Estado, democracia e tecnologia: conflitos políticos e vulnerabilidade no contexto do *big-data*, das *fake news* e das *shitstorms*

Camilo Onoda Luiz Caldas [I]
http://orcid.org/0000-0003-0591-9473

Pedro Neris Luiz Caldas [II]
http://orcid.org/0000-0002-9170-573X

[I] *Universidade São Judas Tadeu, São Paulo, SP, Brasil.*
Pós-doutor em Democracia e Direitos Humanos.
Professor na Faculdade de Direito da Universidade São Judas Tadeu e da Escola Paulista de Direito.

[II] *Instituto Luiz Gama, São Paulo, SP, Brasil.*
Mestrando no Programa de Pós-graduação em Ciências da Comunicação e Artes da Universidade de São Paulo.

http://dx.doi.org/10.1590/1981-5344/3604

O presente artigo trata dos impactos que as novas tecnologias e alguns de seus potenciais fenômenos correspondentes (big-data, shitstorm, candystorm e fake news) têm sobre os processos eleitorais e, consequentemente, o modelo democrático existente na atualidade. O texto resulta de um estudo interdisciplinar, abrangendo um quadro teórico ligado a ciências como comunicação, tecnologia, direito e política. O objetivo é descrever os fenômenos do big-data, shitstorm, candystorm e fake news, a partir da literatura acadêmica existente, e indicar como todos eles têm uma relevância crescente no desenvolvimento dos processos eleitorais contemporâneos, criando a necessidade de novas iniciativas por parte do Poder Executivo, Legislativo e Judiciário, para evitar consequências deletérias capazes de afetar o equilíbrio das disputas eleitorais e a democracia como um todo.

Palavras-chave: *Estado. Conflito. Tecnologia. Shitstorm. Big-data.*

State, democracy and technology: political conflicts and vulnerability in the context of big-date, fake news and shitstorms

The present article discuss the impacts that the new technologies and some of their corresponding phenomena (big-data, shitstorm, candystorm and fake news) have on the electoral processes and, consequently, on the existing democratic model. This work results from an interdisciplinary study, encompassing a theoretical frame related to sciences such as communication, technology, law and politics. The purpose of this article is to describe the phenomena of big-data, shitstorm, candystorm and fake news from the existing academic literature, and to indicate how they will all have a growing relevance in the development of contemporary electoral processes, creating the need for new initiatives in Executive, Legislative and Judicial levels to avoid deleterious consequences capable of affecting the balance of electoral disputes and democracy as a whole.

Keywords: *State. Conflict. Technology. Shitstorm. Big-data.*

Recebido em 13.07.2018 Aceito em 21.03.2019

1 Introdução

No dia 7 de junho de 2018, um ministro do Tribunal Superior Eleitoral (TSE) aplicou pela primeira vez (TRIBUNAL, 2018c) a Resolução nº 23.551/2017, que dispõe sobre propaganda eleitoral, coibindo a divulgação de notícias falsas (*fake news*) na *Internet*. Em liminar oriunda da representação nº 0600546-70.2018.6.00.0000, o ministro do TSE determinou ao *Facebook* a remoção de conteúdo publicado por perfil anônimo a respeito de pré-candidata à Presidência da República. Em seu voto o ministro substituto Sérgio Banhos afirmou que:

> Na pauta do mundo contemporâneo, há um compromisso inescapável: garantir que o processo eleitoral transcorra de modo regular [...]
>
> Tal desiderato é ainda mais importante nos tempos de hoje, em que as mídias sociais multiplicaram a velocidade da comunicação. Qualquer informação sem fundamento pode ser desastrosa.
>
> O uso da Internet como arma de manipulação do processo eleitoral dá vez à utilização sem limites das chamadas *fake news*.
>
> A prática das *fake news* não é recente. É estratégia eleitoral antiga daqueles que fazem política. Como a recepção de conteúdos pelos seres humanos é seletiva e a desinformação reverbera mais que a verdade [...].
>
> A significativa diferença no mundo contemporâneo é que, com as redes sociais, a disseminação dessa informação maliciosa passou a ser mais rápida, mais fácil, mais barata e em escala exponencial. O uso da Internet como arma de manipulação do processo eleitoral dá vez à utilização sem limites das chamadas *fake news*.
>
> [...]
>
> Notícias distorcidas com forte viés ideológico, trazidas pelas mídias sociais, no mais das vezes, ganham maior atenção que as reportagens realizadas pela imprensa tradicional. As matérias falsas, de cunho sensacionalista, tendem à repercussão fácil, a viralizar, a tornar-se *trend topics* mais rapidamente do que aquelas produzidas por jornalistas zelosos que praticam a checagem dos fatos. [...] (BRASIL, 2018c, p. 115).

A decisão do ministro sintetiza o conteúdo do presente artigo. Suas palavras indicam a atenção crescente do Poder Judiciário em relação às *fake news*, fenômeno que, como veremos, encontra-se associado a vários outros: *big-data*, *shitstorm* e *candystorm*, que são objetos de estudo do presente artigo tanto em seus conceitos, quanto em suas implicações no campo jurídico e político. Tais fenômenos se tornam incontornáveis para se pensar os regimes democráticos e os processos eleitorais na atualidade.

Nesse sentido, a eleição para a presidência dos Estados Unidos da América (EUA) que deu a vitória a Donald Trump se tornou emblemática, pois ficou marcada pelas revelações a respeito da utilização – de maneira irregular – de análise de dados de usuários do *Facebook* para promover estratégias de campanha eleitoral e ataques a adversários, sobretudo, à candidata Hillary Clinton. Esse episódio gerou apreensão e expectativas, especialmente, nos países nos quais existem eleições livres e acentuado uso de *Internet* por parte dos cidadãos. No Brasil, as expectativas não são diferentes, ainda mais se considerarmos alguns indicadores bastante significativos a respeito de usuários de serviços da *Internet*.

Relatórios de 2018 da *We Are Social* e da *Hootsuite* (KEMP, 2018) afirmam que os brasileiros passam, em média, mais de nove horas diárias navegando na *Internet*. Ainda que a taxa de penetração da *Internet* seja de 66% (bem inferior à de outros países mais desenvolvidos), dois dados

são bastante significativos: (i) apenas outros dois países têm uma média superior de uso diário da *Internet* (Tailândia e Filipinas); (ii) com as Filipinas, o Brasil é o único país em que os usuários gastam, em média, mais de três horas e meia por dia em redes sociais (valor duas vezes maior que a média de países como Canadá, Irlanda, Austrália, Espanha, Bélgica, França, Holanda, Alemanha, Coreia do Sul e Japão).

Segundo dados do *Facebook*, cento e dois milhões de brasileiros "compartilham seus momentos no Facebook todos os meses" (FACEBOOK, 2016) e conforme pesquisa *Quartz Media LLC*, voltada para avaliar o nível de entendimento das pessoas sobre a *Internet* no mundo, 55% dos brasileiros concordavam com a afirmação "O Facebook é a *Internet*" (MIRANI, 2015), percepção considerada bastante preocupante a respeito do entendimento que as pessoas têm sobre a rede mundial de computadores. Tal índice foi superior em países como Nigéria (65%), Indonésia (61%) e Índia (58%), mas nos Estados Unidos, por exemplo, apenas 5% dos entrevistados concordaram com a afirmação.

Os dados acima servem para indicar a relevância da *Internet* e das redes sociais, em especial o *Facebook*, na vida dos cidadãos brasileiros (justamente a corporação ligada ao escândalo nas eleições norte-americanas de 2016). Conforme explicaremos ao longo deste artigo, a regulamentação eleitoral atual do Brasil prevê expressamente a possibilidade de impulsionamento de conteúdo patrocinado por candidatos, partidos e coligações (portanto, valoriza plataformas como o *Facebook*), portanto, podemos esperar que a utilização de meios de comunicação intermediados pela *Internet* tenha uma relevância cada vez mais crescente nos processos eleitorais. Ao longo dos tópicos a seguir, trataremos de explicar determinados fenômenos oriundos das inovações tecnológicas, relacionados diretamente com o advento da *Internet*, e como eles podem impactar o campo político-jurídico e, portanto, as próprias bases da organização democrática predominante na atualidade.

