VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

EDSON RICARDO SALEME

FERNANDO GALINDO AYUDA

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; Edson Ricardo Saleme; Fernando Galindo Ayuda – Florianópolis; CONPEDI, 2023.

Inclui bibliografia
ISBN: 78-65-5648-746-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

Apresentação do CONPEDI – novas tecnologias.

O grupo constituído por DANIELLE JACON AYRES PINTO, FERNANDO GALINDO e EDSON R. SALEME presidiram o GT Direito, Governança e novas tecnologias II, que tiveram o privilégio de conduzir excelentes trabalhos apresentados, que apontaram as necessidades brasileiras mais prementes, em termos normativos, na era digital. Os trabalhos abordaram as características mais marcantes que estão sujeitos os dados, sobretudo em face da LGPD, mediante a apresentação de propostas para a governança democrática. Outros temas a destacar foram os relacionados ao uso de tecnologias da informação e comunicação nos julgados, bem como de que forma os tribunais brasileiros estão empregando programas de inteligência artificial e como se poderia encontrar limites a essa utilização.

O primeiro a apresentar o trabalho foi o doutorando Ronaldo Felix Moreira Junior acerca da disseminação de notícias falsas e os limites do uso de dados pessoais em campanhas eleitorais, que abarcou a LGPD discutindo como os dados pessoais sensíveis têm sido empregados para fins políticos, como instrumentos de ataque à democracia. O discente Lorenzo Borges de Pietro apresentou o trabalho denominado "A (in) constitucionalidade da suspensão de plataformas da internet em decorrência do descumprimento de decisão judicial: um debate a luz do princípio da proporcionalidade, discutindo o alcance das decisões judiciais em termo de internet. O tema entabulado no próximo artigo foi o "Colonialismo Digital e os entraves à proteção de direitos fundamentais na era do Capitalismo de Vigilância", por Ronaldo Felix Moreira Junior, que apresentou o primeiro trabalho. Discutiu-se que os dados pessoais foram incluídos no rol de direitos fundamentais e que grandes empresas, contratadas para lidar com dados pessoais, podem empregá-los a seu talante. Portanto, deve existir uma tecnologia própria para a proteção deles. Pedro Ribeiro Fagundes apresentou o trabalho acerca da importância da gestão de riscos para a motivação dos atos administrativos. Esta motivação, essencial em todo o ato, deve levar em consideração os riscos que o gestor pode incidir, bem como os respectivos prejuízos que esses riscos podem produzir. Tainara Conti Peres e Deise Marcelino da Silva apresentaram o trabalho "A LGPD e a sua adequação no ambiente laboral: sob a ótica de controle do empregador privado brasileiro." As autoras inferem que a proteção de dados é própria desta época e abordaram, especificamente, as relações trabalhistas e analisam como se aplicam nas relações de trabalho, sobretudo sob a óptica do empregador privado. Valdir Rodrigues de Sá e Irineu

Francisco Barreto Júnior, que se encarregaram do tema “Liberdade de expressão nas plataformas digitais”, teve como objeto a análise da prática de crimes com a abertura da liberdade virtual existente no presente. O próximo trabalho apresentado por Gabrieli Santos Lacerda da Silva, dedicou-se ao tema “Os limites do consentimento frente ao direito fundamental de proteção dos dados pessoais”, que abordou a temática da mudança do comportamento humano diante dos avanços digitais. Nesse sentido, o grande volume de dados da internet, entre eles os dados pessoais, geram implicações na própria dinâmica social, o que fez a CF incluir dispositivos constitucionais e infraconstitucionais. Após a apresentação e aluna Tricieli Radaelli Fernandes e Fernando Hoffmam trouxeram a temática “O capital e a(s) guerra(s) na era do capitalismo de vigilância e a constituição de tecnopolíticas de combate”. O trabalho reflete que pode ser uma guerra real ou de violência simbólica diante da existência de tecnologias que podem perpetuar ou resgatar fórmulas capitalistas existentes nas diversas zonas. A seguir passou-se a apresentar por Estella Ananda Neves o artigo “Análise econômica do impacto da inteligência artificial nos tribunais brasileiros.” O baixo nível de investimentos e a parca participação de empresas brasileiras refletem o desenvolvimento atual do país e afirmam que o Judiciário pode em muito auxiliar o aprimoramento do Brasil. O primeiro bloco finalizou com a apresentação do trabalho “Administração Pública na era digital: uma análise sobre a segurança de dados nas sociedades de economia mista e empresas públicas à luz da LGPD” apresentado por Jean Marcel dos Santos. Como proteger os dados no atual panorama. O primeiro bloco foi encerrado com considerações dos coordenadores do GT, sobretudo o Prof. Galindo, que observou a questão da vigilância de dados nos sistemas jurídicos, a exemplo do que se pode observar na legislação europeia, como a que estabelece regras acerca da inteligência artificial, cuja matéria continua sendo regulada pelo Parlamento Europeu que, no último 14 de junho de 2023, aprovou sua posição negociadora sobre a Lei de Inteligencia Artificial. Importante recordar que esta norma incluí, entre os sistemas de alto risco os sistemas de IA que estão referidos na Administração de Justiça.

