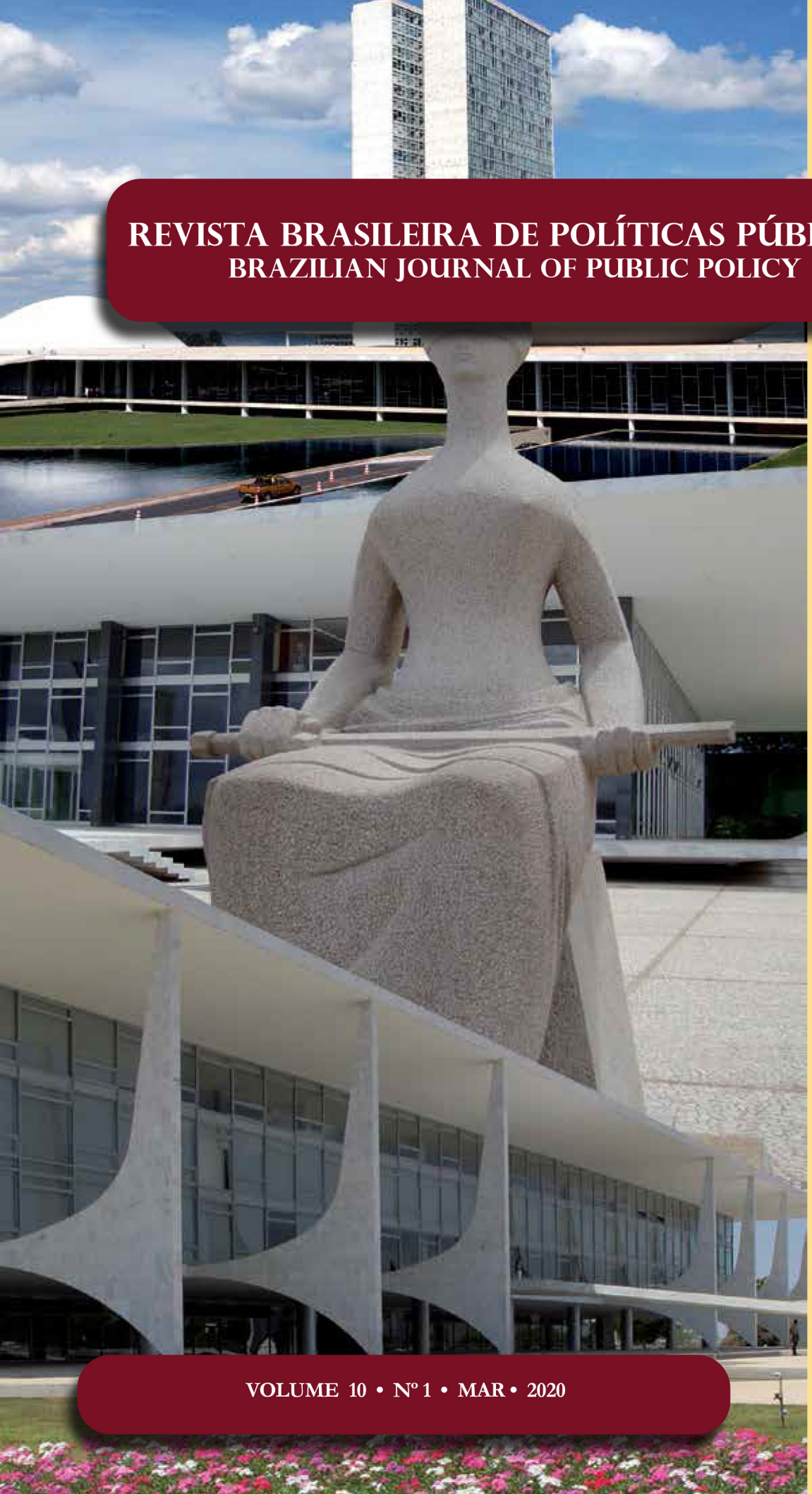

UniCEUB
ISSN 2236-1677

REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS
BRAZILIAN JOURNAL OF PUBLIC POLICY

O uso de *bots* sociais como ameaça à democracia

The usage of social *bots* as a threat to democracy

Mateus de Oliveira Fornasier

VOLUME 10 • Nº 1 • MAR • 2020

Sumário

doi: 10.5102/rbpp.v10i1.6453

O uso de *bots* sociais como ameaça à democracia*

The usage of social *bots* as a threat to democracy

Mateus de Oliveira Fornasier**

Resumo

Este trabalho objetiva conhecer os bots sociais, suas relações com a democracia e características que contribuam para regulação mais condizente com a sua complexidade. Objetivos específicos: i) estabelecer uma tipologia dos bots; ii) apresentar questões específicas acerca da importância do uso dessa tecnologia para a formação da opinião pública; iii) discutir possibilidades de regulação coerentes com a complexidade tecnológica dos bots sociais. Metodologia: método de procedimento hipotético-dedutivo, com abordagem qualitativa e técnica de pesquisa bibliográfico-documental. Resultados: i) os bots exigem abordagem complexa, pois constituem uma categoria múltipla, havendo bots benignos e malignos; ii) além de terem influência deletéria para constituição da opinião pública, os bots são de difícil detecção, pois se valem de avanços tecnológicos bastante significativos, principalmente porque, conforme as ferramentas de detecção de bots evoluem, também evoluem as técnicas de ocultação de tais aparatos; iii) tanto em nível racional quanto emocional, o uso de bots sociais causadores de redundância de informações podem distorcer eleições; iv) é primordial que o problema não seja abordado unicamente com base em desenvolvimento tecnológico, pois, além do descrito descompasso técnico, há a exploração, por parte de políticos mal-intencionados, de características da psiquê e da socialização humanas. Ao serem desenvolvidas estratégias políticas e jurídicas para tal problema, portanto, a transdiciplinaridade entre conhecimentos técnicos e psicossociais (principalmente) deve ser levada em consideração.

Palavras-chave: Bots. Democracia. Opinião pública. Eleições. Regulação.

Abstract

This work aims to know the technology of social bots, its relations with democracy and its characteristics that contribute to a regulation more consistent with its complexity. Specific objectives: i) to establish a typology of bots; ii) to present specific questions about the importance of using this technology for the formation of public opinion; iii) to discuss possibilities for regulation consistent with the technological complexity of social bots. Results: i) Understanding bots requires a complex approach, as they are a multiple category, with benign and harmful bots; ii) in addition to having a deleterious influence on the constitution of public opinion, bots are dif-

* Recebido em 27/01/2020
Aprovado em 14/02/2020

** Professor do Programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI). Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS), com Pós-Doutorado em Direito e Teoria (*Law and Theory)* pela University of Westminster (Reino Unido). E-mail para contato: mateus.fornasier@unijui.edu.br

ficult to detect, as they use very significant technological challenges, mainly because, as the bot detection tools evolve, so do the techniques for hiding such apparatus; iii) both at the rational and at the emotional level the use of social bots that cause redundancy of information can distort elections; iv) it is essential that the problem should be approached not only based on technological development, because, in addition to the described technical gap, there is the exploitation, by malicious politicians, of human psyche and socialization characteristics. When political and legal strategies are developed for such a problem, therefore, the transdisciplinarity between technical and psychosocial knowledge (mainly) must be taken into account. Methodology: hypothetical-deductive procedure method, with qualitative approach and bibliographic and documentary research technique.

Keywords: Bots. Democracy. Public Opinion. Elections. Regulation.

1 Introdução

O relatório *The Global Disinformation Order*, da autoria de Samantha Bradshaw e Philip Howard,[1] ambos pesquisadores da Universidade de Oxford, de 2019, destacou as maneiras pelas quais partidos políticos e agências governamentais usaram as mídias sociais para espalhar propaganda política, poluir o ecossistema de informações digitais e suprimir a liberdade de expressão e a liberdade de imprensa.

No referido estudo, sistematizaram as capacidades de tropas cibernéticas em mínima, baixa, média e alta. A título de resumo, a capacidade média de tropas cibernéticas envolve equipes que têm uma forma e estratégia consistentes, bem como funcionários de tempo integral empregados o ano todo para controlar o espaço de informações. Tais equipes, geralmente, são coordenadas com vários tipos de atores e experimentam ampla variedade de ferramentas e estratégias para manipulação de mídias sociais. Algumas realizam, inclusive, operações de influência no exterior. As equipes de capacidade média incluem: Azerbaijão, Bahrein, Bósnia e Herzegovina, Brasil, Camboja, Cuba, Etiópia, Geórgia, Guatemala, Índia, Cazaquistão, Quirguistão, Malásia, Malta, México, Paquistão, Filipinas, Catar, Sri Lanka, Sudão, Tajiquistão, Tailândia, Turquia, Ucrânia, Reino Unido e Uzbequistão.

A alta capacidade de tropas cibernéticas envolve grande número de funcionários e grandes gastos orçamentários em operações psicológicas ou guerra de informação. Pode, também, haver fundos significativos gastos em pesquisa e desenvolvimento, além de evidências de uma infinidade de técnicas sendo usadas. Essas equipes não operam, apenas, durante as eleições, mas envolvem funcionários em tempo integral dedicados a moldar o espaço de informações. Tais equipes se concentram nas operações estrangeiras e domésticas, e incluem: China, Egito, Irã, Israel, Mianmar, Rússia, Arábia Saudita, Síria, Emirados Árabes Unidos, Venezuela, Vietnã e Estados Unidos.

Tal estudo revelou, dentre outras informações, que, em relação aos 70 (setenta) países estudados (ao redor de todo o globo), 87% destes usam contas humanas e 80% usam contas de *bot*; ademais, 71% espalham propaganda pró-governo ou pró-partido, 89% usam propaganda computacional para atacar oposição política, e 34% espalham mensagens polarizadoras projetadas para impulsionar divisões na sociedade.