Iniciaremos este artigo tratando do *big-data*, para então mostrar sua relação com os fenômenos conhecidos como *shitstorm, candystorm* e *fake news*. Com uma exposição de caráter descritivo, elaborada a partir da literatura especializada sobre o tema, iremos mostrar como tais fenômenos podem interferir e afetar os modelos democráticos e de disputa eleitoral existentes na atualidade, bem como mostraremos como os três poderes do Estado – Executivo, Legislativo e Judiciário – têm iniciado a adoção de medidas – ainda insuficientes – para lidar com tais inovações e seus efeitos.

2 *Big-data*: conceito e características

Nesta segunda década do século XXI, as tecnologias digitais tornaram-se ainda mais ubíquas – especialmente com a notável expansão da *Internet* móvel. Em quaisquer que sejam as esferas de nossa vida – privada ou pública, em ambientes de natureza social ou pessoal – as novas tecnologias se fazem presentes de maneira estrutural, apresentando-se como condições para grande parte das relações dos

sujeitos com o mundo que os rodeia e que os desafia diariamente. O desenvolvimento acelerado das capacidades de processamento e armazenamento de dados vem, progressivamente, expandindo a gama de possibilidades para a aplicação dessas tecnologias nas mais diversas áreas do conhecimento teórico e prático. Entre as transformações de maior relevância desse cenário, privilegiaremos, neste trabalho, a análise do fenômeno do *big-data*, assim como de algumas das consequências nascentes da adoção deste tipo de tecnologia, quando intentada a fins políticos e eleitorais.

A que nos referimos, afinal, quando falamos de *big-data*? Apesar de todo o poder de influência social e econômico que esse fenômeno carrega consigo, o *big*-data é ainda um conceito muito recente e que gera divergências por parte dos autores quando no momento de caracterizá-lo. Pontuaremos aqui, de maneira resumida, duas interpretações para o que pode ser o *big-data*. Há uma primeira visão, de caráter tecnicista, que limita a definição do *big-data* por suas características de funcionamento e aplicação prática. Para esta visão, *big-data* são bancos de dados com capacidades massivas de armazenamento digital, alimentados por quantidades igualmente massivas de dados (SILVEIRA *et al*., 2015). Há, entre estes, os que, para além da capacidade de armazenamento dos bancos de dados, caracterizam o *big-data* segundo cinco qualidades específicas (DEMCHENKO *et al*., 2013), como: volume, velocidade, variedade, veracidade e valor, ou seja, características que extrapolam o tamanho dos bancos de dados e se referem à maneira como estes dados podem ser aplicados em situações de utilização prática visando a um objetivo exterior a eles.

Há uma segunda visão que opta por fazer uma análise de caráter mais teórico, privilegiando as causas e consequências econômicas, sociológicas e filosóficas do advento do *big-data*. Para esta visão, o *big-data* constitui um fenômeno social fruto da mudança de paradigma pela qual o mundo contemporâneo vem passando (VAN DIJCK, 2018). Este novo paradigma, conhecido pela noção de *datificação* (MAYER-SCHONBERGER; CUKIER, 2013), caracteriza-se pelas mudanças graduais e constantes na maneira de absorver e lidar com o mundo, ao relacioná-lo com as quantidades abundantes de dados disponíveis às organizações e pessoas, seja socialmente, seja cientificamente. Em outras palavras, a *datificação*, enquanto paradigma, diz respeito à notável crença na capacidade dos dados para sanar problemas reais que, anteriormente, ou não teriam uma solução aparentemente possível, ou seriam solucionados com eficiência inferior àquela que é possibilitada pelas análises de *big-data*. Portanto, é dentro desta nova conjuntura que o fenômeno do *big-data* constitui-se em seu sentido mais amplo.

São inúmeras as áreas do conhecimento que vêm sendo afetadas pelo patente desenvolvimento das tecnologias da informação e, consequentemente, do *big-data* (BOYD; CRAWFORD, 2012). A coleta massiva de dados dos sujeitos que utilizam a *Internet* diariamente pode representar um grande avanço em alguns aspectos do desenvolvimento das ciências e da economia, mas esse tipo de coleta nem sempre tem um

objetivo majoritariamente deliberado pela sociedade – ainda menos de maneira prévia –, podendo gerar consequências inesperadas e, até mesmo, indesejadas por grande parte da população, como será exemplificado adiante. Segundo van Dijck (2017), desde que Edward Snowden expôs publicamente as políticas de vigilância e coleta de dados continuamente realizados pelo governo norte-americano (GLOBO, 2014), em 2013, há uma luta pública que demanda maior transparência no uso de dados coletados por empresas e agências governamentais. Para além dos setores da economia que são imediatamente influenciados por esses avanços tecnológicos (aqueles que são estruturados por meio da *Internet*, como, por exemplo, as redes sociais digitais e os varejos *on-line*), outras esferas, que são menos óbvias aos olhos do senso comum, recebem iguais – ou maiores – influências do desenvolvimento e adoção desse tipo de tecnologia em seus modelos de funcionamento interno. Algumas dessas esferas, que estão diretamente relacionadas às esferas privada e pública da vida dos cidadãos, como o direito e a política, fazem-nos refletir sobre os traços culturais que essa mudança de paradigma pode vir a alterar, e quais consequências essas mudanças poderiam implicar – ao menos sob um primeiro vislumbre.

Quando se fala de direito e esfera privada, uma questão que é recorrentemente associada à adoção do *big-data*, tanto por parte de empresas, quanto por parte de governos, é a do direito à privacidade dos usuários da *Internet* e, consequentemente, dos cidadãos em geral, ligando-se às discussões sobre os métodos de vigilância possibilitados pelo *big-data* – como aqueles adotados nos departamentos policiais norte-americanos (BRAYNE, 2017). A cada instante, voluntária ou involuntariamente, os usuários de redes sociais e outros produtos da *Internet* (como os produtos do Google) têm quantidades substanciais de informações a seu respeito sendo coletadas (VAIDHYANATHAN, 2011, p. 97-102). Essas informações, que são aglomeradas em formato de dados e metadados, podem ser de diferentes matizes e são utilizadas para diferentes fins, mesmo que sem o conhecimento – e, por vezes, o consentimento – daqueles sujeitos os quais os dados representam. Existem diversas discussões que compõem a temática da privacidade na rede, incluindo uma, de natureza propedêutica, que se propõe a debater o próprio conceito de *privacidade* (VAIDHYANATHAN, 2011) – este, que é frequentemente adotado de forma generalista, sem um compromisso em defini-lo – a fim de melhor compreendê-lo e assegurá-lo. Por outro lado, as organizações que trabalham com análises de *big-data* e dados pessoais dos usuários tentam estar, na maior parte do tempo, um passo à frente de qualquer denúncia que possa vir a ocorrer contra suas instituições, alegando, por vezes (VAIDHYANATHAN, 2011), que o ônus da permissão e entrega dos dados cabe ao usuário, que pode optar, ou não, por utilizar os produtos que possibilitam a coleta, podendo aceitar os termos de uso que lhes são impostos ou rejeitá-los – e, dessa maneira, não utilizar o produto.

3 *Big-data*, política e democracia

É possível ter uma abordagem ainda mais tangível dos problemas acima descritos – envolvendo análises de *big-data* e dados pessoais de usuários – quando os relacionamos com política e eleições populares. As análises de dados já são utilizadas como ferramentas eleitorais há pelo menos seis anos. Bimber (2014) aponta que, já nas eleições presidenciais de 2012, nos Estados Unidos, a campanha eleitoral de Barack Obama – o então presidente norte-americano – "introduziu uma onda de inovação técnica" (BIMBER, 2014, p. 141), adotando, entre outros procedimentos, análises de dados em larga escala. Uma das principais vantagens competitivas que uma organização adquire ao utilizar análises de *big-data*, seja para fins políticos, seja para fins comerciais, é a possibilidade de personalização e difusão de mensagens em termos de indivíduo ou de grupo específico. A partir do momento em que um usuário tem milhares de dados a seu respeito sendo coletados, organizados, relacionados e analisados continuamente, cria-se, então, a oportunidade de lhe transmitir mensagens que sejam mais precisas (BIMBER, 2014) e que abordem temas os quais ele já tenha predisposições a reagir e a interagir. Dessa maneira, organizações como a da campanha de Barack Obama poderiam direcionar mensagens políticas e ideológicas aos usuários de redes sociais, por exemplo, na tentativa de influenciar mudanças de posição e tomadas de decisão – mensagens estas que são, ao mesmo tempo, precisas e inúmeras.