O segundo bloco de intervenções começou com o trabalho de Roseli Rêgo Santos Cunha Silva abordou no trabalho A LGPD e o tratamento de dados por agentes de pequeno porto: uma análise a partir da Resolução CD/ANPD N°2/2022. A abordagem indica que devem ser disponibilizados meios, compatíveis com as atividades de menor porte, considerando o bem que a LGPD objetiva proteger, a Resolução não exclui atores de menor porte; o discente Guilherme Elias Trevisan apresentou o trabalho “Big tech, dados, infraestruturas digitais e as universidades públicas federais brasileiras.” Restringiu-se a analise da verificação do sigilo da infraestrutura de dados e a disparidade de tecnologia que geram impactos geopolíticos, sobretudo nas universidades federais. Lidiana Costa de Sousa Trovão e Igor Marcellus Araujo Rosa apresentaram o trabalho intitulado “Cidades Inteligentes Sustentáveis,

governança e regulamentação de dados"; o trabalho analisa como essas cidades podem atingir o objetivo socioambiental e a quem são efetivamente destinadas. A seguir Luiz Fernando Mingati passou a expor o trabalho Constitucionalismo na era digital: os desafios impostos pela era informacional frente às garantias constitucionais. O artigo versa sobre como o impacto da era da informação e como ocorrem modificações na ordem interna geradas por esse fato. A seguir o Prof. Lucas Gonçalves da Silva apresentou juntamente com o aluno Reginaldo Felix "Tributação e Novas Tecnologias", os autores indicam que há uma tributação apresenta um novo percalço pela falta de transparência que os entes tributantes possuem diante desta atividade. O próximo trabalho trouxe a temática "Das cortes físicas às cortes digitais: a transformação digital dos tribunais como instrumento de acesso à justiça", pelo aluno Dennys Damião Rodrigues Albino; a temática se concentra na possibilidade de o Judiciário acompanhar a atual tendência digital e quais seriam as condicionantes a essas mudanças. A seguir David Elias Cardoso Camara apresentou o trabalho "Software de decisão automatizada como ferramenta de compliance no Tribunal de Justiça do Maranhão." O artigo estabelece uma análise geral sobre alguns documentos do Banco Mundial que analisa algumas ineficiências do Poder Judiciário. A seguir o aluno Pedro Gabriel C. Passos analisa no artigo "Desafios para concretização do ODS 8: análise a partir da dinâmica da indústria 4.0" que trata das TICs no ambiente do trabalho e alguns fenômenos que este pode apresentar em termos de prestação de serviços no mundo digital. Thiago Leandro Moreno seguiu apresentando o trabalho "Direito e Tecnologia: criptoativos e tokens não fungíveis", o trabalho versa sobre a ideia do metaverso e as transações ocorridas nos espaços virtuais. Novamente Irineu Francisco Barreto Jr e Kelly Cristina Maciel da Silva apresentaram o trabalho "O paradoxo entre a garantia constitucional do direito à informação e a preservação da privacidade em banco de dados públicos e privados." Constata-se pelo artigo que não existe ainda proteção suficiente para eventuais ataques virtuais.