Estudar o tema da influência dos *bots* nas comunicações sociais é de extrema importância para a sociedade e para a manutenção dos regimes democráticos no mundo. Esse tipo de comunicação tem sido cada vez mais presente em campanhas eleitorais, marcando transformação paradigmática na comunicação social. Assim, tem grande potencial para a formação de opiniões na esfera pública. No que tange à importância

[1] BRADSHAW, Samantha; HOWARD, Philip N. The global disinformation order: 2019 global inventory of organised social media manipulation. *In*: WORKING PAPER, 2., 2019, Oxford. *Proceedings*...Oxford: Project on Computational Propaganda, 2019. Disponível em: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf. Acesso em: 26 dez 2019.

jurídica do tema, trata-se de tópico fundamental para entender a liberdade de expressão e seus limites a partir de novas tecnologias. Tanto legisladores quanto juízes terão de entender não apenas sua faceta deletéria à democracia, mas também, de que formas tal tecnologia pode ser utilizada em relação aos limites que não ofendam direitos e liberdades fundamentais.

A questão fundamental que moveu a elaboração desta pesquisa pode ser assim descrita: como se caracteriza a tecnologia de uso de *bots* sociais, e de que forma essa tecnologia pode ser regulada para que seu uso não "coloque em xeque" um dos principais pilares da democracia, qual seja, a formação de opinião de modo coerente? A hipótese que se apresenta para tal problema é de que a tecnologia de *bots* sociais pode ter tanto usos benignos quanto malignos no que tange à democracia e ao respeito a direitos fundamentais. Esse entendimento é basilar para que se construa uma regulação que também corresponda a tal complexidade. Assim, a regulação do uso da tecnologia dos *bots* não deve se dar apenas com base em atividade estatal — tendo de compreender a colaboração de entes privados, os quais detêm maior conhecimento de causa acerca de tal tecnologia. Contudo, a força normativa do Estado e das constituições é elemento-chave para que tal regulação ocorra com base em moldes legítimos.

O objetivo geral deste trabalho é conhecer a tecnologia dos *bots* sociais, suas relações com a democracia e características que contribuam para uma regulação mais condizente com a sua complexidade. Para a consecução de tal objetivo, estruturou-se o texto com base em partes. Na primeiro, uma tipologia acerca dos *bots* foi realizada. Já na segunda, foram apresentadas questões específicas acerca da importância do uso dessa tecnologia para a formação da opinião pública. Por fim, uma discussão acerca de possibilidades de regulação coerentes para com a complexidade tecnológica dos *bots* sociais foi traçada.

Quanto aos aspectos metodológicos, a pesquisa apresentada neste artigo tem natureza exploratória, com método de procedimento hipotético-dedutivo, abordagem qualitativa e técnica de pesquisa bibliográfico-documental.

2 Bots e democracia: noções gerais

Os *bots* sociais preenchem os sistemas tecnossociais, sendo, geralmente, benignos e/ou úteis, apesar de muitos serem criados para prejudicar, adulterando, manipulando e enganando os usuários de mídia social.[2] Eles são usados, às vezes, de maneira indevida no discurso político, para manipular o mercado de ações, roubar informações pessoais e espalhar informações erradas. A taxonomia dos diferentes sistemas de detecção de *bots* sociais propostos na literatura explica técnicas baseadas em rede, estratégias de *crowdsourcing*, aprendizado supervisionado baseado em recursos e sistemas híbridos.

Bots são, basicamente, programas de computador usados com fins de automação na internet — daí o porquê da sua denominação (abreviatura para o termo *robot*). Tratar do que são os *bots* exige uma abordagem complexa, que perpassa analisar quais são estrutura, a função e o uso do tipo de sistema automatizado de que se irá tratar.[3] Conforme tais categorias, há vários tipos — normalmente denominados conforme nomenclatura técnica proveniente da Língua Inglesa —: desde o início da internet, há *bots* que realizam a tarefa de acessar, arquivar e rastrear os milhares de sites que diariamente são adicionados à rede (os chamados *web robots,* essenciais para desenvolver os motores de busca de páginas na internet); há os bots que realizam diálogos entre computador e ser humano, que operam em linguagem natural (conhecidos como *chatbots,* tais como a Siri da Apple e a Alexa, da Amazon); outros que servem para espalhar publicidade comercial e

[2] FERRARA, Emilio; VAROL, Onur; DAVIS, Clayton; MENCZER, Filippo, FLAMMINI, Alessandro. The rise of social bots. *Communications of the ACM,* New York, v. 59, n. 7, p. 96-104, 2016. DOI: 10.1145/2818717.

[3] GORWA, Robert; GUILBEAULT, Douglas. Unpacking the social media bot: a typology to guide research and policy. *Policy and Internet*, 2018. DOI: 10.1002/poi3.184.

vírus em massa (os *spambots*); e há, por fim, contas automatizadas em redes sociais (tais como o Facebook e o Twitter), que assumem uma identidade fabricada, se infiltram em redes de usuários, produzindo conteúdo diversos e interagindo, assim, com usuários humanos (os *social bots*). Quando necessitam da intervenção humana para disseminar conteúdo, os *bots* sociais são conhecidos como *sockpuppets* ("fantoches", numa tradução livre); e os *sockpuppets*, quando possuem motivação política e/ou intervenção governamental, são frequentemente chamados de *trolls*. Quando ocorre a combinação entre *bots* e humanos, uns prestando assistência aos outros, configuram-se os ciborgues ou contas híbridas. Essa terminologia é meramente exemplificativa, dependendo do usuário (e/ou da cultura), ocorrem variações e confusões.

Bots sociais, quando projetados para prejudicar e manipular os usuários das mídias sociais, podem ser usados para roubar informações pessoais, espalhar desinformação, manipular o mercado de ações e se infiltrar no discurso político, por exemplo.[4] Quando se trata de uso político nocivo, podem inflar artificialmente o apoio de um candidato político durante as eleições — ou seja, representam uma ameaça concreta aos procedimentos democráticos. Durante as eleições presidenciais de 2016 nos EUA, *bots* sociais foram usados para apoiar candidatos e difamar adversários, difundindo milhões de postagens (*tweets*) na plataforma Twitter sites contendo notícias falsas. Os robôs podem dar a impressão de que uma informação é altamente importante, precisa, difundida e endossada por muitas pessoas, influenciando o comportamento dos usuários de mídia social.

Howard, Wooley e Calo[5] consideram que, dentre os *bots* sociais, há uma categoria específica, dos "bots políticos" — categoria que se refere a contas de usuário equipadas com os recursos ou o *software* para automatizar a interação com outras contas de usuário sobre política. Suas ilustrações são focadas em *bots* políticos no Twitter, devido à política relativamente aberta dos *sites* de automação e ao grande número de *bots* que funcionam em tal plataforma, mas situações semelhantes poderiam ocorrer, hipoteticamente, em outras plataformas sociais.

Os *bots* políticos estão entre as mais recentes ferramentas de comunicação das equipes de campanhas digitais.[6] Essa tecnologia difundida desempenha um papel cada vez mais importante para o sentimento do público, manipulação de opiniões e contenção de procedimentos legais permanentes. Particularmente em relação à democracia digital e à direção eleitoral, esses autômatos controlados por *software* são de crescente importância para os estudiosos da comunicação política, da democracia e dos processos nela contidos. Os *bots* políticos também são motivo de preocupação para os formuladores de políticas, jornalistas e interessados em um processo eleitoral justo e transparente.

Bots sociais, assim, corroboram a polarização da discussão política nas mídias sociais, alteram a percepção da influência de tal forma de comunicação, afetam a percepção humana da realidade, arruinam reputações, aumentam, artificialmente, a audiência das pessoas, com fins econômicos ou políticos.[7] Atualmente, simulam comportamentos humanos, pesquisando materiais na internet, os quais são publicados em horários predeterminados, incluindo padrões de rotinas diárias humanas.[8] Podem também manter conversas com as

[4] OBERER, Birgit; ERKOLLAR, Alptekin; STEIN, Anna. Social bots: act like a human, think like a bot. *In*: STUMPF, Marcus (ed.). *Digitalisierung und kommunikation*: konsequenzen der digitalen transformation für die wirtschaftskommunikation. Wiesbaden: Springer, 2019. p. 311-327; p. 314-315.

[5] HOWARD, Philip N.; WOOLEY, Samuel; CALO, Ryan. Algorithms, bots, and political communication in the US 2016 election: the challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics*, Oxfordshire, v. 15, n. 2, p. 81-93, 2018. DOI: 10.1080/19331681.2018.1448735, p. 85.

[6] HOWARD, Philip N.; WOOLEY, Samuel; CALO, Ryan. Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics,* Oxfordshire, v. 15, n. 2, p. 81-93, 2018. DOI: 10.1080/19331681.2018.1448735, p. 91-92.

[7] OBERER, Birgit; ERKOLLAR, Alptekin; STEIN, Anna. Social bots: act like a human, think like a bot. *In:* STUMPF, Marcus (ed.). *Digitalisierung und kommunikation*: konsequenzen der digitalen transformation für die wirtschaftskommunikation. Wiesbaden: Springer, 2019, p. 311-327; p. 316.

[8] OBERER, Birgit; ERKOLLAR, Alptekin; STEIN, Anna. Social bots: act like a human, think like a bot. *In:* STUMPF, Marcus (ed.). *Digitalisierung und kommunikation:* konsequenzen der digitalen transformation für die wirtschaftskommunikation. Wiesbaden:

pessoas, colocando comentários em suas postagens ou respondendo perguntas. Outros pesquisam pessoas influentes ou favoritas nas redes sociais, seguindo-as ou chamando sua atenção. Isso pode influenciar discussões, facilitar a aquisição de visibilidade e gerar conteúdo. A fim de não serem confundidos com agentes não humanos, esses *bots* podem pesquisar, nas redes sociais, informações adequadas a cada tópico de discussão e adaptar suas contribuições às conversas atuais. Os *bots* avançados podem produzir respostas automáticas por meio de algoritmos de linguagem natural, geralmente com informações apontando para recursos externos. Os *bots* podem roubar perfis, fotos e *links* de usuários reais e agir como esses humanos reais, espalhando conteúdo para tópicos predefinidos. Às vezes permitem a clonagem do comportamento de usuários humanos reais, interação com seus amigos reais e postagem de conteúdo em tempo hábil, que se ajusta ao comportamento real do usuário. Os *bots* avançados podem evitar os algoritmos padrão de detecção de *bots*: seguem uns aos outros nas redes sociais, tendo, portanto, uma proporção equilibrada de amigos e seguidores, seguindo um cronograma em suas publicações para simular pausas e períodos de sono de usuários de mídia social humana. Além disso, eles podem reutilizar mensagens já postadas, alterando, ligeiramente, as mensagens de modo aleatório, a fim de evitar a detecção como mensagens de *bot* por programas automáticos.