Um exemplo ainda mais recente de como o *big-data* pode ter influência direta sobre a política e, mais especificamente, sobre pleitos democráticos, é o caso da empresa *Cambridge Analytica*, que esteve por trás de campanhas como a do *Brexit*, no Reino Unido, e do atual presidente dos Estados Unidos, Donald Trump. Tratava-se de uma organização privada, de origem inglesa[1], que esteve sob os holofotes nos últimos meses às custas de um escândalo envolvendo a corporação *Facebook* e dados pessoais de milhões de usuários. Segundo matéria publicada pelo jornal *El País* (GUIMÓN, 2018), a *Cambridge Analytica* teria utilizado irregularmente os dados de cerca de oitenta milhões de usuários da rede social *Facebook* para fins eleitorais. A empresa realizava análises de dados provenientes de *big-data* tendo por objetivo obter informações proveitosas para a disputa política, e então as vendia assegurando a seus clientes maior possibilidade de vitória por meio de tais análises. Uma vez feita a coleta e a análise, os resultados eram direcionados aos eleitores em formato de ações via redes sociais, visando obter o voto daqueles que se mostravam mais sujeitos à mudança de opinião – chegava-se ao resultado de quais eram os usuários mais suscetíveis à mudanças fazendo o uso das análises de *big-data*. Devido ao uso não autorizado de dados pessoais dos usuários, tanto a empresa *Cambridge Analytica*, quanto a corporação *Facebook*, responderam à justiça norte-americana por possível influência irregular nas eleições presidenciais de 2016 nos Estados Unidos.

Diante desse contexto, no qual existe um volume de informações sendo armazenado e com potencial de ser utilizado com finalidades

1 Após o escândalo envolvendo os dados de usuários do *Facebook*, a empresa encerrou suas atividades.

políticas, sobretudo em períodos eleitorais, podemos destacar que instituições do Estado brasileiro (polícia, Ministério Público e Poder Judiciário) e sua legislação precisam se adequar para lidar com as inovações decorrentes do advento do *big-data*.

Nas últimas décadas, as instituições brasileiras voltadas à repressão de crimes têm dado mostras de incapacidade em operar adequadamente dentro de um cenário permeado por inovações tecnológicas que envolvem, dentre outras novidades, sistemas eletrônicos de armazenamento e transmissão de informações. As decisões do Poder Judiciário que levaram a episódios de suspensão temporária de funcionamento do conhecido aplicativo de comunicação "WhatsApp" ilustram isso (GLOBO, 2018). Nas ocasiões, as iniciativas dos juízes prejudicaram milhões de usuários sem que a finalidade das decisões judiciais fosse satisfatoriamente alcançada (obtenção de informações sobre conteúdo de mensagens enviadas, que a empresa afirmou não ser tecnologicamente possível disponibilizar). Tais episódios ilustram como uma nova realidade demanda, por parte do Poder Judiciário, novos conhecimentos e estratégias.

Ainda nesse sentido, temos os constantes relatos a respeito da falta de estrutura estatal adequada para atuar dentro de um cenário de crescimento das tecnologias digitais. Levantamento da *SaferNet Brasil*, associação civil focada na promoção e defesa dos Direitos Humanos na *Internet* no Brasil, aponta que em 2018 apenas catorze estados brasileiros, além do Distrito Federal, contavam com uma Delegacia especializada em crimes "cibernéticos" (CRIMES NA WEB, 2018). Tendo em vista que, em 2017, o Brasil foi considerado o segundo país que mais perdeu dinheiro com crimes "cibernéticos" e que existe a tendência de que a *Internet* seja vetor de práticas criminais (DFNDR, 2018a) (inclusive no âmbito eleitoral), a ausência de órgãos estatais de repressão especializados nesse ambiente é um indicador bastante preocupante.

A legislação brasileira, mesmo após passar por recentes reformas, que abrangem desde a criação do *Marco Civil* (BRASIL, 2014) *da Internet* até modificações nas regras para disputa eleitoral em 2018, ainda não se mostra suficiente para lidar com todas as questões relacionadas ao *big-data*. Vejamos que, a princípio, a atual legislação estabelece (BRASIL, 2014) que tanto o armazenamento de dados do usuário quanto seu fornecimento para terceiros ficam condicionados ao livre consentimento:

> Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> [...]
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

> [...]
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; (BRASIL, 2014)

Não iremos considerar aqui o fato de que termos de consentimento são comumente aceitos pelos usuários sem um mínimo de análise crítica. Também desconsideraremos o fato de que muitos *sites* na *Internet*, *softwares* e aplicativos condicionam sua utilização à aceitação de seus termos que incluem permissão de uso, armazenamento e tratamento de dados pessoais de modo (quase) irrestrito. Para o propósito deste artigo, destacamos apenas que não há sequer, por parte das instituições de Estado e dos cidadãos em geral, conhecimento de qual é a dimensão dos dados já coletados e de como os dados armazenados nos últimos anos estão (e estarão) sendo utilizados por sujeitos, instituições e partidos políticos dentro do espaço de embate político e, principalmente, de disputa eleitoral.

Por um lado, pode-se argumentar que os mecanismos para restringir a coleta e a utilização de dados acabarão por se mostrar inócuos, uma vez que a natureza do sistema e parte de sua sobrevivência econômica consiste justamente em absorver tais informações para os mais diferentes propósitos. Por outro lado, existe a demanda por transparência acerca do que constitui o *big-data* e para quais finalidades ele está sendo utilizado. Nesse cenário, soma-se outro problema. A coleta de tais dados, ainda que consentida, é praticamente "involuntária" e o usuário não tem dimensão do quanto é coletado e de como esses dados estão circulando na *Internet* e sendo apropriados por terceiros. Portanto, é preciso evitar que medidas para dar transparência ao *big-data* acabem implicando na violação do direito constitucional à intimidade (Art. 5º, inciso X da Constituição Federal) (BRASIL, 1988). Apenas a título de exemplo, podemos citar que estudos a respeito do perfil e comportamento dos usuários nas redes sociais permitem predizer com alto grau de probabilidade, por exemplo, características como raça e orientação sexual (DUSSEL, 2018), ou ainda, as preferências políticas do cidadão, mesmo se o usuário não as explicite em tais ambientes por meio de palavras ou "postagens", apenas com base naquilo que o sujeito acessa, "curte" e compartilha em redes sociais, por exemplo.

Nesse ponto, podemos traçar um paralelo com uma situação pretérita que demandou reações do Legislativo e do Judiciário. A legislação brasileira, nas últimas décadas, tratou de regulamentar as

pesquisas eleitorais, criando obrigações ligadas ao seu registro como forma de divulgação das informações, transparência na metodologia, etc. Em suma, percebendo a relevância das pesquisas (e como elas podiam influenciar os cidadãos, por exemplo, criando ondas de voto útil), as instituições estatais reagiram.

O cenário do *big-data*, contudo, se revela muito mais complexo. Nesse contexto, os institutos podem se apoderar de informações sem que os "entrevistados" – os fornecedores de informação – sequer tenham conhecimento que fazem parte de uma amostra. Evidentemente, pode-se argumentar que as regulamentações estatais sobre pesquisas eleitorais estabelecem regras diferentes para aquelas que são usadas internamente e para aquelas que são divulgadas publicamente. No entanto, devemos considerar que o *big-data* cria uma dinâmica totalmente distinta das tradicionais pesquisas, pois, como dito, o cidadão colabora involuntariamente, sem sequer compreender de que modo e em que medida está alimentando as estratégias de *marketing* político e pautando os discursos políticos com os quais irá se defrontar durante o processo eleitoral.

Outro ponto relevante diz respeito ao nível de acesso ao *big-data* que cada candidato ou partido terá. Considerando que obter informação qualificada é um diferencial significativo e que o *big-data* será uma fonte cada vez mais relevante, evidentemente candidatos terão parte de sua força política determinada pela quantidade e qualidade no acesso e interpretação das informações armazenadas. Consequentemente, quem detiver maior poder econômico, tem a tendência de ter vantagens nessa disputa. É evidente que o argumento da influência do poder econômico poderia ser aplicado a qualquer instrumento existente (não apenas ao *big-data*), no entanto, é necessário considerar duas particularidades a seguir explicadas.