O último bloco iniciou-se com o artigo "Mercosul X União Europeia: necessária adequação da autoridade nacional de proteção de dados" por Bruno Alexander Mauricio e Kennedy Josué Grecca de Mattos. A seguir apresentou-se o artigo "Mitigação de vieses algorítmicos em processos decisórios: os impactos da diversidade na constituição de equipes desenvolvedoras de inteligência artificial", por Airto Chaves Jr e Pollyanna Maria da Silva. O objetivo da investigação é verificar os impactos da constituição de equipes responsáveis pelas inteligências artificiais. Na sequencia José Octávio de Castro Melo apresentou o trabalho "Novas tecnologias e regulação: uma análise do PL 872/2021 face ao dever de diligência do Estado na proteção do direito à privacidade." A apresentação do trabalho "O uso da inteligência artificial no âmbito do processo judicial: desafios e oportunidades" por Jordy Arcadio Ramirez Trejo e Saulo Capelari Junior abordou de que forma deve ser implementada a inteligência artificial no âmbito do Poder Judiciário. A seguir Luciana

Cristina de Souza apresentou o trabalho “Risco no uso das inteligências artificiais e segurança digital” levando em consideração a atual forma que se aborda possíveis culpados com possível transgressão ao principio da presunção de inocência. Na sequência, Thais Aline Mazetto Corazza, expôs o trabalho “Os riscos na tomada de decisões por máquinas”. Já existe, no âmbito dos tribunais, certa triagem para evitar repetições e assim proporcionar melhores benefícios. Deve-se ter cuidado ao aplicar essas ferramentas, pois possuem subjetividades complexas. Bruno Mello Corrêa de Barros Beuron apresentou o trabalho “Revolução tecnológica e sociedade pós-moderna: perspectivas da obsolescência programada e do direito do consumidor à luz da metateoria do direito fraterno” . Luciana Rodrigues dos Santos e Aparecida Moreira de Oliveira Paiva apresentaram o artigo “Risco no uso das inteligências artificiais e segurança digital” em que se observa a questão relacionada a inteligência artificial pelos órgãos públicos e as questões discriminatórias.

Ao final houve manifestação de todos relativamente ao conteúdo apresentado e o quanto enriquecedor o Grupo de Trabalho foi para todos com ponderações extremamente profícuas de todos os presentes.

A DISSEMINAÇÃO DE NOTÍCIAS FALSAS E OS LIMITES DO USO DE DADOS PESSOAIS EM CAMPANHAS ELEITORAIS

THE SPREAD OF FAKE NEWS AND THE LIMITS OF THE USE OF PERSONAL DATA IN ELECTORAL CAMPAIGNS

Ronaldo Felix Moreira Junior

Resumo

O presente artigo tem como objetivo analisar a relação entre a proteção de dados sensíveis e o processo eleitoral em tempos de Big Data. Com base na análise da Lei Geral de Proteção de Dados (LGPD) e da legislação eleitoral, especificamente a Lei n. 9.504/1997, que permite a propaganda eleitoral na internet, o trabalho busca traçar os limites legais para o uso de informações pessoais para fins eleitorais. Por meio de pesquisa bibliográfica e análise de casos concretos envolvendo empresas como Quickmobile, Croc Services, SMS Market e Yacows, o artigo ilustra os limites do uso de dados pessoais e identifica possíveis violações aos direitos fundamentais protegidos pela LGPD. Com a crescente utilização de tecnologias digitais e Big Data no processo eleitoral, torna-se ainda mais relevante a discussão sobre a proteção de dados pessoais e sua relação com os direitos fundamentais, especialmente em um momento em que o uso indevido de informações sensíveis pode influenciar significativamente o resultado das eleições. Portanto, o artigo conclui enfatizando a importância da conscientização sobre a proteção de dados pessoais no contexto eleitoral e a necessidade de se estabelecer limites claros para o uso dessas informações, a fim de garantir a proteção dos direitos fundamentais e a integridade do processo democrático.

