bessi e Ferrara (2016) coletaram por volta de 20 milhões e 700 mil *tweets* postados por mais de 2 milhões e 700 mil usuários. As duas principais hashtags foram #trump (3.290.636 tweets) e #hillary (1.516.318 tweets).

Para determinar se as ações eram realizadas por *bots*, os autores utilizaram uma solução chamada *BotOrNot*. A ferramenta consiste, de acordo com Bessi e Ferrara (2016), em uma estrutura baseada em machine learning que extrai e analisa um conjunto complexo de recursos que vão desde conteúdo e estrutura de rede, atividades temporais, dados provenientes de perfis de usuários e até a análise de sentimento externalizado nos conteúdos. Com esses dados processados, é produzida uma pontuação que infere a probabilidade de a conta ser ou não um *social bot*.

De acordo com os autores, a ferramenta também apresentou indicadores que sinalizam maior probabilidade de ser um robô, sendo os seguintes:

1) baixo nível de customização do perfil do *Twitter;*
2) falta de metadados geográficos e *digital footprints*;
3) maior atividade relacionada ao compartilhamento de conteúdo de terceiros do que a criação de *tweets* originais;
4) número de seguidores, uma vez que bots tendem a seguir mais contas do que serem seguidos;
5) data de criação da conta muito recente;
6) aleatoriedade do nome de usuário;

Ranqueando as contas por volume de atividade, os autores chegaram a 50.000 contas na rede social, sendo essas responsáveis por produzir mais de 12 milhões de tuítes relacionados às palavras-chave e hashtags. Ou seja, cerca de 60% de todo o conteúdo discutido. Deste total, 7.183 foram definidos como robôs, sendo deles 2.330.252 tuítes. O restante das contas foi dividido entre não conclusivo (~2.000 contas) e de humanos (40.163). Ao extrapolar esse dado estatístico para a população total de usuários discutindo as eleições dos Estados Unidos, Bessi e Ferrara (2016) estimaram a existência de pelo menos 400 mil social bots envolvidos, responsável por aproximadamente 3,8 milhões de tuítes.

Bessi e Ferrara (2016) também identificaram o posicionamento dos bots acerca dos seus candidatos. Ficou evidente através da análise realizada pelo algoritmo *SentiStrength*

que tanto os robôs quanto os humanos favoráveis ao então candidato Trump falavam muito positivamente de seu candidato. Bressi e Ferrara (2016) discorrem que uma fração relevante dos tuítes não-negativos gerados por bots nas hashtags monitoradas no período, o que correspondia por volta de 200.000 tuítes, apoiavam Donald Trump.

O fato de haver a presença de bots atuando sistematicamente em produzir e compartilhar conteúdo positivo de um candidato pode enviesar a percepção dos indivíduos expostos a ele. Isso é especialmente perigoso se neste contexto foi sugerido que exista um apoio orgânico crescente para um dos candidatos, ainda que tenha sido gerado artificialmente (BESSI e FERRARA, 2016). Outro ponto que Bessi e Ferrara (2016) evidenciam é sobre como os grupos pró Clinton estabeleciam suas discussões sobre a sua própria candidata, enquanto o grupo pró Trump, fossem humanos ou bots, dedicavam um número significativo de seus tweets para seu oponente. Bressi e Ferrari (2016) afirmam ainda que "[…], na verdade, a maioria dos tweets negativos gerados por ambos humanos e robôs foram endereçados à Hillary Clinton.", enquanto os apoiadores da candidata democrata direcionaram a maioria de seus tweets negativos à própria candidata.

Já os estudos de SANTINI, R. M. et al. (2021) teve como foco o processo eleitoral brasileiro de 2018, onde o então candidato à presidência Jair Bolsonaro teve como principal estratégia eleitoral o uso das redes sociais. Segundo SANTINI, R. M. et al. (2021), a estratégia eleitoral deu-se início no ano de 2016, ainda no processo eleitoral do âmbito municipal, quando foram estabelecidos padrões comportamentais nas redes sociais no município do Rio de Janeiro. SANTINI, R. M. et al. (2021) sugere que a automação de diferentes perfis e a disseminação experimental de narrativas divisivas garantiram a eficácia de sua persuasão na comunicação. Os resultados da pesquisa e análises indicam que o candidato e seus colegiados, com as ações tomadas durante o processo eleitoral de 2016, puderam avançar suas iniciativas e preparar o discurso mais bem aceito por seu público-alvo para as eleições que se dariam em 2018.

SANTINI, R. M. et al. (2021) apontou a construção gradual de um chamado "Exército digital" para apoiar o candidato, composto por trolls e bots. Para tanto, foram traçados perfis que apresentaram potencial apoio em seu discurso. Visando apoio maciço da comunidade evangélica, com o compromisso da agenda moral contra o aborto e Direitos LGBT+. A partir disso, foi observado que o uso de bots sociais com identidades evangélicas

na campanha de 2016 foi um método importante e obteve resultado para condução da discussão da temática e conseguiu ampla adesão por este grupo de pessoas.