Como as mídias sociais tornaram-se um local de discussão e debate sobre temas controversos, oferecem uma oportunidade de influenciar a opinião pública. Essa possibilidade deu origem a um comportamento específico conhecido como *trolling*, encontrado em quase todas as discussões que incluem tópicos emocionalmente atraentes. O *troll* — usuário de comunicação mediada por computador que constrói a identidade de querer sinceramente fazer parte do grupo em questão, transmitindo intenções pseudo-sinceras, mas cuja intenção real é interromper e/ou desencadear/exacerbar conflitos — é uma ferramenta útil para qualquer organização disposta a forçar uma discussão fora dos trilhos quando não há fatos adequados para apoiar os argumentos.[9]

Comentários ofensivos e ataques pessoais podem inibir a participação de cidadãos em espaços de discussão — razão pela qual é necessária uma moderação automatizada de conteúdo, que visa superar esse problema usando classificadores de aprendizado de máquina treinados em grandes corpos de textos classificados como ofensivos. Apesar de tais sistemas serem capazes de incentivar mais debates civilizados e racionais, eles devem navegar por fronteiras normativamente contestáveis, estando sujeitos a normas idiossincráticas dos avaliadores humanos que fornecem os dados de treinamento.[10] Um objetivo importante das plataformas que implementam essas medidas pode ser garantir que elas não sejam indevidamente tendenciosas em relação ou contra normas particulares de ofensa. Em outras palavras: *bots* podem ser usados para ajudar a construir ambientes mais éticos e racionais; porém, até o momento, é necessário que agentes humanos os treinem para identificar conteúdo malicioso — e tal treinamento de identificador pode ficar sujeito às tendências dos programadores. Ou seja: se programadores tiverem preconceitos (de sexo, de raça, religiosos, de posicionamento político etc.), poderão inseri-los nos *bots* programados como moderadores de conteúdo.

Os cenários em que a aplicação de *bots* sociais é comprovadamente prejudicial são significativamente centrais em relação à vida *on-line* e, portanto, significativos para a formação da opinião pública. Vários pesquisadores propõem soluções para detectar o comportamento humano dessas entidades autônomas. O trabalho de Zago et al.[11] identifica vários desafios do social *bots*, com o objetivo de auxiliar pesquisadores na construção de metodologias sólidas contra essa ameaça em evolução. No que tange a procedimentos

Springer, 2019. p. 311-327; p. 317.

9 PAAVOLA, Jarkko; HELO, Tuomo; JALONEN, Harri; SARTONEN, Miika; HUHTINEN, Aki-Mauri. Understanding the trolling phenomenon: the automated detection of bots and cyborgs in the social media. *Journal of Information Warfare*, Yorktown, v. 15, n. 4, p. 100-111, 2016. p. 100; p. 104.

10 BINNS, Reuben Binns; VEALE, Michael; VAN KLEEK, Max; SHADBOLT, Nigel Shadbolt. Like trainer, like bot? Inheritance of bias in algorithmic content moderation. *In*: INTERNATIONAL CONFERENCE SOCINFO, 9., 2017, Oxford. *Proceedings*… Oxford: Springer, 2017. p. 405-415. Part II. DOI: 10.1007/978-3-319-67256-4_32.

11 ZAGO, Mattia; NESPOLI, Pantaleone; PAPAMARTZIVANOS, Dimitrios; PÉREZ, Manuel Gil; MÁRMOL, Félix Gómez; KAMBOURAKIS, Georgios; PÉREZ, Gregorio Martínez. Screening Out Social Bots Interference: Are There Any Silver Bullets? *IEEE Communications Magazine*, New York, v. 57, n. 8, p. 98-104, Aug. 2019. DOI: 10.1109/MCOM.2019.1800520. p. 99.

democráticos, as principais ameaças realizadas por estratégias que usam *bots* sociais maliciosos relacionam-se à manipulação da opinião pública, mediante o abuso de ferramentas de automação *online* para gerar uma grande quantidade de postagens de mídias sociais para apoiar ou atacar de maneira oposta pessoas, marcas e ideologias específicas.

O uso de *bots* sociais em tempos de eleição totalmente influenciada pela internet remete à noção de guerra neocortical, a qual molda ou controla o comportamento inimigo sem destruí-lo, até o ponto de regular a percepção, a consciência e a vontade da liderança do adversário (ou seja, o seu sistema neocortical).[12] Em outros termos, trata-se de penetrar na observação, na orientação, na decisão e na ação dos adversários, apresentando aos líderes do adversário (seu cérebro coletivo) percepções, dados sensoriais e cognitivos projetados para resultar em uma faixa ora estreita e controlada, ora grande e desorientadora (a depender das necessidades de quem a controla) de cálculos e avaliações. Essas avaliações e cálculos produzem escolhas adversas que correspondem às escolhas e resultados desejados, influenciando os líderes adversários a não lutarem, principalmente. Para Andrew Korybko,[13] trata-se de uma estratégia não linear, possuindo elementos inerentes de caos. Ademais, em se tratando de uso programação neurolinguística direcionada ao indivíduo, uma das maneiras atuais mais eficazes de se usar estratégias de guerra neocortical é por meio da mídia social e das redes.

O grande objetivo da infiltração de inteligência nas redes de mídia social é criar uma mente de colmeia, a qual pode fazer com que seus membros invadam taticamente seu alvo de maneira aparentemente caótica, a fim de interromper seu ciclo de observação, orientação e decisão, o que leva ao colapso do adversário.[14] No contexto da Guerra Híbrida, essas são as massas que se encontram nos centros de poder simbólico e administrativo das autoridades como um todo unificado (se descentralizado), a fim de levar à mudança de regime pelo domínio da multidão (ou seja, caos organizado e direcionado).

As mentes da colmeia podem ser projetadas por meio de plataformas de mídia social e princípios de guerra em rede. As técnicas de "relações públicas" são muito utilizadas no mundo virtual e físico para que isso aconteça. O objetivo de tal estratégia é reunir o maior número possível de pessoas que passaram a compartilhar as mesmas convicções antigovernamentais. É importante ressaltar que esses indivíduos também devem ser "programados" por meio de uma guerra neocortical reversa para que se deseje provocar ativamente essa mudança quando o movimento for deflagrado. Com a mente de colmeia, as partes díspares contrárias a um regime se unificam. E, nesse sentido, o uso de *bots* maliciosos cumpre com grande competência a estratégia de guerra neocortical e de formação de mente de colmeia.

Os *bots* sociais apresentam características que desafiam os sistemas de detecção — sendo as principais:[15]

a) *Big data* social: coletar, armazenar e gerenciar dados de tal magnitude representa uma tarefa desafiadora. Além disso, algoritmos e ferramentas legados para gerenciamento de dados são inadequados para processá-los efetivamente. Os robôs sociais exploram a dificuldade de processamento dos dados de mídias sociais (que têm grandes volumes, alta velocidade e alta variedade) para não serem descobertos, dificultando o processo de detecção.

b) Conjuntos de dados modernos de robôs sociais: é limitado o número de conjuntos de dados sociais de robôs disponíveis publicamente. E faltam conjuntos de dados modernos que incluem traços de *bots* con-

[12] SZAFRANSKI, Richard. Neocortical warfare? The acme of skill. *Rand Publications MR All Series,* 1997. Disponível em: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch17.pdf. Acesso em: 27 Jan. 2020, p. 404.

[13] KORYBKO, Andrew. *Hybrid wars:* the indirect adaptive approach to regime change. Moscow: The People's Friendship University of Russia, 2015. p. 37.

[14] KORYBKO, Andrew. *Hybrid wars:* the indirect adaptive approach to regime change. Moscow: The People's Friendship University of Russia, 2015. p. 43-44.

[15] ZAGO, Mattia; NESPOLI, Pantaleone; PAPAMARTZIVANOS, Dimitrios; PÉREZ, Manuel Gil; MÁRMOL, Félix Gómez; KAMBOURAKIS, Georgios; PÉREZ, Gregorio Martínez. Screening out social bots interference: are there any Silver Bullets? *IEEE Communications Magazine*, New York, v. 57, n. 8, p. 98-104, Aug. 2019. DOI: 10.1109/MCOM.2019.1800520; p. 100.

temporâneos. Entre outros fatores, o número de seguidores, atividades recentes e a frequência de postagem são informações importantes que fornecem valor agregado para inspecionar os dados de mídias sociais, revelando *bots* malignos.

c) Detecção de comportamento semelhante ao humano dos *bots:* um desafio importante é o estudo das métricas e recursos para identificar diferenças comportamentais dos *bots* sociais entre as diversas redes sociais. Além disso, os comportamentos de *bot* já são bastante sofisticados, podendo imitar comportamentos realistas e produzir conteúdo credível com padrões temporais semelhantes aos humanos.

d) Comportamento em constante mudança dos robôs: conforme as estratégias de detecção evoluem, isso ocorre também com os exércitos que adaptam seu comportamento para permanecerem ocultos e continuarem silenciosamente suas atividades enganosas. É possível, assim, a eclosão de uma corrida armamentista interminável entre sistemas de detecção e *bots* em constante evolução.

e) Falta de ferramentas apropriadas de visualização: em razão da complexidade da estrutura de dados e da sua massividade, revelar e visualizar interconexões entre contas é uma tarefa complicada. As ferramentas tradicionais de visualização atingem seus limites ao lidar com conjuntos de dados em larga escala em constante evolução. Se a visualização de *big data* é uma tarefa difícil, a visualização de *big data* social é ainda mais difícil devido ao aumento da complexidade. Dessa forma, ter uma estrutura clara da interconexão entre os perfis ajudaria a identificar o grupo de influenciadores que guia o exército e, possivelmente, expor o ator principal por trás dele.