Em primeiro lugar, é preciso considerar que não existem sinais externos que permitam mensurar em que medida um candidato faz uso do *big-data*. A comunicação tradicionalmente utilizada no campo da disputa eleitoral se realizava por meios corpóreos (camisetas, adesivos, faixas, cartazes, santinhos, etc.), portanto, havia sinais exteriores que permitiam ter alguma ideia da dimensão do investimento financeiro realizado. Mesmo após as reformas eleitorais que restringiram tais instrumentos de propaganda, as estruturas de campanha de um candidato eram indicadores visíveis do poder econômico do partido ou candidato, pois tinham uma materialidade evidente (número de cabos eleitorais, deslocamento em aviões particulares, estrutura física dos comícios, qualidade da produção das propagandas eleitorais televisivas, etc.). No caso do uso do *big-data*, os cidadãos não têm ideia da grandeza de valor investido nesse campo, especialmente se o modo de difusão ocorrer em redes sociais da *Internet* (como *Facebook*[2] e *Twitter*, por exemplo) ou por

2 No caso de conteúdo patrocinado, há uma evidência de investimento, mas fora desse contexto, a percepção de investimento é muito mais difícil. Mesmo no caso de conteúdo pago, o cidadão tem ideia de quanto foi investido na divulgação, mas não de quanto se despendeu para concluir que aquela postagem é a mais adequada para aquele público.

meio de aplicativos de comunicação (como *WhatsApp* e *Telegram*, por exemplo). Ainda que a legislação determine a declaração de gastos de campanha, inclusive os de impulsionamento, todo investimento em *big-data* não fica evidenciado aos cidadãos o quanto contribuíram com dados e, como dito, isso pode ter ocorrido dentro de uma ordem de grandeza muito substancial.

Em segundo lugar, é necessário considerar que o *big-data* não é um banco de dados público, em relação ao qual, todos os agentes privados têm igual acesso e contribuem igualmente para sua constituição. A própria formação do *big-data* pode sofrer interferência de seus participantes, especialmente por aqueles que entendem seu funcionamento, no caso, as grandes corporações. Isso significa que mesmo um partido ou candidato com poder econômico para acessar adequadamente o *big-data*, pode não contar com a contribuição das corporações que são responsáveis pela constituição do *big*-data, caso haja uma divergência de interesses entre eles. Podemos supor os problemas que uma força política teria caso tivesse propostas que contrariam interesses de gigantes como *Google* e *Facebook*. Tais corporações seguramente poderiam agir de modo não colaborativo. Tal fenômeno faz com que determinados grupos políticos, mesmo reunindo recursos financeiros para garantir seu acesso à informação, possam ser prejudicados porque, não obstante terem recursos, estão desprovidos de uma plataforma política que interesse aos grupos econômicos que têm poder de influência sobre o *big-data*. Temos, portanto, aqui, todo um universo novo de problemáticas no campo ético, político e jurídico.

Uma vez delineadas tais questões, veremos que o *big-data*, uma realidade incontornável no século XXI, se conjuga com outros fenômenos crescentes no cenário político contemporâneo, dentre eles, *shitstorm*, *candystorm* e *fake news.*

4 *Shitstorm*, *candystorm* e *fake news*: conceito e características

Como foi explanado, anteriormente, diversas informações úteis de usuários de redes sociais e *Internet* em geral circulam pelos bancos de dados de organizações comerciais e políticas, e são usadas para fins diversos, incluindo causas eleitorais. Mas como, precisamente, é possível transformar rastros digitais e informações básicas dos usuários em movimentações reais para objetivos em escala massiva? Dentre as possíveis ações políticas e ideológicas que emergem da adoção de análises de *big-data* enquanto instrumentos de cunho eleitoral, abordaremos aqui, três fenômenos que se mostram imprescindíveis à discussão: as chamadas *shitstorms*, as *candystorms* e as *fake news*. Abordaremos especificamente estas três, dada a relevância e a atualidade dos conceitos que as envolvem, seja em esferas acadêmicas, seja em esferas midiáticas e jurídicas. Para, além disso, os caracteres de novidade de tais fenômenos refletem, também, a escassez de instrumentos jurídicos (e mesmo

tecnológicos) para lidar com as consequências geradas por eles, especialmente no âmbito político e eleitoral, como será mostrado adiante.

Antes de defini-los, entretanto, faz-se necessária a colocação de duas observações – que serão ilustradas ao decorrer desta seção – acerca do uso de tais fenômenos enquanto instrumentos pragmáticos. A primeira das observações diz respeito a uma qualidade que é marca comum entre os três (especialmente entre as *shitstorms* e as *candystorms*): a instrumentalização contingente desses acontecimentos, para fins políticos ou não. Ou seja, esses conceitos referem-se a eventos que, na prática, podem ser realizados de maneira premeditada (propositalmente; visando a um objetivo), ou podem, simplesmente, ser estimulados organicamente, enquanto efeitos de um acontecimento anterior que sirva de gatilho para reações de massa em cadeia. A segunda observação diz respeito à utilização específica de análises de *big-data* para produzir fenômenos como *shitstorms*, *candystorms* e *fake news*. Qualquer um destes eventos que tenha sido gerado e estimulado artificialmente não carrega consigo a certeza de um *big-data* na sua fonte – como em casos anteriores ao advento da *Internet*. Ou seja, é possível que se produzam fenômenos como estes sem, necessariamente, ter-se utilizado de análises de *big-data* para produzi-los. Neste trabalho, entretanto, abordaremos esta temática, tendo em vista as suas utilizações enquanto instrumentos políticos e eleitorais, além de terem sido possibilitados por análises de *big-data* prévias.

O primeiro dos três conceitos a ser definido é o de *shitstorm*. Este termo, de origem lexical inglesa, foi incluído no dicionário alemão Duden em 2013 e, à época, o acontecimento causou grande repercussão, especialmente porque este anglicanismo tem uma denotação vulgar em sua língua de origem. Enquanto o dicionário Oxford (2018, *on-line*), de língua inglesa, define a palavra *shitstorm* por "uma situação marcada por controvérsia violenta" (tradução nossa), o Duden (2018, *on-line*) a define de maneira distinta: "tempestade de indignação em um meio de comunicação da *Internet*, que anda de mãos dadas com observações ofensivas" (tradução nossa). Adotando-se a definição proposta pelo dicionário alemão, portanto, temos que, para além do conteúdo essencialmente negativo do termo, as *shitstorms* são, ainda, fenômenos inerentes ao ambiente da *Internet*. São reações verbais difamatórias em massa contra pessoas ou instituições, que se caracterizam pelo uso de grande carga emocional em detrimento de embates argumentativos. Para Garcia (2015, p. 185), "a definição de '*shitstorm*' não contém qualquer dimensão de crítica ou debate coletivo, mas a banalização do insulto em bloco na *Internet* e manifestações de ódio coletivo [...]". Soma-se a isto a combinação entre encurtamento de distâncias e instantaneidade de reações – que é primorosamente possibilitada pelas tecnologias digitais e pela internet móvel – e que age como um catalisador fundamental para que as *shitstorms* e seus efeitos possam ser absolutamente implacáveis e, em alguns casos, irreversíveis.

O conceito de *candystorm*, por sua vez, deve ser compreendido no sentido contrário ao de *shitstorm* – especialmente no que se refere ao

conteúdo valorativo de cada um dos respectivos fenômenos que os acompanham. "O termo *candystorm* foi usado pela primeira vez na Alemanha, em 12 de novembro de 2012, pelo político alemão Volker Beck em uma postagem na rede social *Twitter*", e significa "uma onda de popularidade e simpatia nas redes sociais" (MARKETING, 2016). Enquanto as *shitstorms* se referem às tempestades de reações negativas propagadas pela *Internet*, as *candystorms* têm a característica peculiar de atingir a imagem do seu alvo com inúmeros julgamentos positivos. As características formais deste fenômeno carregam consigo diversas semelhanças com aquele que foi explicado anteriormente: as reações de massa em cadeia, o aspecto emocional em detrimento do argumentativo, a rápida disseminação das informações envolvendo o evento em pauta e, por último, mas não menos importante, a inerência ao ambiente da *Internet*. Trata-se de um conceito menos adotado quando comparado ao de *shitstorm*, especialmente em produções acadêmicas. Por serem antônimos, um mesmo fenômeno prático pode ser considerado uma *shitstorm* diante das reações de um determinado grupo e, por reações contrárias, uma *candystorm*.