Ainda segundo SANTINI, R. M. et al. (2021), outro fator de exploração das redes sociais foi o descontentamento da população com os partidos políticos, o que gerou descrédito e projetou adesão nos discursos nacionalistas, religiosos e étnicos, sendo o elo entre diferentes grupos conservadores brasileiros. Aqui apontou-se um importante fator, o papel das "paixões" e do comportamento emocional na política, revelando-se como grande frente de adesão e compartilhamento, com ampla difusão de pensamentos e aceitabilidade, gerando com isso conflitos partidários e a tomada de decisões.

SANTINI, R. M. et al. (2021) reconhece certa limitação em sua metodologia, sendo essa baseada em rastreamento digital, dados, e análise qualitativa, onde se sugere a hipótese sobre o uso de bots sociais para modelar a campanha presidencial de 2018 e propõe o uso de diferentes conjuntos de dados e métodos. No entanto, os resultados não devem ser considerados isoladamente, mas como uma evidência entre muitos outros relatórios investigativos (sendo citados Campos Mello, 2018; Hunter & Power, 2019; Isaac & Roose, 2018; Phillips, 2018) sobre os controversos esforços online de Bolsonaro para vencer a eleição presidencial brasileira.

Por fim, SANTINI, R. M. et al. (2021) refuta a culpabilidade das plataformas de mídia social e as ferramentas computacionais nos resultados da eleição de 2018 do Brasil. Porém, destaca haver muitas variáveis que contribuem para este resultado, tais como dinâmicas econômicas, ideológicas, morais, religiosas e institucionais que refletem e são refletidas no ecossistema midiático. Ao mesmo tempo, reforça que é inegável que a tecnologia pode aumentar a vantagem de qualquer campanha reduzindo custos, riscos e imprevisibilidade, que pode alavancar a ciência comportamental para manipular as crenças dos usuários e suas atitudes. Com o uso de técnicas de big data, modelagem de dados, manipulação de algoritmos etc., são inovações poderosas, independentemente de quem as use e para quais propósitos.

5. Considerações Finais

Este artigo teve por objetivo demonstrar, por meio de um estudo de caso, a intervenção de agentes tecnológicos em processos eleitorais. Duas campanhas eleitorais presidenciais foram destacadas ao longo do artigo: Estados Unidos (2016) e Brasil (2018). Em ambas se notou o uso marcante de redes sociais evidenciado pela presença massiva de social bots, um tipo de robô que explora o comportamento humano ao mimetizá-lo. No caso das eleições nos Estados Unidos, foi estimado que cerca de 400 mil social bots participaram das discussões na rede social *Twitter*, responsáveis por mais de 3 milhões de tweets. Nas eleições brasileiras, porém, realizou-se uma análise qualitativa que contribuiu com a discussão ao apontar o envolvimento emocional do eleitor nos debates em redes sociais. Esse foi um dos principais aspectos explorados pelos perfis automatizados na eleição nacional.

A utilização de social bots nem sempre é maliciosa, mas nos casos destacados no decorrer do artigo fica evidente o caráter manipulatório e dissociativo. A presença massiva de robôs abusa dos algoritmos das próprias redes sociais, atuando no direcionamento de conteúdo e criando artificialmente uma "bolha informacional" que enviesa a percepção dos usuários presos dentro dela. Ocorre portando uma tendência de radicalização, uma vez que esses mecanismos de manipulação buscam atingir o emocional do seu alvo por meio de crenças e paixões. Quando seu objetivo é alcançado na adesão do discurso, é iniciado um processo de invalidação de discursos contrários ou fontes que possam apresentar contrapontos a sua própria base de argumentação, conduzindo seu público a consumir somente das fontes que propagam os ideais inicialmente difundidos.

Esse método de ação, por meio da manipulação das informações, vem colocando em risco a manutenção da visão de sociedades livres e conduzindo a resultados políticos que podem ser inclusive consequências de operações estratégica de nações rivais, se analisado sob a perspectiva da Guerra Híbrida e Cibersegurança Social. A possível interferência de nações rivais nos processos democráticos de outras nações pode gerar impactos significativos nas políticas internas de um país rival, interferir na economia dessa nação e até mesmo em questões ideológicas e culturais.