Quando se analisa o efeito dos *bots* em escala micro — ou seja, na influência que a difusão de informações que realizam —, podem causar danos epistêmicos significativos às deliberações internas de cada um. Cada cidadão delibera internamente ao formar julgamentos — e isso tem consequências políticas, pois esses julgamentos relacionam-se aos votos de cada indivíduo em um processo eleitoral.[16] Nesse sentido, algumas violações da independência epistêmica (como a repetição de mensagens, por exemplo) podem fazer com que os indivíduos considerem duas vezes as informações que sopesaram, distorcendo, assim, seus julgamentos, se os receptores não estiverem cientes da repetição. Disso resulta a necessidade normativa de que cada cidadão deve ignorar ou desconsiderar certos tipos de entradas de informações (por exemplo, mensagens de *bot* ou *retweets*) que provavelmente são apenas uma repetição daquilo que já foi levado em consideração em suas deliberações internas anteriores.

Pessoas aprendem umas com as outras — e, quanto mais pessoas relatam a mesma coisa, mais credível é provável que uma informação seja. Isso faz sentido se todos estiverem fornecendo evidências genuinamente independentes, mas não faz sentido se, como ocorreu nas eleições presidenciais dos EUA em 2016, muitos dos aparentes "relatórios de confirmação" constituírem réplicas do relatório original, reeditadas automaticamente por algum *bots* sociais. Quando se considera uma réplica como se fosse informação nova, as evidências equivalem à contagem dupla do relatório original — e as evidências de contagem dupla são tão ruins do ponto de vista epistêmico quanto a contagem de votos seria de uma perspectiva democrática.[17]

Agentes epistêmicos que não sejam completamente independentes, como os *bots*, podem impactar, significativamente, a opinião pública. Em primeiro lugar, cerca de metade do tráfego da web é proveniente de *bots*, e até milhões de contas no Facebook e no Twitter são contas de *bots* sociais.[18] Em segundo, os indivíduos são vulneráveis à repetição de mensagens e provavelmente superestimam o peso epistêmico das mensagens repetidas; eles também não têm condições de distinguir um argumento de clone de uma reivin-

[16] TANASOCA, Ana. Against bot democracy: the dangers of epistemic double-counting. *Perspectives on Politics*, Washington, v. 17, n. 4, p. 988-1002, 2019. DOI: https://doi.org/10.1017/S1537592719001154, p. 988.

[17] TANASOCA, Ana. Against bot democracy: the dangers of epistemic double-counting. *Perspectives on Politics*, Washington, v. 17, n. 4, p. 988-1002, 2019. DOI: https://doi.org/10.1017/S1537592719001154, p. 988.

[18] CONFESSORE, Nicholas; DANCE, Gabriel J. X.; HARRIS, Richard; HANSEN, Mark. The follower factory. *New York Times*, Jan. 27, 2018. Disponível em: https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html. Acesso em: 21 dez. 2019.

dicação independente. Terceiro, uma proporção substancial da população dos EUA recebe suas notícias das plataformas de mídia social: em agosto de 2017, 67% dos americanos relataram receber "pelo menos algumas de suas notícias nas mídias sociais", com o Twitter, em particular, aumentando sua acessibilidade em 15 pontos percentuais.[19] Quando se combinam esses fatos, é razoável pensar que agentes *bots* poderiam minar as deliberações internas e, inclusive, realmente transformar uma eleição. Eles fariam isso artificialmente, aumentando a credibilidade de alguns argumentos, levando os cidadãos a superestimar seu peso epistêmico.

Existe claramente um argumento para proibir *bots* de discussões políticas, mas a razão para isso — o dano epistêmico que pode ser causado ao julgamento das pessoas quando elas são expostas involuntariamente à repetição de mensagens — vai muito além de *bots*. Muitas repetições de mensagens também ocorrem nas interações humanas. Para saber o que fazer com o que os outros dizem, as pessoas precisam saber onde obtiveram suas informações e se é algo que já levaram devidamente em consideração.[20] Novas normas e políticas que regem as práticas discursivas são necessárias, especialmente devido ao modo como a interação *online* torna, cada vez mais difícil, para os indivíduos humanos, determinar o que precisam saber para avaliar com precisão as informações que estão recebendo.

A técnica de propaganda que mais se assemelha à batalha dos *bots*, para Peter Hirsch,[21] é o que tem sido chamado de campanhas "*Astroturf*", um tipo de propaganda empresarial (geralmente) projetada para simular a força da opinião pública sobre um assunto específico. Tais campanhas usaram uma variedade de técnicas, incluindo forjar centenas de cartas aos membros do Congresso, criar grupos de defesa de cidadãos supostamente preocupados e estabelecer operações para encontrar cidadãos neutros para endossar as opiniões dos interesses corporativos. Essas técnicas, como as redes de *bots*, produzem a impressão de que grandes segmentos da população apoiam as opiniões e a agenda da entidade patrocinadora (grupo de defesa, empresa, candidato, governo etc.). Mas o surgimento dos *bots* políticos é alarmante porque há uma competição como pano de fundo — representada pelos embates entre interesses corporativos que começarem a empregar essas técnicas primeiro ou os grupos de defesa de direitos — e fica difícil imaginar que qualquer grupo na batalha da opinião pública renuncie, voluntariamente, ao seu uso.

3 Bots e a formação do discurso político online

É fundamental ilustrar a presente pesquisa com dados e considerações mais específicas acerca da interferência dos *bots* sociais para formação do discurso político *on-line*. Nesse sentido, destaca-se a pesquisa de Emilio Ferrara,[22] sobre o papel dos *bots* no discurso político *on-line* em associação com três grandes eventos políticos (eleições presidenciais dos EUA de 2016; eleições da França de 2017; e eleições de meio-termo dos EUA de 2018). Sua primeira descoberta foi de que uma quantidade significativa de *bots* distorceu a discussão *online* na eleição presidencial dos EUA de 2016. Tais *bots* promoveram interações bem-sucedidas para com humanos por meio de *retweets* na mesma proporção que os usuários humanos.

Quanto às eleições francesas de 2017, *bots* promoveram uma campanha de desinformação pouco antes do pleito (conhecida como *MacronLeaks*).[23] Foi possível, para o pesquisador, identificar facilmente o início

[19] SHEARER, Elisa; GOTTFRIED, Jeffrey. News use across social media platforms. *Pew Research Center*, Sep. 2017. Disponível em: http://www.journalism.org/2017/09/ 07/news-use-across-social-media-platforms-2017/. Acesso em: 21 dez. 2019.

[20] TANASOCA, Ana. Against bot democracy: the dangers of epistemic double-counting. *Perspectives on Politics,* Washington, v. 17, n. 4, p. 988-1002, 2019. DOI: https://doi.org/10.1017/S1537592719001154, p. 999.

[21] HIRSCH, Peter Buell. Windmills in cyberspace. *Journal of Business Strategy*, Bingley, v. 38, n. 3, p. 48-51, 2017. DOI: 10.1108/JBS-02-2017-0023, p. 50.

[22] FERRARA, Emilio. Bots, elections, and social media: a brief overview. *Arxiv.org*. 03 Oct. 2019. Disponível em: https://arxiv.org/abs/1910.01720. Acesso em: 22 dez 2019, p. 15-16.

[23] MOHA, Megha. Macron leaks: the anatomy of a hack. *BBC News,* 9 May 2017. Disponível em: https://www.bbc.com/news/blogs-trending-39845105. Acesso em: 22 dez. 2019.

dessa campanha de desinformação no Twitter, bem como ilustrar como seu pico de popularidade era comparável ao da discussão política regular. Mas considera que essa campanha de desinformação não foi bem-sucedida, em parte porque foi adaptada às necessidades de informação e aos padrões de uso da comunidade de direita alternativa americana em vez do público de Língua Francesa. É interessante também observar a descoberta de que centenas de contas de *bots* foram redirecionadas das eleições de 2016 nos EUA para a França — o que sugere a existência de um mercado negro de *bots* políticos reutilizáveis.

Em relação às eleições de meio-termo de 2018 dos EUA, a análise ilustrou que não apenas os *bots* eram quase tão predominantes quanto nos outros dois eventos, mas também que os *bots* de discurso conservador foram centrais no núcleo altamente conectado da rede de *retweet*. As descobertas de Ferrara a partir de uma análise comparativa que contrastou a atividade de *bots* e humanos em 2016 e 2018 destacaram que um núcleo de mais de 245 mil usuários, dos quais 12,1% eram *bots*, estava ativo em ambos os eventos. Tais resultados sugerem que os *bots* podem ter evoluído para melhor mimetizar padrões temporais de atividade humana — o que, com a evolução da inteligência artificial, pode tornar ainda mais eficiente o trabalho de desinformação por *bots*, mas também mais difícil a sua diferenciação da atividade humana. Sendo assim, o pesquisador sugere que ferramentas tecnológicas de detecção não são mais suficientes, sendo necessário aprimorar políticas públicas e desenvolver melhor a regulação para obliterar a interferência de *bots* sociais no discurso político.

É interessante, no que concerne às ideologias dos *bots* políticos no Twitter e suas interações para com humanos, o estudo realizado por Luceri et al.,[24] em que se analisou o Twitter para estudar o discurso durante as eleições de meio-termo dos EUA de 2018. Nessa oportunidade, foram reunidos 2,6 milhões de tweets por 42 dias no dia da eleição de quase 1 milhão de usuários. Como resultado, os pesquisadores revelaram que os *bots* sociais conservadores compartilham a maioria dos tópicos de discussão com suas contrapartes humanas, enquanto os robôs liberais mostram menos sobreposição e uma atitude mais inflamatória. Ademais, os *bots* conservadores estão mais profundamente enraizados na rede social, sendo mais eficazes do que os liberais em exercer influência sobre os seres humanos.

Rofrío et al.[25] também apresentam evidências suficientes para mostrar que *bots* políticos foram usados nas mídias sociais durante as eleições de 2017 no Equador, e que tais contas automáticas foram usadas para promover ou desacreditar candidatos. Nesse sentido, quase 46% de todos os *bots* coletados apoiaram o candidato oficial, Lenín Moreno, e outros candidatos, como Guillermo Lasso, receberam quase um tweet contra para cada tweet a favor. Deixaram claro, também, que todos os candidatos equatorianos, sem exceção, prepararam contas no Twitter e suas contas aumentaram seus seguidores durante a campanha. E, nas eleições do Chile de 2017, Santana e Huerta Cánepa[26] investigaram quase 2 milhões de tweets coletados sobre a eleição, e analisados ou vinculados a qualquer um dos candidatos ou suas campanhas. E, no Facebook, foram analisadas 2.927 publicações oficiais dos candidatos e seus 453.668 comentários. Assim, descobriram que, embora no Facebook o comportamento era relativamente normal, no Twitter foi descoberto, no primeiro turno, que havia brigadas digitais que agem autonomamente tentando criar uma ilusão de apoio nas bases.