A fim de ilustrar esses dois conceitos, serão tomados como exemplo, aqui, dois casos que ocorreram nos últimos quatro anos e que foram marcados por evidenciarem o notável poder dos usuários das redes sociais para julgar e condenar determinada conduta. Segundo uma reportagem publicada pelo portal de notícias *El País*, Justine Sacco, diretora sênior de comunicações corporativas na IAC/InterActiveCorp, teve sua carreira arruinada por conta de uma mensagem infeliz, carregada de preconceitos, que postou em seu perfil da rede social *Twitter*: "A caminho da África. Espero não pegar Aids. É brincadeira. Sou branca!" (SALAS, 2015). Quando publicou o pequeno texto, a jovem embarcava em um avião rumo à África do Sul, onde iria passar o Natal. Ao reativar seu *smartphone*, chegando ao seu destino, Justine Sacco se deparou com milhares de respostas coléricas destinadas a seu texto racista, incluindo ameaças à sua pessoa. A empresa para a qual trabalhava a demitiu imediatamente. Javier Salas, o jornalista que assinou a reportagem do *El País*, apontou, ainda, para a total impossibilidade de resposta que a jovem teve após a situação. Pode-se observar, nesse acontecimento, o vigor e a eficiência de uma *shitstorm*.

Quatro anos após o caso de Justine Sacco, a França conhece e reconhece um novo herói nacional por meio de um vídeo amador. Segundo a notícia publicada pelo jornal *Folha de S. Paulo* (FOLHA, 2018), Mamoudou Gassama, um imigrante de vinte e dois anos oriundo da República do Mali, salvou uma criança de apenas quatro anos que se encontrava pendurada para fora de um apartamento no quarto andar de um prédio da cidade de Paris. O resgate executado por Gassama tomou grandes proporções por ter sido filmado e, principalmente, por ter sido compartilhado nas redes sociais *on-line*. Em menos de um dia, o vídeo do jovem imigrante escalando os quatro andares do prédio sem nenhum equipamento de segurança rodou as redes do mundo e já contava com milhões de visualizações. As exaltações e elogios à figura de Gassama

foram tantas que, dias após o ocorrido, o presidente francês Emannuel Macron recebeu o imigrante pessoalmente para agradecer-lhe e propor a ele a nacionalidade francesa. Tem-se, portanto, neste caso, um exemplo de como se dá uma *candystorm* na prática.

Por fim, conceituaremos as chamadas *fake news* (*notícias falsas*, em uma tradução livre). Para este termo, adotaremos uma definição específica, a qual, já de antemão, nos dá a garantia de não incorrer no erro de confundir notícias falsas não intencionais com o tipo de *fake news* que pretendemos abordar neste trabalho. Segundo a conceituação proposta por Allcott e Gentzkow (2017), podemos concluir que as *fake news* são notícias comprovadamente falsas, comunicadas com a possibilidade de enganar os receptores de maneiras diversas. Ou seja, a utilização de *fake news* será, dentro desta definição específica, sempre um instrumento. Pensando nesta questão, o jornalista Lins da Silva propôs a tradução do termo em português como "notícias fraudulentas", almejando, justamente, descolar do termo os casos de notícias falsas não intencionais (BUCCI, 2018, p. 22). Ainda que em alguns casos esse fato não seja explícito, as *fake news* são produzidas para fins diversos. É importante, neste momento, destacar a palavra "produzidas". Diferente das notícias falsas não intencionais, produzem-se *fake* news intentando desarmonia e conflitos entre pessoas e grupos. Ademais, uma vez que esse tipo de notícia é disseminado, é pouco provável que se reverta todo dano causado.

Não é difícil deduzir que as *fake news* podem, inclusive, ser usadas para provocar *shitstorms* e *candystorms* de maneira premeditada, visando prejudicar a imagem de uma pessoa ou instituição sem que a vítima endereçada tenha, sequer, ciência do ocorrido ou de sua precedência. No entanto, existem pelo menos três fatores que imediatamente prejudicam o combate à disseminação de *fake news*. O primeiro deles é a dificuldade de identificá-las, tendo em vista que muitas delas não são dadas como óbvias, pois há uma ação deliberada para ocultar as partes falsas da notícia por meio de diferentes técnicas (confusão de datas; notícias parcialmente verdadeiras; nomes de pessoas e instituições trocados; caracterização ou denominação semelhante a portais de notícias com credibilidade, etc.). O segundo diz respeito à dificuldade de se chegar à fonte propagadora original, que frequentemente se esconde por trás de identidades falsas e computadores protegidos. O terceiro e último ponto diz respeito aos meios pelos quais as *fake news* são propagadas. Como se não bastasse a volubilidade provocada pelas redes sociais no que se refere à propagação de notícias, um estudo realizado Monitor do Debate Político no Meio Digital da USP (MONITOR, 2018), as *fake news* começam a ser difundidas principalmente no aplicativo de troca de mensagens instantâneas *WhatsApp*, para só então se espalharem por redes sociais como *Facebook* e *Twitter*, o que dificulta ainda mais a busca pela fonte original.

Tendo em vista o conteúdo explanado anteriormente, relacionaremos, neste momento, os fenômenos da *shitstorm*, *candystorm* e das *fake news* às análises de *big-data* segundo dois aspectos relevantes.

O primeiro aspecto da relação central entre estes conceitos se refere à inerência destes ao ambiente digital *on-line*. Apesar de serem fenômenos disseminávéis independentemente de ações realizadas através da *Internet*, a relação propiciada pelo ambiente *on-line*, especialmente por meio das redes sociais, é relevante na medida em que intensifica a capacidade de coleta e análises de *big-data*. O segundo e, talvez, mais importante aspecto relacionável diz respeito à possibilidade de direcionar mensagens de cunho político e ideológico por do meio do uso de *big-data*. Uma vez que são identificados os usuários mais suscetíveis a reagir de determinada maneira a tipos específicos de notícias ou informações, cria-se a possibilidade do direcionamento de *fake news* a fim de fomentar *shitstorms* ou *candystorms*. Esse direcionamento é granulado e se estende ao nível individual ou de grupos particulares, gerando resultados com alto grau de precisão e penetração. Finalmente, soma-se a isso a possível utilização de dados de usuários para fins políticos e eleitorais sem que estes tenham ciência dos objetivos que concernem às respectivas coletas.

5 *Shitstorm*, *candystorm* e *fake news*: impactos no âmbito eleitoral e contramedidas

Do quarto trimestre de 2017 para o primeiro de 2018, o acesso a notícias falsas aumentou 11,97% no Brasil, atingindo um patamar de 2,9 milhões de acessos, segundo o *Relatório da Segurança Digital no Brasil* (DFNDR, 2018b). O mesmo relatório indica que há uma tendência de crescimento em ano eleitoral, uma vez que as experiências em outros países, notadamente os Estados Unidos da América, já evidenciaram ocorrências nesse sentido.

A proliferação de notícias falsas, contudo, não tem apenas objetivos puramente políticos. Estudos demonstram que informações falsas têm maior probabilidade de "viralizar" – de se proliferarem rapidamente – do que notícias verdadeiras – segundo estimativas, 70% mais chances (VOSOUGHI; ROY; ARAL, 2018). Portanto, notícias falsas não são difundidas apenas porque podem provocar efeitos eleitorais. Lucrar com a difusão de informações inverídicas é um elemento que mobiliza núcleos irradiadores de *fake news.* Esse cenário se torna ainda mais crítico considerando que as duas principais corporações do mundo digital na atualidade – *Facebook* e *Google* – têm modelos de monetização que estimulam a difusão de notícias falsas, uma vez que parte das receitas depende da publicidade e, consequentemente, de um número crescente de acessos, justamente o que as *fake news* garantem com maior eficácia. Estudo realizado pela Universidade de Stanford mostra que a relação do *Facebook* com as *fake news* não é produto de acaso:

> A questão final dentro deste tópico é como o próprio modelo de lucro do *Facebook* se cruza com o problema das *fake news*. Os *Knight Fellows* acreditam que o *Facebook* recebe mais dinheiro quando os URLs obtêm mais cliques, e os artigos destinados a serem provocadores, sensacionalistas ou indutores de emoções tendem a gerar mais receita. Eles veem esse modelo financeiro em

> oposição ao objetivo de promover o jornalismo sério e verdadeiro, e o compartilhamento de informações na plataforma. (FEINGOLD et al., 2018 – Tradução nossa)

O problema das *fake news* soma-se ao do *shitstorm* e do *candystorm*, uma vez que determinados partidos e candidatos, utilizando-se das informações obtidas a partir do *big-data*, aumentam seu poder de interferir no processo eleitoral por meio da divulgação de informações falsas que possam destruir (*shitstorm*) ou construir (*candystorm*) a reputação de determinado candidato ou legenda. Dois pontos dentro desse contexto merecem ser destacados. Primeiro, o hiato existente entre a capacidade de propagação e de contenção. O segundo é o da existência dos mencionados "robôs digitais" (*bots*), com a finalidade de difundir conteúdos em redes sociais.