É preciso que se reconheça esta instabilidade mundial e que medidas de contenção e prevenção ocorram em todas as esferas da sociedade, passando por identificação e

responsabilização das ações conduzidas na rede. Os esforços das principais redes sociais, como Twitter, Facebook e Instagram em mediar seus espaços informacionais contra discursos extremistas têm se tornado muito relevantes, mas pouco se relacionam ao combate às ações coordenadas e estratégicas, como é o caso dos *social bots*. Ainda que debates acerca da regulamentação dessas mídias tenham sido levantados, inclusive por parte do poder público brasileiro, questões como os limites da liberdade de expressão compõem as complexas dinâmicas envolvidas. Porém, há de modo geral a urgência em se promover ações no sentido de educar usuários da Internet, apresentando amplamente suas contribuições e seus riscos e empoderando cada indivíduo para que tomem decisões conscientes online.

Para futuros desdobramentos das temáticas abordadas neste artigo, cabe ainda o aprofundamento sobre os agentes envolvidos na orquestração de ações com uso de *social bots*, uma vez que apesar de suas presenças e interesses ainda não serem bem delimitados, as consequências conforme apontadas podem ser preocupantes.

Referências

ABOKHODAIR, Norah; YOO, Daisy; MCDONALD, David W. Dissecting a Social Botnet: Growth, Content and Influence in Twitter. **CSCW '15: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing**; 2015, Vancouver, BC, Canada. Disponível em <https://dl.acm.org/doi/pdf/10.1145/2675133.2675208>. Acesso em: 20 de set. de 2022.

BESKOW, David M; CARLEY, Kathleen M. Social Cybersecurity: An Emerging National Security Requirement. **Military Review: The professional Journal of The U.S. Army**; April 2019. Disponível em <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/#> Acesso em: 25de set. de 2022.

BESSI, Alessandro; FERRARA, Emilio, Social Bots Distort the 2016 US Presidential Election Online Discussion (November 7, 2016). **First Monday, Volume 21, Number 11 •- 7 November 2016** Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2982233 > Acesso em: 04 de nov. 2022.

BRACHTEN et al. Social Bots in a 2017 German state election. **Australasian Conference on Information Systems**; 2017, Hobart, Australia. Disponível em: <https://arxiv.org/ftp/arxiv/papers/1710/1710.07562.pdf>. Acesso em: 04 de nov. 2022.

CASSA, C.A.; CHUNARA, R.; MANDL, K; and BROWNSTEIN, J.S. Twitter as a sentinel in emergency situations: Lessons from the Boston marathon explosions. **PLoS Currents: Disasters (July 2013)**. Disponível em <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3706072/>. Acesso em: 16 de out. 2022.

CHEN, Long; CHEN, Jianguo; XIA, Chunhe; Social network behavior and public opinion manipulation. **Journal of Information Security and Applications 64 (2022) 103060**. Disponível em <https://www.sciencedirect.com/science/article/abs/pii/S2214212621002441?via%3Dihub>. Acesso em: 23 de set. 2022.

FERRARA, Emilio; VAROL, Onur; DAVIS, Clayton; MENCZER; Filippo; FLAMMINI, Alessandro. The Rise of Social Bots. **Communications of the ACM, July 2016, Vol. 59 No. 7**, Pages 96-104. Disponível em <https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext?mobile=false>. Acesso em: 01 de out. de 2022.

KIMURAI, H.; BASSO, L. F. C. ; MARTIN, D. M. L. Redes sociais e o marketing de inovações. **RAM. Revista de Administração Mackenzie, v. 9, p. 157 – 181, 2008**. Disponível em <https://www.scielo.br/j/ram/a/7m7tJbtYFtk8cyFGxZ7ct9c/?lang=pt> Acesso em: 20 de set. de 2022.

LEITE, Vanessa Quadros Godim. **Geração de *Dataset* a partir da criação de uma *Social Botnet***. Tese (Mestrado). Instituto Militar de Engenharia, Rio de Janeiro, 2018. Disponível em <http://www.defesacibernetica.ime.eb.br/pub/repositorio/2018_Vanessa_Leite.pdf>. Acesso em: 01 de out. 2022.

SCHERER-WARREN, Ilse. Manifestações de rua no Brasil 2013: encontros e desencontros na política. **Caderno CRH [online]. 2014, v. 27, n. 71, pp. 417-429**. Disponível em <https://doi.org/10.1590/S0103-49792014000200012>. Acesso em: 16 de out. 2022.

SANTINI, R. M.; SALLES, D.; TUCCI, G.; ESTRELLA, C. A militância forjada dos bots: A campanha municipal de 2016 como laboratório eleitoral. **Lumina, [S. l.], v. 15, n. 1, p. 124–142, 2021. DOI: 10.34019/1981-4070.2021.v15.29086**. Disponível em <https://periodicos.ufjf.br/index.php/lumina/article/view/29086>. Acesso em: 18 out. 2022.

YADAV, Shashank. Propagation of Social Botnets: Policy Consequences. **ArXiv abs/2205.04830 (2022)**. Disponível em <https://arxiv.org/abs/2205.04830>. Acesso em 01 de out. 2022.