Corrobora esses dados todos a pesquisa de Kris Shaffer,[27] que, ao estudar as intersecções entre o uso de dados e a democracia, explorou vários problemas que deixam os cidadãos vulneráveis à desinformação, propaganda e *hackers* cognitivos. O primeiro tipo de problema é baseados na psicologia humana. Nesse tipo

[24] LUCERI, Luca; DEB, Ashok; BODAWY, Adam; FERRARA, Emilio. Red bots do it better: comparative analysis of social bot partisan behavior. *In:* WORLD WIDE WEB CONFERENCE, 2019, San Francisco. *Proceedings*…San Francisco: ACM, 2019. p. 1007-1012. DOI: 10.1145/3308560.3316735.

[25] ROFRÍO, Daniel *et al.* Presidential elections in Ecuador: bot presence in Twitter. *In:* INTERNATIONAL CONFERENCE ON EDEMOCRACY & EGOVERNMENT, 6., 2019, Quito. *Proceedings*…Quito: IEEE, 2019. p. 218-223. DOI: 10.1109/ICEDEG.2019.8734426.

[26] SANTANA, Luis E.; HUERTA CÁNEPA, Gonzalo. ¿Son bots?: automatización en redes sociales durante las elecciones presidenciales de Chile 2017. *Cuadernos.info*, Chile, v. 44, p. 61-77, 2019. DOI: 10.7764/cdi.44.1629.

[27] SHAFFER, Kris. *Data versus democracy*: how big data algorithms shape opinions and alter the course of history. Colorado: Apress, 2019. DOI: 10.1007/978-1-4842-4540-8_7, p. 109-110.

se encontra o que o autor denominou viés de confirmação (*confirmation bias*), a predisposição a acreditar em reivindicações que são consistentes com as crenças já defendidas pelas pessoas, fechando suas mentes em relação a reivindicações que desafiam suas visões de mundo. Também o piscar de atenção (*attentional blink*) torna difícil às pessoas manter suas faculdades críticas ativas ao encontrarem informações em um ambiente de mídia em constante mudança e em ritmo acelerado. Já o preparo (*priming*) torna as pessoas vulneráveis à mera repetição, especialmente quando não estão conscientes dela, pois a exposição repetida a uma ideia facilita que nossas mentes processem e, portanto, acreditem nessa ideia. Essas características, desenvolvidas ao longo da evolução, facilitam a formação de preconceitos e estereótipos reforçados e amplificados, ao longo do tempo, sem a ajuda da tecnologia digital.

Já o segundo tipo é técnico. A *mineração excessiva de dados pessoais*, combinada à *filtragem colaborativa*, além de permitir que as plataformas segmentem os usuários com mídia que incentiva o envolvimento *on-line*, reforçam as tendências que levaram a essa segmentação. A publicidade segmentada coloca, funcionalmente, esses dados do usuário à disposição daqueles que os usariam para direcionar o público para ganhos financeiros ou políticos.

Um terceiro tipo de problema diz respeito ao plano social, e se relaciona ao *rápido aumento do acesso à informação e às pessoas que a tecnologia digital oferece*. Se, por um lado, isso tem o potencial de libertar as pessoas de sua ignorância pluralista; por outro, revela que não estão prontas para lidar com as implicações sociais da informação que trafega por e entre comunidades com base principalmente em laços sociais fracos.

Em última análise, o autor expõe que a desinformação, da qual políticos tendenciosos se valem em suas estratégias, é um problema humano, e não técnico. Novas tecnologias de comunicação e dados não são inerentemente positivas, negativas ou neutras. Cada nova tecnologia tem seus próprios recursos e limitações que, assim como a mente humana, tornam certas vulnerabilidades mais severas que outras. E isso faz com que não haja solução puramente técnica para o problema, já que a desinformação é um comportamento perpetrado pelas pessoas, contra as pessoas, de acordo com os traços fundamentais da cognição e das comunidades humanas. Sendo assim, as soluções para esses problemas na esfera política da formação de opinião pública devem também ser humanas.

Não apenas em períodos eleitorais os *bots* políticos são usados. As contas falsas das mídias sociais também espalham mensagens pró-governamentais, aumentam os números de seguidores de sites e causam tendências artificiais. A propaganda gerada por *bot* e o desvio de direção se tornaram estratégia política mundial, tendo sido tais estratégias implementadas em vários países: Rússia, México, China, Austrália, Reino Unido, Estados Unidos, Azerbaijão, Irã, Bahrein, Coreia do Sul, Turquia, Arábia Saudita e Marrocos e Venezuela.[28] De fato, os especialistas estimam que o tráfego de *bots* agora representa mais de 60% de todo o tráfego *on-line* — quase 20% em relação a, apenas, dois anos atrás.

4 Questões fundamentais para a regulação do uso dos bots

Conforme ocorre a evolução e a expansão da automação digital em direção aos contextos sociais, as respostas do sistema jurídico à produção e difusão de comunicações falsas e odiosas por algoritmos representam um problema político urgente. Conforme as comunicações entre humanos se tornam cada vez mais embasadas em e dependentes de soluções digitais, a legalidade (e a legitimidade) das informações criadas por algoritmos que prejudicam a reputação ou a dignidade de indivíduos, entidades ou grupos é uma questão política colocada e respondida de maneira diferente em todo o mundo. Nesse sentido, Meg Leta Jones[29]

[28] FORELLE, Michelle; HOWARD, Phil; MONROY-HERNÁNDEZ, Andrés; SAVAGE, Saiph. Political bots and the manipulation of public opinion in Venezuela. *Arxiv.org*. 25 June 2015. Disponível em: https://arxiv.org/abs/1507.07109. Acesso em: 22 dez 2019, p. 6.

[29] JONES, Meg Leta. Silencing bad bots: global, legal and political questions for mean machine communication. *Communication Law*

apresenta uma série de questões pendentes, nos ordenamentos jurídicos ao redor do mundo, que passam a exigir atenção internacional e interdisciplinar em relação ao uso dos *bots*.

Primeiramente, há de se entender que a complexidade e a consideração de muitos detalhes, portanto, são fundamentais na regulação dos *bots*.[30] Todos os envolvidos tecnológica ou normativamente com plataformas sociais que incluam ou dependam de comunicação gerada por algoritmos designers, produtores, usuários e reguladores de plataformas que incluem ou dependem de comunicação gerada por algoritmos devem abordar o potencial de comunicação ruim (falha ou odiosa) da máquina. Mesmo aplicativos aparentemente inocentes — por exemplo, que sugerem a próxima palavra para uma pesquisa na internet ou um chatbot amigável — correm o risco de responsabilidade civil e criminal e modificações caras nos programas (na esteira dos exemplos acima dados, é de se imaginar, por exemplo, um algoritmo que associe determinadas etnias e raças a animais, comportamentos desonrosos, ou algo similar, numa sugestão de busca do Google).

Há muitas questões jurídicas interessantes que provavelmente não serão respondidas com base na política existente de remoção rápida para uma comunicação corriqueira de máquina. Bons exemplos de tais questões dizem respeito: i) à hermenêutica das normas de responsabilidade dos intermediários nas comunicações (ou seja, que artigos, de que leis/tratados, devem ser aplicados ou não às práticas concernentes ao discurso dos *bots*); ii) às distinções nebulosas entre editor e criador de conteúdo na comunicação por máquina (em outras palavras, quem deve ser responsabilizado pelo discurso proferido por *bots*); iii) a elementos humanos de normas atinentes às ofensas contra a honra e discurso de ódio (em suma, o que pode ser considerado ofensivo ou não, considerando-se cada caso das comunicações potencialmente danosas). Assim como ocorre com muitas tecnologias emergentes, algumas dessas preocupações e aplicações dependem de pesquisas de cientistas sociais que podem ajudar a formar um enquadramento teórico e obter inspiração sobre a integração e o impacto de tais tecnologias.

Nathalie Marechal[31] considera que uma boa estrutura normativa para o uso de *bots* em redes sociais deve ter três componentes: i) divulgação (as contas de *bot* devem ser claramente identificadas como tal); ii) consentimento (*bots* não devem iniciar contato com usuários humanos sem o seu consentimento, incluindo interações como curtir, favoritar ou retwittar); iii) uso secundário (os proprietários de *bots* não devem usar as informações coletadas sobre os usuários para outros fins que não os divulgados aos usuários no momento da coleta). Esses pilares normativos, inspirados no projeto *Ranking Digital Rights*, deveriam ser usados, principalmente, nas estratégias de autorregulação das plataformas de redes sociais.

Conforme Lamo e Calo,[32] tramitam no Estado da Califórnia e no Senado dos EUA projetos de lei sobre divulgação de *bots* —, no caso da primeira, tornar-se-á ilegal o envolvimento de *bots* em marketing ou propaganda eleitoral sem revelar que não são humanos. O Senado dos Estados Unidos também está avaliando uma possível lei geral de divulgação de *bots*. A princípio, os autores parecem não considerar censura a obrigatoriedade da revelação do caráter não humano do *bot* ao realizar a sua comunicação. Porém, alertam para a possibilidade de desrespeito à liberdade de expressão qualquer restrição muito cabal à possibilidade de anonimato. Tem sido comum na história da evolução da civilização a desconfiança acerca de novas formas tecnológicas de comunicação (palavra escrita, imprensa, internet etc.). E é muito fácil fazer com que essa desconfiança degringole em censura. Contudo, tecnologias úteis de comunicação encontram, com o tempo, maneiras de florescer. E a liberdade de expressão, primordial para a democracia, se expandiu para atender a essas tecnologias amplamente em seus próprios termos.[33]

and Policy, Belgium, v. 23, n. 2, p. 159-195, 2018. DOI: 10.1080/10811680.2018.1430418, p. 159 e ss.