A questão do hiato entre a capacidade de propagação e de contenção se torna mais sensível, considerando que ambos os fenômenos apresentam uma velocidade de propagação muito rápida e, portanto, podem ser deflagrados às vésperas do dia da eleição, sem que as instituições de Estado tenham mecanismos para impedir uma tormenta digital e seus efeitos. O Poder Judiciário brasileiro tem demonstrado que essa questão entrou definitivamente na pauta de discussão e estratégias, desenvolvendo inclusive um seminário específico sobre o tema em parceria com instituições europeias (TRIBUNAL, 2018b). Justamente por não dispor de ferramentas capazes de interromper rapidamente tais tempestades, surgem manifestações públicas de membros do Poder Judiciário de que *fake news* em massa podem levar à anulação das eleições (RAMALHO, 2018), com base no artigo 222 do Código Eleitoral brasileiro[3]. Em suma, trata-se de admitir que só é possível lidar com os efeitos da tormenta, não com o curso de sua ocorrência.

Os robôs utilizados na *Internet*, por sua vez, têm diversas funções e não são necessariamente elementos nocivos ao ambiente digital. No nosso caso interessa destacar aqueles que são utilizados nas redes sociais da *Internet* com objetivo de propagar informações falsas, maliciosas, gerar debates artificialmente, polemizar artificialmente questões com outros usuários, etc. Nesse sentido, surgem estudos para mensurar o impacto desses instrumentos:

> O estudo feito pela FGV/DAPP aponta que esse tipo de conta chegou a ser responsável por mais de 10% das interações no Twitter nas eleições presidenciais de 2014. Durante protestos pelo Impeachment, essas interações provocadas por robôs representaram mais de 20% do debate entre apoiadores de Dilma Rousseff, que usavam significativamente esse tipo de mecanismo. Um outro exemplo analisado mostra que quase 20% das interações no debate entre os usuários favoráveis a Aécio Neves no segundo turno das eleições de 2014 foi motivado por robôs.

3 "Art. 222. É também anulável a votação, quando viciada de falsidade, fraude, coação, uso de meios de que trata o Art. 237, ou emprego de processo de propaganda ou captação de sufrágios vedados por lei" (BRASIL, 1965).

> Nas discussões políticas, os robôs têm sido usados por todo o espectro partidário não apenas para conquistar seguidores, mas também para conduzir ataques a opositores e forjar discussões artificiais. Eles manipulam debates, criam e disseminam notícias falsas e influenciam a opinião pública postando e replicando mensagens em larga escala (RUEDIGER *et al*, 2017).

O mesmo estudo destaca que uma das funções dos robôs é justamente fazer ataques em massa, sufocando o debate natural sobre um tema. Antevendo tal questão, o próprio Tribunal Superior Eleitoral também já demonstrou iniciativas no sentido de conter esse tipo de estratégia (TRIBUNAL, 2018a). Portanto, podemos indicar que o processo eleitoral no Brasil terá a presença de robôs como instrumentos para ampliar *shitstorms* e *candystorms* em relação a determinados candidatos, partidos ou ideias políticas.

As inovações introduzidas pela a Lei Federal nº 13.488/2017, conhecida como minirreforma eleitoral de 2017, que modificou o Código Eleitoral e a Lei das Eleições, trouxe algumas inovações significativas no que diz respeito à utilização da *Internet* no processo de disputa eleitoral. Alguns artigos merecem destaque:

> Art. 57-B. A propaganda eleitoral na internet poderá ser realizada nas seguintes formas: (Incluído pela Lei nº 12.034, de 2009) (Vide Lei nº 12.034, de 2009)
>
> [...]
>
> IV - por meio de blogs, redes sociais, sítios de mensagens instantâneas e aplicações de internet assemelhadas cujo conteúdo seja gerado ou editado por: (Redação dada pela Lei nº 13.488, de 2017)
>
> a) candidatos, partidos ou coligações; ou (Incluído pela Lei nº 13.488, de 2017)
>
> b) qualquer pessoa natural, desde que não contrate impulsionamento de conteúdos. (Incluído pela Lei nº 13.488, de 2017)
>
> [...]
>
> § 2o Não é admitida a veiculação de conteúdos de cunho eleitoral mediante cadastro de usuário de aplicação de internet com a intenção de falsear identidade. (Incluído pela Lei nº 13.488, de 2017)
>
> Art. 57-C. É vedada a **veiculação de qualquer tipo de propaganda eleitoral paga na internet, excetuado o impulsionamento** de conteúdos, desde que identificado de forma inequívoca como tal e contratado exclusivamente por partidos, coligações e candidatos e seus representantes. (Redação dada pela Lei nº 13.488, de 2017)
>
> [...]
>
> § 3º O impulsionamento de que trata o *caput* deste artigo deverá ser contratado diretamente com provedor da aplicação de internet com

> sede e foro no País, ou de sua filial, sucursal, escritório, estabelecimento ou representante legalmente estabelecido no País e apenas com o fim de promover ou beneficiar candidatos ou suas agremiações. (Incluído pela Lei nº 13.488, de 2017)
>
> (BRASIL, 2017, Grifo nosso).

Os artigos acima mencionados versam sobre duas questões importantes. A primeira, a autorização para utilização de impulsionamento patrocinado de conteúdo na *Internet*, sem restrições para sua utilização nas redes sociais. A segunda diz respeito à proibição da utilização de perfis falsos, portanto, igualmente de robôs, para promover interações nas redes sociais e promover ou sufocar artificialmente os debates no ambiente da *Internet*. De um lado, a lei, ao tentar coibir a utilização de robôs, cria uma contratendência na ocorrência de *shitstorms* e *candystorms*. De outro lado, ao permitir o impulsionamento pago, aumenta a possibilidade de ocorrências destes fenômenos, que, como dito, podem se combinar com a utilização das informações oriundas do *big-data* (a única restrição ao impulsionamento pago se dirige às pessoas físicas, limitando tal instrumento a candidatos, partidos ou coligações). Nesse sentido, especialistas da área de direito eleitoral avaliam:

> Com o impulsionamento pago, abrem-se brechas para os ilícitos de abuso de poder econômico, abuso de poder político, abuso dos meios de comunicação social, propaganda vedada (realizada por igrejas, sindicatos e pessoas jurídicas em geral), *fake news*, entre outros possíveis ilícitos. Alguns desses ilícitos podem levar à cassação do registro de candidatura, diploma (caso eleito) e perda do mandato. (ALMEIDA; LOURA JUNIOR, 2018)

O texto original da lei continha medidas mais efetivas para inibição de *shitstorms* e *candystorms* por meio de *fake news* durante o processo eleitoral. Todavia, o principal dispositivo existente nesse sentido foi objeto de veto presidencial, trata-se do §6º do art. 57-B, que previa originalmente o seguinte:

> "§ 6º A denúncia de discurso de ódio, **disseminação de informações falsas** ou ofensa em desfavor de partido ou candidato, feita pelo usuário de aplicativo ou rede social na internet, por meio do canal disponibilizado para esse fim no próprio provedor, implicará suspensão, em no máximo vinte e quatro horas, da publicação denunciada até que o provedor certifique-se da identificação pessoal do usuário que a publicou, sem fornecimento de qualquer dado do denunciado ao denunciante, salvo por ordem judicial. (BRASIL, 2017, Grifo nosso).

O dispositivo acima tinha potencial inibitório para propagação de *fake news* e consequentemente para ocorrência de *shitstorms* e *candystorms*, fenômenos que, como dissemos, tendem a ocorrer combinados com as informações oriundas do *big-data*, justamente porque permitem que sejam identificados pontos vulneráveis ou positivos que podem ser explorados mediante impulsionamento de conteúdos. Há, no entanto, uma justificativa para o veto, pois, existe o fundado receio de

que uma legislação de repressão às *fake news* possa gerar cerceamento à liberdade de expressão especialmente dentro de um ambiente no qual o ativismo Judiciário no campo político se intensifica e encontra-se permeado por intensa polarização política, no qual as paixões políticas fazem com que a fronteira entre a verdade, do ponto objetivo e subjetivo, se esmaeça.