Palavras-chave: Fake news, Democracia, Liberdade de expressão, Processo democrático, Proteção de dados sensíveis

Abstract/Resumen/Résumé

This article aims to analyze the relationship between the protection of sensitive data and the electoral process in times of Big Data. Based on the analysis of the General Data Protection Law (LGPD) and electoral legislation, specifically Law No. 9.504/1997, which allows electoral propaganda on the internet, the work seeks to establish legal limits for the use of personal information for electoral purposes. Through bibliographic research and analysis of concrete cases involving companies such as Quickmobile, Croc Services, SMS Market, and Yacows, the article illustrates the limits of the use of personal data and identifies possible violations of fundamental rights protected by the LGPD. With the growing use of digital technologies and Big Data in the electoral process, the discussion about the protection of personal data and its relationship with fundamental rights becomes even more relevant, especially at a time when the misuse of sensitive information can significantly influence the outcome of elections. Therefore, the article concludes by emphasizing the importance of

awareness about the protection of personal data in the electoral context and the need to establish clear limits on the use of this information in order to guarantee the protection of fundamental rights and the integrity of the democratic process.

Keywords/Palabras-claves/Mots-clés: Fake news, Democracy, Freedom os speech, Democratic process, Sensitive data protection

1 INTRODUÇÃO

O presente trabalho tem como escopo abordar a relação entre dois importantes temas: 1) o processo eleitoral; e 2) a proteção de dados pessoais. Sabe-se que o modelo representativo de democracia buscou, com o passar do tempo, aperfeiçoar-se, o que fez com o crescente uso de aparatos tecnológicos e com o desenvolvimento das tecnologias de comunicação e informação.

Se em um determinado momento foi importante o tratamento legal de comícios e, posteriormente, do tempo de apresentação em rádio ou televisão, hoje se faz essencial não apenas tratar da propaganda política no meio digital, mas também da forma como essa propaganda poderá fazer uso de dados pessoais dos eleitores.

Essa preocupação ocorre porque o processo eleitoral, como instrumento de ilustração da soberania popular, possui o voto como um de seus elementos essenciais. O voto, realizado sem ingerências externas, compõe um dos requisitos para o funcionamento do modelo representativo atualmente existente. Ocorre que a manipulação de dados sensíveis pode fazer com que sejam direcionadas informações falsas aos eleitores. Essas informações, conforme será demonstrado, afetam a maneira de votar do indivíduo e, consequentemente, também afetam de modo negativo o processo democrático.

A proteção dos dados individuais não configura uma preocupação recente, haja vista que possui base constitucional ligada à inviolabilidade da intimidade, bem como da vida privada, honra e imagem (conforme o art. 5º, X, CF). Não obstante, é importante destacar a proteção que consta no inciso XI (do mesmo dispositivo) a respeito da inviolabilidade do sigilo de correspondência e de comunicações telegráficas – exceto nas hipóteses em que há devida ordem judicial fundamentada.

Muito embora não trate a Carta Magna de dados pessoais digitais (haja vista sua promulgação em 1988), pode-se compreender a existência constitucional da proteção da privacidade, vista como direito fundamental.

O Brasil, por outro lado, conta com uma recente legislação específica quanto à proteção do tratamento de dados pessoais feitos por pessoa natural ou jurídica (de direito público ou privado): a chamada Lei Geral de Proteção de Dados (Lei 13.709/18). Pode-se dizer que a legislação tem como principal objetivo a proteção dos direitos fundamentais de liberdade e privacidade, além do devido desenvolvimento da personalidade da pessoa natural (tal como consta no art. 1º, da legislação mencionada). De forma conexa, a lei

também aborda o tratamento de dados considerados sensíveis, que incluem elementos como a opinião política e filiação partidária (em seu art. 5º, I).

Ainda assim, é possível evidenciar a violação desses direitos não apenas para fins comerciais (como o direcionamento de anúncios e propagandas não autorizados), mas também políticos, como ocorreu no exterior com o caso *Cambridge Analytica* (no exterior) e *Yacows* (no Brasil).

Dessa maneira, com base na legislação vigente, o artigo pretende demonstrar quais são os limites legais para o uso de dados pessoais para fins eleitorais.