30 JONES, Meg Leta. Silencing bad bots: global, legal and political questions for mean machine communication. *Communication Law and Policy*, Belgium, v. 23, n. 2, p. 159-195, 2018. DOI: 10.1080/10811680.2018.1430418, p. 195.

31 MARECHAL, Nathalie. When bots tweet: toward a normative framework for bots on social networking sites. *International Journal of Communication*, Los Angeles, v. 10, p. 5022–5031, 2016, p. 5029.

32 LAMO, Madeline; CALO, Ryan. Regulating bot speech. *UCLA Law Review*, Los Angeles, v. 66, p. 988-1028, 2019. DOI: 10.2139/ssrn.3214572, p. 990.

33 LAMO, Madeline; CALO, Ryan. Regulating bot speech. *UCLA Law Review*, Los Angeles, v. 66, p. 988-1028, 2019. DOI:

Apenas o tempo dirá se os vários tipos de *bots* que existem e que podem vir a surgir atendem ao limite da utilidade. É claro que já se demonstrou que seu abuso pode causar danos sérios, e que a regulação é necessária. Não se pode, contudo, deixar de lado preocupações fundamentais da liberdade de expressão mesmo na regulação dos *bots*. Eles representam uma nova forma de comunicação (na capacidade de surpreender, na capacidade de produzir fala em escala e na maneira como alguns tipos de *bots* testam as intuições humanas sobre os limites entre pessoa e máquina), muitas vezes assustadora e, em várias, prejudicial.

Há de se reafirmar a preocupação com a propagação de notícias falsas mediante o uso de bots em relação às reputações (individuais ou de grupos), seu uso eleitoral e os danos civis que podem vir a causar. Programadores desenvolvem *bots* para decifrar e resumir grandes quantidades de dados, e empresas de notícias usam tais *bots* para coletar informações e rapidamente publicar histórias. Conforme a tecnologia evolui, *bots* escreverão histórias, as quais correrão o risco de retratar falsamente a situação de um ser humano — o qual, se prejudicado, processará a empresa por difamação, perdas e danos etc. Conforme Laurel Witt,[34] para aplicar a lei a um caso envolvendo *bots*, um tribunal deve eliminar o elemento de negligência da lei de difamação e acrescentar a doutrina do respondente superior, responsabilizando o supervisor ou o proprietário do *bot*, porque esses indivíduos podem verificar a história em busca de informações falsas ou realizar correções. Traduzindo-se o posicionamento para o âmbito constitucional e civilístico brasileiro, pode-se afirmar que o autor defende a responsabilização objetiva por abuso do direito à livre manifestação do pensamento — o que deve ser sopesado quando da criação de regulação específica para a conduta para com *bots* em mídias sociais.

No que concerne à regulação do uso de *bots* sociais em eleições, Ruediguer et al.[35] indicam que, ainda, não há normatizações específicas na legislação eleitoral brasileira, ou na atividade judicial, ou na esfera regulatória.[36] Sendo os *bots* sociais espécie de ferramenta de alta complexidade técnica que pode potencializar a desinformação em massa e produzir efeitos deletérios sobre o funcionamento de uma democracia, é fundamental que os atores envolvidos na sua regulação sejam instruídos substantivamente em relação às peculiaridades técnicas do fenômeno e aos desafios políticos que dele decorrem — particularmente, a falta de transparência e *accountability* que permeia atualmente a utilização dessas ferramentas no meio digital. Expandir a conscientização da sociedade civil e dos eleitorados sobre os riscos de desinformação digital possibilita o surgimento de novas estratégias não estatais de contenção do problema (como estratégias de checagem de fatos) , mas legisladores e magistrados eleitorais também têm de se engajar ativamente no debate e na busca por soluções adequadas, que coíbam as estruturas de desinformação que atuam usando *bots* sociais, mas que também não constranjam a inovação e a experimentação nos processos eleitorais democráticos.

Karine K. e Silva[37] retrata que a indústria, devido à sua experiência e infraestrutura estratégica, está bem

10.2139/ssrn.3214572, p. 1028.

[34] WITT, Laurel. Preventing the rogue bot journalist: protection from non-human defamation. *Colorado Technology Law Journal*, Boulder, v. 15, n. 2, p. 517-548, 2017, p. 547-548.

[35] RUEDIGUER, Marco Aurélio *et al. Bots e o direito eleitoral brasileiro:* nas eleições de 2018. Rio de Janeiro: FGV/DAPP, 2019. Disponível em: http://hdl.handle.net/10438/26227. Acesso em: 23 dez 2019.

[36] Apesar da falta de menção específica a *bots* ou robôs na legislação eleitoral brasileira, Ruediguer et al. (2019) apontam e comentam diversos instrumentos regulatórios análogos em relação a práticas que os envolvam. O artigo 57-B, §2º da Lei nº 9.504/97 (BRASIL, 1997) proíbe a criação de perfis falsos em redes sociais com a finalidade de propagar conteúdo eleitoral. E o art. 57-B, §3º da mesma Lei proíbe que o impulsionamento de propaganda eleitoral na internet ocorra com ferramentas não disponibilizadas pelo provedor da aplicação em que a propaganda será impulsionada (ainda que gratuitamente). Assim, quem usar *bots* para propagar conteúdo eleitoral e obter maior visibilidade por interação em uma rede social está agindo ilicitamente, pois os *bots* não são disponibilizados pelo provedor da rede social. Ademais, usar *bots* para administrar de perfis falsos é tentativa de evitar a identificação e responsabilização do divulgador do conteúdo eleitoral, colocando-o em posição de pretenso anonimato — o que é vedado pelo art. 57-D da Lei nº 9.504/97 em campanha eleitoral na internet. Observa-se que, conforme apontado no art. 33, §2º da Resolução TSE 23.551/17 (BRASIL, 2017), somente é considerada anônima a divulgação de conteúdo quando não for possível a identificação dos usuários após a adoção das providências previstas nos arts. 10 e 22 da Lei nº 12.965/14 (Marco Civil da Internet) (BRASIL, 2014).

[37] SILVA, Karine K. How industry can help us fight against botnets: notes on regulating private-sector intervention. *International Review of Law, Computers & Technology,* Abingdon, v. 31, n. 1, p. 105-130, 2017. DOI: 10.1080/13600869.2017.1275274.

equipada para lidar com redes de *bots* de uma maneira que a aplicação da lei pelo setor público, por si só, não pode igualar. As empresas envolvidas com a comunicação pela Internet, por sua vez, pode se beneficiar dessas operações por terem uma oportunidade essencial de defender suas redes, proteger seus clientes e fortalecer seu modelo de negócios. Ou seja, as empresas, e não as autoridades públicas, estão em uma posição privilegiada para detectar, prevenir e reagir oportunamente às redes de *bots*.

Mas a participação da indústria enfrenta desafios importantes, pois tal participação encontra obstáculos nas críticas à viabilidade e legitimidade de um modelo híbrido de aplicação da lei — já que as promessas de que, ao envolver as nações mais significativas para a indústria da Internet, esta aumentará sua resposta às redes de *bots*. Dentre os elementos críticos encontram-se a falta de transparência e responsabilidade das atividades da indústria da Internet, regras pouco claras de responsabilidade, medo de violações de direitos fundamentais e captura regulatória e a ausência de incentivos suficientes para garantir que as empresas ajam no interesse público. Ademais, as empresas do setor de internet podem não possuir as melhores informações para decidir sobre a legalidade das contramedidas e, assim, ver suas atividades prejudicadas por altos riscos de responsabilidade. Assim, sem instrumentos regulatórios que esclarecem esses desafios, os atores privados podem não apenas ter os meios para decidir se e em que circunstâncias eles devem responder a um ataque, mas também os incentivos para combater os crimes nas redes de *bots*.

Para Richard L. Hasen,[38] no que tange ao Direito Eleitoral na era da pós-verdade (situação agravada pela difusão de notícias falsas por *bots*), tem-se que tal ramo jurídico pode ajudar em alguns aspectos (i.e. com requisitos aprimorados de rotulagem de verdade na campanha para lidar com falsidades, ou com leis aprimoradas de divulgação de financiamento de campanhas). Ambos os tipos de leis ajudariam os eleitores a se tornarem mais informados ao fazerem escolhas de campanha e dar-lhes melhor noção de quem está tentando influenciar sua opinião e como — mas a lei não pode fazer mais do que isso. Conforme a sociedade se divide em questões fundamentais da verdade, torna-se mais difícil tomar decisões racionais e aceitar dados provenientes de "bolhas" de informação externas. Nesse ponto, parece pouco o que pode ser feito para impedir essas divisões, além de tentar escolher os juízes mais abertos.

Acerca de uma regulação híbrida entre público e privado para tecnologias que envolvam robôs, Villaronga e Golia[39] afirmam que, devido à sua natureza específica de *soft law* privada, os padrões atuais que governam a tecnologia de robôs tendem a ser baseados em princípios únicos — nesse caso, segurança. Os padrões privados tendem a desconsiderar outros princípios e valores jurídicos profundamente enraizados nos sistemas sociais em que humanos e tecnologia de robôs operam. Juntamente à falta de uma dimensão legal mais ampla, além disso, esses padrões carecem de legitimidade social e responsabilidade. Sustentam, contudo, que a formulação de políticas públicas fornece proteção abrangente aos usuários de robôs. Ainda assim, leis rígidas e os possíveis processos legislativos estão longe de serem adequados para as tecnologias emergentes de robôs. A volatilidade desse campo temático dificulta o entendimento dos riscos e impactos associados e a antecipação de medidas efetivas para mitigá-los. Propõe-se, para a regulação híbrida púbico-privada de robôs nesse sentido, a vinculação de avaliações de impacto de tecnologia a avaliações de impacto regulatórias mediante a criação de repositórios de dados compartilhados. Além disso, propõe-se o fortalecimento dos padrões privados por meio de sua inclusão na regulamentação, em contratos privados ou por meio de sanções sociais e de reputação. Ou seja, deve haver um aproveitamento do conhecimento privado para formulação de políticas públicas, mas também um fortalecimento das iniciativas privadas de regulação.