O Art. 25 da Resolução nº 23.551/2017 do Tribunal Superior Eleitoral (TSE), redigido com base no art. 57-D da Lei Federal nº 13.488/2017, contém dispositivo para tentar evitar a propagação de *fake news*. No entanto, a celeridade da justiça provavelmente não será suficiente para impedir a ocorrência de *shitstorms* e *candystorms*, justamente porque sua característica é a velocidade na propagação. Baseado na experiência de que a mera positivação jurídica de sanções, mesmo penais, não é medida suficiente inibitória para coibir condutas ilícitas, uma das saídas seria justamente a de aperfeiçoar mecanismos de controle ao acesso dos dados de usuários, justamente porque ataques políticos não são feitos de modo aleatório, eles dependem de um direcionamento de conteúdo adequado ao perfil de um público. Nesse sentido, a União Europeia criou em 25 de maio de 2018 o Regulamento Geral sobre a Proteção de Dados (COMISSÃO EUROPEIA, 2018) após estudos que indicavam que a propagação de *fake news* era feita a partir da análise de dados de usuários (MARTENS et al., 2018). Caminhando nesse sentido, em 11 de junho de 2018, o Conselho Nacional de Direitos Humanos aprovou a Recomendação nº 04, de 11 de junho de 2018, que trata "sobre medidas de combate às *fake news* (notícias falsas) e a garantia do direito à liberdade de expressão" (BRASIL, 2018b), que recomenda a aprovação de Projeto de Lei voltado para proteção de dados pessoais (BRASIL, 2018a), considerando que "a produção e direcionamento das chamadas *fake news* hoje estão diretamente relacionadas com a coleta e tratamento massivos e indiscriminados de dados pessoais" (BRASIL, 2018b).

6 Conclusão

Sem dúvida, as inovações tecnológicas têm trazido novas questões para serem estudadas por cientistas de diversas áreas, inclusive, cientistas políticos, juristas e sociólogos. No caso específico do fenômeno *big-data* é preciso entender como ele pode relacionar-se com a difusão de *fake news* criando ações para interferir de modo ilegal e antiético, mas eficiente, no processo eleitoral, gerando, inclusive, *shitstorms* contra adversários políticos e *candystorms* a favor de aliados.

Especialmente em relação aos fenômenos de *shitstorms* e *candystorms*, não existem meios tecnológicos suficientes, tampouco instrumentos jurídicos, que sejam capazes de neutralizar totalmente o curso da ocorrência de tais fenômenos sem que sejam adotadas medidas extremamente radicais e agressivas e, portanto, indesejáveis, capazes de resultar, por exemplo, na paralisação das atividades em redes sociais, aplicativos de comunicação ou da *Internet* como um todo. Tornar

inoperante tais espaços de comunicação em tamanha escala acabaria por ser mais contraproducente à democracia do que a própria ocorrência de um episódio de *shitstorm* ou *candystorm*. A ausência de mecanismos de prevenção de *shitstorms* e *candystorms*, bem como de meios capazes de interromper de modo eficaz sua ocorrência, significa que estamos dentro de um contexto no qual episódios dessa natureza podem desequilibrar significativamente o processo eleitoral, produzindo o favorecimento antiético e ilegal de candidaturas e partidos específicos em detrimento de outros.

As dificuldades para lidar com fenômenos de *shitstorm* e *candystorm*, que se propagam em poucas horas, mas reverberam durante dias ou semanas, demandam que o Poder Judiciário, mais do que nunca, desenvolva meios para identificar de modo rápido e eficaz tais ocorrências, reagindo com celeridade no sentido de evitar sua contínua propagação e a perpetuação de seus efeitos.

Por fim, considerando que os fenômenos *shitstorms* e *candystorms* podem produzir desequilíbrios capazes de, no limite, levar à anulação de eleições, estamos diante da possibilidade de que tais ocorrências interfiram diretamente no modelo democrático estabelecido na atualidade. Nesse sentido, além de iniciativas oriundas do Poder Legislativo e do Executivo, o Poder Judiciário precisa aprimorar suas ferramentas para identificar quais os agentes responsáveis por determinados episódios, bem como aperfeiçoar os instrumentos utilizados para mensurar a extensão de danos provocados e o impacto para o equilíbrio da disputa eleitoral. Tais desafios são incontornáveis para que os processos eleitorais e, portanto, o modelo de democracia existente consiga subsistir, evitando, assim, um aumento da já existente crise de legitimidade que perpassa o ambiente político nos tempos presentes.

Referências

ALLCOTT, H.; GENTZKOW, M. Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, 31(2): 211-36, 2017. Disponível em: https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211. Acesso em: 19 jun. 2018.

ALMEIDA, R.; LOURA JUNIOR, J. Campanhas políticas devem ter as redes sociais como principal arena. *Consultor Jurídico*, 16 mai. 2018. Disponível em: https://www.conjur.com.br/2018-mai-16/opiniao-disputa-eleitoral-redes-sociais-principal-arena. Acesso em: 01 jul. 2018.

BIMBER, B. Digital Media in the Obama Campaigns of 2008 and 2012: Adaptation to the Personalized Political Communication Environment. *Journal of Information Technology & Politics*, 2014. Disponível em: https://www.researchgate.net/publication/272532756. Acesso em: 19 jul. 2018.

BRASIL. *Lei nº 4.737, de 15 de julho de 1965.* Institui o Código Eleitoral*.* Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4737.htm. Acesso em: 10 jul. 2018.

BRASIL. [Constituição (1988)]. *Constituição da república federativa do Brasil de 1988*. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 30 jun. 2018.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 jun. 2018.

BRASIL. *Lei nº 13.488, de 6 de outubro de 2017.* Altera as Leis nos 9.504, de 30 de setembro de 1997 (Lei das Eleições), 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 (Código Eleitoral), e revoga dispositivos da Lei no 13.165, de 29 de setembro de 2015 (Minirreforma Eleitoral de 2015), com o fim de promover reforma no ordenamento político-eleitoral. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13488.htm. Acesso em: 30 jun. 2018.

BRASIL. Câmara dos Deputados. *Projeto de Lei da Câmara n° 53, de 2018a.* Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 30 jun. 2018.

BRASIL. Conselho Nacional dos Direitos Humanos. *Recomendação nº 04, de 11 de junho de 2018b.* Recomenda sobre medidas de combate às fake news (notícias falsas) e a garantia do direito à liberdade de expressão. Brasília, DF. Disponível em: http://www.mdh.gov.br/informacao-ao-cidadao/participacao-social/recomendacao-ndeg-04-2018_fake-news-e-liberdade-de-expressao.pdf. Acesso em 28 jun. 2018.

BRASIL. Tribunal Superior Eleitoral. *Representação n. 0600546-70.2018.6.00.0000*. Relator: Ministro Sérgio Banhos. DJ: 08 jun. 2018. Representante: Rede Sustentabilidade (Rede) - Diretório Nacional e Maria Osmarina Marina da Silva Vaz de Lima. Representado: Facebook Serviços Online do Brasil Ltda. Brasília, 07 jun. 2018c. Disponível em: http://inter03.tse.jus.br/djeRest/rest/downloadDiario?tribunal=TSE&numDiario=112&anoDiario=2018. Acesso em: 15 jul. 2018.

BRAYNE, S. Big Data Surveillance: The Case of Policing. *American Sociological Review*, 2017. Disponível em: http://journals.sagepub.com/doi/10.1177/0003122417725865. Acesso em: 01 jul. 2018.

BOYD, D.; CRAWFORD, K. Critical Questions for Big Data. *Information, Communication & Society*, 15:5, 2012, p.662-679. Disponível em: https://doi.org/10.1080/1369118X.2012.678878. Acesso em: 23 jun. 2018.

BUCCI, E. Pós-política e corrosão da verdade. *Revista USP*, n. 116, 2018, p.19-30. Disponível em: https://www.revistas.usp.br/revusp/article/view/146574. Acesso em: 23 jun. 2018.

COMISSÃO EUROPEIA. Reforma de 2018 das regras de proteção de dados da UE. *Comissão Europeia*, 2018. Disponível em: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt. Acesso em: 30 jun. 2018.

CRIMES NA WEB. *Delegacias Cibercrimes*. SaferNet Brasil. Disponível em: http://new.safernet.org.br/content/delegacias-cibercrimes#. Acesso em: 29 jul. 2018.

DEMCHENKO, Y.; GROSSO, P.; DE LAAT, C.; MEMBREY, P. *Addressing big data issues in Scientific Data Infrastructure***,** 2013 International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, 2013, pp. 48-55. Disponível em: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6567203&isnumber=6567186. Acesso em: 20 jun. 2018.

DFNDR LAB. *Relatório da Segurança Digital no Brasil*. PSafe, n.2, jan. 2018a. Disponível em: https://www.psafe.com/dfndr-lab/pt-br/relatorio-da-seguranca-digital/. Acesso em: 29 jun. 2018.

DFNDR LAB. *Relatório da Segurança Digital no Brasil*. PSafe, n.3, jan. 2018b. Disponível em: https://www.psafe.com/dfndr-lab/pt-br/relatorio-da-seguranca-digital/. Acesso em: 30 jun. 2018.

DUDEN. *Duden Die Grammatik*. 2018. Disponível em: https://www.duden.de/suchen/dudenonline/shitstorm. Acesso em: 18 jun. 2018.

DUSSEL, J. Cómo ganar elecciones contando "me gusta". *Página 12*, 28 mar. 2018. Disponível em: https://www.pagina12.com.ar/104359-como-ganar-elecciones-contando-me-gusta. Acesso em: 28 jun. 2018.

FACEBOOK. *102 milhões de brasileiros compartilham seus momentos no Facebook todos os meses*. 19 abr. 2016. Disponível em: https://www.facebook.com/business/news/102-milhes-de-brasileiros-compartilham-seus-momentos-no-facebook-todos-os-meses. Acesso em: 01 jul. 2018.

FEINGOLD, R*. et al*. Fake News and Misinformation: The Roles of the Nation's Digital Newsstands, Facebook, Google, Twitter, and Reddit. Fake News/Misinformation: The Challenge and the Most Effective Solutions. *Stanford Law School, Law and Policy Lab*, out. 2018. Disponível em:

https://law.stanford.edu/wp-content/uploads/2017/10/Fake-News-Misinformation-FINAL-PDF.pdf. Acesso em: 29 jun. 2018.

GLOBO Comunicação e Participações S.A. Entenda o caso de Edward Snowden que revelou espionagem dos EUA. *G1*. São Paulo, 14 fev. 2014. Disponível em: http://glo.bo/19Rj2g6. Acesso em: 22 jun. 2018.

GLOBO Comunicação e Participações S.A. WhatsApp bloqueado: Relembre todos os casos de suspensão do app. *G1*, São Paulo, 19 jul. 2016. Disponível em: http://glo.bo/29SFN9i. Acesso em: 25 jun. 2018.

GARCIA, J. Uma crítica da economia da informação na era das mídias digitais. *Revista Novos Olhares.* USP: São Paulo, v.4, n.1, 2015. Disponível em: http://dx.doi.org/10.11606/issn.2238-7714.no.2015.102233. Acesso em: 22 jun. 2018.

GUIMÓN, P. Cambridge Analytica, empresa pivô no escândalo do Facebook*,* é fechada. *El País*. Londres, 2 mai. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/05/02/internacional/1525285885_691249.html. Acesso em: 18 jun. 2018.

FOLHA de S. Paulo. Imigrante do Mali escala 4 andares para salvar bebê e vira herói na França. *Folha de S. Paulo*, 28 mai. 2018. Disponível em: https://www1.folha.uol.com.br/mundo/2018/05/imigrante-do-mali-escala-4-andares-para-salvar-bebe-e-vira-heroi-na-franca.shtml. Acesso em: 21 jun. 2018.

KEMP, S. Digital In 2018: World's Internet Users Pass The 4 Billion Mark. *We Are Social*, 30 jan. 2018. Disponível em: https://wearesocial.com/blog/2018/01/global-digital-report-2018. Acesso em: 29 jun. 2018.

MARKETING & KOMMUNIKATION. Was ist ein Candystorm?. *Marketing & Kommunikation*, 19 mai. 2016. Disponível em: https://www.m-k.ch/was-ist-ein-candystorm/. Acesso em: 23 jun. 2018.

MARTENS, B.; AGUIAR, L.; GOMEZ-HERRERA, E;. MUELLER-LANGER, F. The digital transformation of news media and the rise of disinformation and fake news. *JRC Technical Reports*: *JRC Digital Economy Working Paper* 2018-2, p.24-25, abr. 2018. Disponível em: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf. Acesso em: 01 jul. 2018.

MAYER-SCHONBERGER, V.; CUKIER, K. *Big Data:* a revolution that will transform how we live, work, and think. Londres: John Murray, 2013.

MIRANI, L. Millions of Facebook users have no idea they're using the internet. *Quartz Media LLC*, 09 fev. 2015. Disponível: https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/. Acesso em: 29 jun. 2018.

MONITOR DO DEBATE POLÍTICO NO MEIO DIGITAL. A difusão dos boatos sobre Marielle Franco: do Whatsapp aos sites de notícias. *Nota técnica n.2*. Universidade de São Paulo, 24 abr. 2018. Disponível em:

https://www.monitordigital.org/relatorios/nota-tecnica-2/. Acesso em: 25 jun. 2018.

OXFORD English. *Oxford*: Oxford University Press, 2018. Disponível em: https://en.oxforddictionaries.com/definition/shitstorm. Acesso em: 18 jun. 2018.

RAMALHO, R. Fux diz que Justiça pode anular uma eleição se resultado for influenciado por 'fake news' em massa. *G1*, São Paulo, 21 jun. 2018. Disponível em: https://g1.globo.com/politica/eleicoes/2018/noticia/fux-diz-que-justica-pode-anular-eleicao-se-resultado-for-fruto-de-fake-news-em-massa.ghtml. Acesso em: 28 jun. 2018.

RUEDIGER, M. *et al*. Robôs, Redes Sociais e Política: Estudo da Fgv/Dapp Aponta Interferências Ilegítimas no Debate Público na Web. *FGV-DAPP*, Rio de Janeiro, 2017. Disponível em: http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web/. Acesso em: 25 jun. 2018.

SALAS, J. Os novos 'inquisidores' tomam conta da rede. *El País*, 28 abr. 2015. Disponível em: https://brasil.elpais.com/brasil/2015/04/23/ciencia/1429788932_491782.html. Acesso em: 20 jun. 2018.

SILVEIRA, M.; MARCOLIN, C.; FREITAS, H. O big data e seu uso corporativo: uma revisão de literatura. São Paulo: *SINGEP*, 4, 2015. *Anais...* Disponível em: https://singep.org.br/4singep/resultado/245.pdf. Acesso em: 21 jun. 2018.

TRIBUNAL SUPERIOR ELEITORAL. *Presidente do TSE instaura procedimento para averiguar uso de notícias falsas na internet*. Brasília, 29 mar. 2018a. Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2018/Marco/presidente-do-tse-instaura-procedimento-para-averiguar-uso-de-noticias-falsas-na-internet. Acesso em: 1 jul. 2018.

TRIBUNAL SUPERIOR ELEITORAL. *Seminário Internacional Brasil-União Europeia. Fake News: Experiências e Desafios*. Brasília, 21 jun. 2018b. Disponível em: http://www.tse.jus.br/hotsites/fakenews/. Acesso em: 03 jul. 2018.

TRIBUNAL SUPERIOR ELEITORAL. *TSE aplica pela primeira vez norma que coíbe notícias falsas na internet*. Brasília, 07 jun. 2018c. Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2018/Junho/tse-aplica-pela-primeira-vez-norma-que-coibe-noticias-falsas-na-internet. Acesso em: 02 jul. 2018.

VAIDHYANATHAN, S. A Googlelização de Nós Mesmos: Vigilância Universal e Imperialismo Infraestrutural. In: _____. Googlelização *de tudo*. São Paulo: Cultrix, 2011.

VAN DIJCK, J. Confiamos nos dados? As implicações da datificação para o monitoramento social. *Matrizes*, São Paulo, v. 11, n. 1, jan./abr., 2017. Disponível em:

https://www.revistas.usp.br/matrizes/article/view/131620/127911. Acesso em: 19 jun. 2018.

VOSOUGHI, S.; ROY, D.; ARAL, S. The Spread Of True And False News Online. *MIT Initiative On The Digital Economy Research Brief*, 09 mar. 2018. Disponível em: http://ide.mit.edu/sites/default/files/publications/2017%20IDE%20Research%20Brief%20False%20News.pdf. Acesso em: 27 jun. 2018.