Apesar de uma primeira análise superficial sugerir que o problema do uso de *bots* para influenciar eleições presidenciais brasileiras (e outras questões democráticas importantes de nível nacional) é um problema pos-

[38] HASEN, Richard L. Deep fakes, bots, and siloed justices: american election law in a post-truth world. *St. Louis University Law Journal*, St. Louis, 2019. Disponível em: https://ssrn.com/abstract=3418427. Acesso em: 25 dez. 2019, p. 33.

[39] VILLARONGA, Eduard Fosch; GOLIA, Angelo Jr. Robots, standards and the law: rivalries between private standards and public policymaking for robot governance. *Computer Law & Security Review,* Amsterdã, v. 35, n. 2, p. 129-144, 2019. DOI: 10.1016/j.clsr.2018.12.009, p. 141-142.

terior ao pleito nacional de 2016 dos EUA (em que foi eleito Donald Trump), há pesquisas que demonstram ser esse problema bastante anterior e influente. A Diretoria de Análise de Políticas Públicas, da Fundação Getúlio Vargas[40] e o *Oxford Internet Institute* (OII), no âmbito do *Computational Propaganda Research Project*[41] produziram relatórios de pesquisas bastante interessantes a respeito disso. Segundo o estudo do DAPP/FGV,[42] os *bots* foram responsáveis por cerca de 10% das interações no Twitter durante a campanha para as eleições presidenciais brasileiras de 2014. Especificamente no momento do debate na Rede Globo de Televisão, entre Dilma Rousseff (PT) e Aécio Neves (PSDB) no segundo turno, aproximadamente 20% das interações favoráveis a Aécio Neves no Twitter foram impulsionadas por robôs.

Ademais, o relatório do OII ressalta que robôs estiveram por trás das campanhas de Aécio Neves, Dilma Rousseff e também de Eduardo Campos nas eleições de 2014.[43] Foi identificado que as *hashtags* relacionadas ao candidato do PSDB triplicaram em 15 minutos de debate transmitido pela TV. Também é de se ressaltar que a OII cita um estudo realizado pelo Muda Mais, movimento ligado ao PT, acusando a presença de mais de 60 contas automatizadas no Twitter e no Facebook em favor de Aécio Neves. Conforme o relatório do OII, tanto a campanha do PT quanto a do PSDB usaram *bots*, mas nesse caso, a plataforma do PSDB fez isso em maior escala, tendo investido cerca de R$ 10 milhões no desenvolvimento de contas automatizadas em redes sociais populares (Facebook WhatsApp e Twitter , mormente).

No que tange ao pleito presidencial de 2018 no Brasil, ocorreram importantes denúncias relacionadas a indícios de contratação de serviços de disparo de mensagens por *bots* e outras ferramentas automatizadas — serviço cada vez mais oferecido por empresas a campanhas eleitorais, que ainda não tem regulamentação específica pela legislação eleitoral brasileira.[44] Paradigmático disso é o exemplo das investigações conduzidas pelo Tribunal Superior Eleitoral brasileiro em razão de reportagem do jornal "Folha de São Paulo", que apurou a eventual contratação não declarada desse tipo de serviços por empresas apoiadoras da candidatura de Jair Bolsonaro (PSL/PRTB), com disparo em massa de mensagens via WhatsApp: na ausência de norma clara versando sobre o uso de *bots* e outras ferramentas automatizadas, alegou-se abuso de poder econômico (por causa do recebimento de doação irregular de pessoas jurídicas, que é proibida desde 2015, por força de decisão do Supremo Tribunal Federal), uso de perfis falsos para propaganda eleitoral e compra irregular de cadastros de usuários. Mas, até o momento, não houve, ainda, decisão de mérito proferida no âmbito dessas ações ou em outras similares, e sequer há sinais claros acerca do posicionamento da Justiça Eleitoral quanto a esse tipo de questão na ausência de regulação específica.

5 Considerações finais

Entender o fenômeno do surgimento dos *bots* exige uma abordagem complexa. Estes constituem uma categoria múltipla , de acordo com sua estrutura, função e utilidade. Há *bots* úteis, benignos; mas também há aqueles destinados a causar distorções, confusões, difundir notícias falsas etc. E, na atualidade, são altamente elaborados, a ponto de mimetizaram, de forma bastante competente, comportamentos humanos nas redes,

[40] RUEDIGUER, Marco Aurélio; GRASSI, Amaro; GUEDES, Ana (coord.). *Robôs, redes sociais e política no Brasil*: análise de interferências de perfis automatizados de 2014. Rio de Janeiro: DAPP/FGV-Rio, 2018. Disponível em: http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web. Acesso em: 27 jan. 2020.

[41] ARNAUDO, Dan. Computational propaganda in Brazil: social bots during elections. *Oxford University Research Archive*, 2017. Disponível em: https://ora.ox.ac.uk/objects/uuid:e88de32c-baaa-4835-bb76-e00473457f46. Acesso em: 27 jan. 2020.

[42] RUEDIGUER, Marco Aurélio; GRASSI, Amaro; GUEDES, Ana (coord.). *Robôs, redes sociais e política no Brasil*: análise de interferências de perfis automatizados de 2014. Rio de Janeiro: DAPP/FGV-Rio, 2018. Disponível em: http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web. Acesso em: 27 jan. 2020.

[43] ARNAUDO, Dan. Computational propaganda in Brazil: social bots during elections. *Oxford University Research Archive,* 2017. Disponível em: https://ora.ox.ac.uk/objects/uuid:e88de32c-baaa-4835-bb76-e00473457f46. Acesso em: 27 jan. 2020, p. 12-15.

[44] RUEDIGUER, Marco Aurélio *et al. Bots e o direito eleitoral brasileiro*: nas eleições de 2018. Rio de Janeiro: FGV/DAPP, 2019. Disponível em: http://hdl.handle.net/10438/26227. Acesso em: 23 dez. 2019, p. 12-13.

evitando, assim, a detecção por ferramentas comuns. Dentre esses comportamentos nocivos que mimetizam o humano, pode-se encontrar o *trolling*, que reforça posicionamentos em discussões *on-line* de modo falso e perverso, gerando desestabilização de discussões, quebra de confiança em comunidades de debates — muitas vezes de modo automatizado, pois os *bots* sociais também podem ser programados para agirem como trolls — e, portanto, enfraquecendo as possibilidades de formação de opinião, bem como fortalecendo a polarização de opiniões com base em posicionamentos emotivos, mediante o uso de redes sociais.

Um uso interessante e benéfico de *bots* seria seu "treino" (programação) para agirem como moderadores em espaços virtuais (comunidades, fóruns etc.) de discussão de tópicos publicamente importantes. Contudo, mesmo esse uso está sujeito à interferência de preconceitos humanos, pois os programadores poderiam (até mesmo involuntariamente) inserir suas concepções, muitas vezes errôneas, nos algoritmos dos *bots*. Portanto, melhorar o humano que programa é passo importante para que o instrumento não seja passível desses vícios anti-democráticos.

Além de terem influência deletéria para a constituição da opinião pública, os *bots* sociais são de difícil detecção, pois se valem de desafios tecnológicos bastante significativos — principalmente porque, conforme as ferramentas de detecção de *bots* evoluem, também evoluem as técnicas de ocultação de tais aparatos.

Bots causam danos epistêmicos a processos eleitorais no nível macro, principalmente por terem a capacidade de influenciar, em nível micro, a relevância de determinadas informações (sejam elas verdadeiras ou falsas). Fazem com que determinados argumentos sejam tão redundantes que tenham a aparência de verdadeiros em razão da repetição. Isso dificulta a deliberação racional individual — o que, quando elevado a potências numéricas elevadas, já é nocivo por si só. Agrava essa situação o fato de que posicionamentos políticos se valem não apenas da racionalização, mas sim de argumentos de peso emotivo muito alto — como ocorre com fake news por exemplo. Ou seja: tanto no nível racional quanto no emotivo o uso de *bots* sociais causadores de redundância de informações podem distorcer eleições.

Soluções tecnológicas, apesar do grande descompasso entre o desenvolvimento do problema e o dessas soluções — o que, infelizmente, parece seguir um padrão do tipo "enxugar gelo" — devem continuar a ser desenvolvidas no âmbito dos *bots* sociais que disseminam desinformação. Contudo, é primordial que o problema não seja abordado unicamente com base no desenvolvimento tecnológico, pois, além do descrito descompasso técnico, há a exploração, por parte de políticos mal-intencionados, de características da psiquê e da socialização humanas. Ao serem desenvolvidas estratégias políticas e jurídicas para tal problema, portanto, a transdiciplinaridade entre conhecimentos técnicos e psicossociais (principalmente) deve ser considerada.

Qualquer discussão democrática acerca da regulação do uso dos *bots* deve considerar, em primeiro lugar, o fato de que não se trata de um problema meramente técnico — ou seja, da necessidade de se investir tempo e recursos materiais em políticas públicas de detecção de *bots* prejudiciais, ou assemelhados. É necessário conceber que a desinformação elevada a altas potências é apenas uma possibilidade de uso dos *bots*, e que nem todos são nocivos inerentemente. E, também, que boa parte da desinformação não ocorre, apenas, por causa da tecnologia em si, mas também, em razão do conhecimento da natureza humana e das interações sociais por aqueles que nocivamente buscam fazer usos antidemocráticos da tecnologia.

Ademais, questões que dizem respeito às técnicas legais/jurídicas de interpretação das leis existentes e válidas acerca das práticas relacionadas a *bots*, bem como sobre quem pode (ou não) ser responsabilizado por esse discurso, devem ser consideradas para a construção da regulação da comunicação automatizada dependente de algoritmos.

Mas é primordial, em tal debate democrático, para além da transdiciplinaridade tecnologia/humanidades/ciências sociais, considerar o perigo sempre iminente de se exagerar na regulação, bem como essa nova forma de liberdade de expressão passível de censura.

É importante considerar, também, que o estabelecimento de princípios e regras claras — tanto nas experimentações normativas estatais quanto autorregulatórias — que versem sobre a divulgação, o consentimento e o uso secundário de dados de usuários humanos que entrem em contato com contas de *bots* é importante. Tais pilares normativos impõem limites que dizem respeito à privacidade das pessoas, e, como em qualquer comunicação, auxiliam até mesmo a estabilização de expectativas de comportamentos *on-line* (ou seja, as pessoas poderão saber até onde pode ocorrer comunicação acerca de suas individualidades). Dentre o estabelecimento de bases normativas claras para a regulação, no que concerne à difamação, uma boa solução talvez seja elencar, na principiológica atinente ao uso de *bots*, o Princípio da Responsabilização Objetiva pelo abuso do direito fundamental à liberdade de expressão, no que tange à regulação pelo Direito brasileiro (e de outros ordenamentos que possuam tal possibilidade).

Uma opção para auxiliar a elaboração da regulação das práticas relacionadas a *bots* na internet seria a participação do setor privado, com suas experiências, em um modelo híbrido em que o Poder Público, munido da sua força coercitiva e processo legislativo legítimo, estabeleça a regulação geral, e o setor privado, dotado de *know how* e meios tecnológicos adequados, auxilie tanto a elaboração da lei quanto a tarefa de executá-la. Porém, essa possibilidade não deve ser sopesada ingenuamente, uma vez que o setor privado padece de críticas totalmente fundadas relacionadas ao mau uso de informações, desrespeito a direitos fundamentais e falta de transparência, por exemplo.

Referências

ARNAUDO, Dan. Computational propaganda in Brazil: social bots during elections. *Oxford University Research Archive*, 2017. Disponível em: https://ora.ox.ac.uk/objects/uuid:e88de32c-baaa-4835-bb76-e00473457f46. Acesso em: 27 jan. 2020.

BINNS, Reuben Binns; VEALE, Michael; VAN KLEEK, Max; SHADBOLT, Nigel Shadbolt. Like trainer, like bot? Inheritance of bias in algorithmic content moderation. *In*: INTERNATIONAL CONFERENCE SOCINFO, 9., 2017, Oxford. *Proceedings*… Oxford: Springer, 2017. p. 405-415. Part II. DOI: 10.1007/978-3-319-67256-4_32.

BRADSHAW, Samantha; HOWARD, Philip N. The global disinformation order: 2019 global inventory of organised social media manipulation. *In*: WORKING PAPER, 2., 2019, Oxford. *Proceedings*...Oxford: Project on Computational Propaganda, 2019. Disponível em: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf. Acesso em: 26 dez. 2019.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 dez. 2019.

BRASIL. *Lei nº 9.504, de 30 de setembro de 1997*. Estabelece normas para as eleições. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9504.htm. Acesso em: 23 dez. 2019.

BRASIL. Tribunal Superior Eleitoral. *Resolução nº 23.551, de 18 de dezembro de 2017*. Dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral nas eleições. Disponível em: http://www.tse.jus.br/legislacao-tse/res/2017/RES235512017.html. Acesso em: 23 dez. 2019.

CONFESSORE, Nicholas; DANCE, Gabriel J. X.; HARRIS, Richard; HANSEN, Mark. The follower factory. *New York Times*, Jan. 27, 2018. Disponível em: https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html. Acesso em: 21 dez. 2019.

FERRARA, Emilio. Bots, elections, and social media: a brief overview. *Arxiv.org*. 03 Oct. 2019. Disponível

em: https://arxiv.org/abs/1910.01720. Acesso em: 22 dez. 2019.

FERRARA, Emilio; VAROL, Onur; DAVIS, Clayton; MENCZER, Filippo, FLAMMINI, Alessandro. The rise of social bots. *Communications of the ACM*, New York, v. 59, n. 7, p. 96-104, 2016. DOI: 10.1145/2818717.

FORELLE, Michelle; HOWARD, Phil; MONROY-HERNÁNDEZ, Andrés; SAVAGE, Saiph. Political bots and the manipulation of public opinion in Venezuela. *Arxiv.org*. 25 June 2015. Disponível em: https://arxiv.org/abs/1507.07109. Acesso em: 22 dez. 2019.

GORWA, Robert; GUILBEAULT, Douglas. Unpacking the social media bot: a typology to guide research and policy. *Policy and Internet*, 2018. DOI: 10.1002/poi3.184.

HASEN, Richard L. Deep fakes, bots, and siloed justices: american election law in a post-truth world. *St. Louis University Law Journal,* St. Louis, 2019. Disponível em: https://ssrn.com/abstract=3418427. Acesso em: 25 dez. 2019.

HIRSCH, Peter Buell. Windmills in cyberspace. *Journal of Business Strategy*, Bingley, v. 38, n. 3, p. 48-51, 2017. DOI: 10.1108/JBS-02-2017-0023.

HOWARD, Philip N.; WOOLEY, Samuel; CALO, Ryan. Algorithms, bots, and political communication in the US 2016 election: the challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics*, Oxfordshire, v. 15, n. 2, p. 81-93, 2018. DOI: 10.1080/19331681.2018.1448735.

JONES, Meg Leta. Silencing bad bots: global, legal and political questions for mean machine communication. *Communication Law and Policy*, Belgium, v. 23, n. 2, p. 159-195, 2018. DOI: 10.1080/10811680.2018.1430418.

KORYBKO, Andrew. *Hybrid wars:* the indirect adaptive approach to regime change. Moscow: The People's Friendship University of Russia, 2015.

LAMO, Madeline; CALO, Ryan. Regulating bot speech. *UCLA Law Review*, Los Angeles, v. 66, p. 988-1028, 2019. DOI: 10.2139/ssrn.3214572.

LUCERI, Luca; DEB, Ashok; BODAWY, Adam; FERRARA, Emilio. Red bots do it better: comparative analysis of social bot partisan behavior. *In:* WORLD WIDE WEB CONFERENCE, 2019, San Francisco. *Proceedings*…San Francisco: ACM, 2019. p. 1007-1012. DOI: 10.1145/3308560.3316735.

MARECHAL, Nathalie. When bots tweet: toward a normative framework for bots on social networking sites. *International Journal of Communication*, Los Angeles, v. 10, p. 5022–5031, 2016.

MOHA, Megha. Macron leaks: the anatomy of a hack. *BBC News*, 9 May 2017. Disponível em: https://www.bbc.com/news/blogs-trending-39845105. Acesso em: 22 dez. 2019.

OBERER, Birgit; ERKOLLAR, Alptekin; STEIN, Anna. Social bots: act like a human, think like a bot. *In*: STUMPF, Marcus (ed.). *Digitalisierung und kommunikation:* konsequenzen der digitalen transformation für die wirtschaftskommunikation. Wiesbaden: Springer, 2019. p. 311-327.

PAAVOLA, Jarkko; HELO, Tuomo; JALONEN, Harri; SARTONEN, Miika; HUHTINEN, Aki-Mauri. Understanding the trolling phenomenon: the automated detection of bots and cyborgs in the social media. *Journal of Information Warfare*, Yorktown, v. 15, n. 4, p. 100-111, 2016.

ROFRÍO, Daniel *et al.* Presidential elections in Ecuador: bot presence in Twitter. *In:* INTERNATIONAL CONFERENCE ON EDEMOCRACY & EGOVERNMENT, 6., 2019, Quito. *Proceedings*…Quito: IEEE, 2019. p. 218-223. DOI: 10.1109/ICEDEG.2019.8734426.

RUEDIGUER, Marco Aurélio *et al. Bots e o direito eleitoral brasileiro:* nas eleições de 2018. Rio de Janeiro: FGV/DAPP, 2019. Disponível em: http://hdl.handle.net/10438/26227. Acesso em: 23 dez. 2019.

RUEDIGUER, Marco Aurélio; GRASSI, Amaro; GUEDES, Ana (coord.). *Robôs, redes sociais e política no*

Brasil: análise de interferências de perfis automatizados de 2014. Rio de Janeiro: DAPP/FGV-Rio, 2018. Disponível em: http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web. Acesso em: 27 jan. 2020.

SANTANA, Luis E.; HUERTA CÁNEPA, Gonzalo. ¿Son bots?: automatización en redes sociales durante las elecciones presidenciales de Chile 2017. *Cuadernos.info,* Chile, v. 44, p. 61-77, 2019. DOI: 10.7764/cdi.44.1629.

SHAFFER, Kris. *Data versus democracy:* how big data algorithms shape opinions and alter the course of history. Colorado: Apress, 2019. DOI: 10.1007/978-1-4842-4540-8_7.

SHEARER, Elisa; GOTTFRIED, Jeffrey. News use across social media platforms. *Pew Research Center*, Sep. 2017. Disponível em: http://www.journalism.org/2017/09/ 07/news-use-across-social-media-platforms-2017/. Acesso em: 21 dez. 2019.

SILVA, Karine K. How industry can help us fight against botnets: notes on regulating private-sector intervention. *International Review of Law, Computers & Technology,* Abingdon, v. 31, n. 1, p. 105-130, 2017. DOI: 10.1080/13600869.2017.1275274.

SZAFRANSKI, Richard. Neocortical warfare? The acme of skill. *Rand Publications MR All Series,* 1997. Disponível em: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch17.pdf. Acesso em: 27 Jan. 2020.

TANASOCA, Ana. Against bot democracy: the dangers of epistemic double-counting. *Perspectives on Politics,* Washington, v. 17, n. 4, p. 988-1002, 2019. DOI: https://doi.org/10.1017/S1537592719001154.

VILLARONGA, Eduard Fosch; GOLIA, Angelo Jr. Robots, standards and the law: rivalries between private standards and public policymaking for robot governance. *Computer Law & Security Review,* Amsterdã, v. 35, n. 2, p. 129-144, 2019. DOI: 10.1016/j.clsr.2018.12.009.

WITT, Laurel. Preventing the rogue bot journalist: protection from non-human defamation. *Colorado Technology Law Journal*, Boulder, v. 15, n. 2, p. 517-548, 2017.

ZAGO, Mattia; NESPOLI, Pantaleone; PAPAMARTZIVANOS, Dimitrios; PÉREZ, Manuel Gil; MÁRMOL, Félix Gómez; KAMBOURAKIS, Georgios; PÉREZ, Gregorio Martínez. Screening Out Social Bots Interference: Are There Any Silver Bullets? *IEEE Communications Magazine*, New York, v. 57, n. 8, p. 98-104, Aug. 2019. DOI: 10.1109/MCOM.2019.1800520.

Para publicar na revista Brasileira de Políticas Públicas, acesse o endereço eletrônico www.rbpp.uniceub.br
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.