O trabalho, portanto, será dividido em três tópicos para melhor responder à indagação proposta: 1) em um primeiro momento é necessário demonstrar a já existente utilização ilegal de dados pessoais para finalidades eleitorais. O caso da empresa *Yacows* (entre outras) será analisado para este fim; 2) a segunda parte do trabalho tem como objetivo apresentar a LGPD (Lei 13.709/18), abordando a importância dessa legislação, inclusive para o bom andamento do processo eleitoral; 3) por fim, será apontado como a legislação mencionada, além de outros regramentos eleitorais específicos, abordam a questão do tratamento de dados sensíveis para fins políticos. Busca-se também apontar eventuais omissões legais.

2 O TRATAMENTO DE INFORMAÇÕES SENSÍVEIS EM TEMPOS DE BIG DATA

Há uma dependência que se formou em relação ao uso da rede mundial de computadores em todos setores da sociedade. No campo jurídico, busca-se eliminar (ou diminuir) o número de processos físicos, ao mesmo tempo em que se pretende dar maior agilidade aos atos processuais, como ocorre por meio de intimações eletrônicas. A questão é que são poucos os setores da vida humana que não sofreram maior ou menor influência das novas tecnologias de informação ou comunicação.

Afirma-se, portanto, que as estruturas sociais e também políticas (vinculadas a fluxos de dados e comunicações em escala mundial) acabam por remodelar a própria organização da sociedade, proporcionando mudanças consideráveis nas estruturas tradicionais do exercício de poder (LOPES; MOREIRA JÚNIOR, 2019, p. 33).

O que se pode concluir é que tanto entidades privadas e públicas, além de movimentos sociais (e também os próprios indivíduos) estão atualmente conectados por

meio dessa vasta rede informacional. A consequência de tal conexão é um impacto cada vez maior nos campos da economia, política e até mesmo na cultura.

Um conceito de extrema importância nesse contexto é o de *big data* (ou megadados), que se refere à enorme quantidade de dados que são produzidos em alta velocidade, além de grande volume e considerável variedade. Para Soares (2018, p. 152), por mais que possa parecer que os megadados são consequência de um processo de construção técnica e que pode ser controlado por parte da sociedade, há um grande desafio colocado pelos algoritmos e também pelo fluxo de dados no que diz respeito às suas implicações na organização social. Isso se torna algo notável a partir do momento em que as tecnologias preditivas (que são utilizadas para mapear padrões nos comportamentos individuais e de grupos) fazem com que diversas empresas mantenham seu foco aquisição de dados pessoais e no direcionamento específico de publicidade.

Esse grande número de informações é utilizado, como se pode inferir, por diversos entes (individuais ou coletivo, públicos ou privados) para diferentes fins. Por exemplo: nas redes sociais digitais, em decorrência do comportamento das pessoas, há uma constante recomendação de conteúdo ligado aos eventuais gostos do usuário.

Há uma preocupação global com o uso arbitrário e ilícito de tais dados, de modo que os últimos anos foram marcados pelo nascimento de legislações responsáveis por regulamentar o tratamento de dados pessoais. No Brasil, a legislação mais marcante a respeito deste assunto é a Lei Geral de Proteção de Dados (Lei 13.709/18), que será tratada em tópico específico.

Ainda assim, é possível verificar a existência de diversas ocorrências ilícitas em relação ao uso de tais dados. No âmbito internacional, ganhou notoriedade o caso da empresa *Cambridge Analytica*. Em 2016, houve extensa discussão quanto a papel exercido pela corporação na campanha eleitoral estadunidense na qual saiu vitorioso Donald Trump. Alegou-se (OLIVEIRA, 2018) que o trabalho feito pela empresa se baseou na utilização de informações de inúmeros usuários de *internet* para o impulsionamento de notícias. Conforme o próprio CEO da *Cambridge Analytica*, Alexander Nix, há grande importância de fatores demográficos, geográficos e econômicos na visão de mundo de um indivíduo (ou mesmo de grupos), contudo "[...] é a personalidade que guia os comportamentos, e os comportamentos obviamente influenciam como você vota" (OLIVEIRA, 2018).

A empresa teria, portanto, realizado um complexo procedimento que dependeu da participação de usuários de redes como o *Facebook*, que tiveram seus dados coletados (e de seus contatos) sem o devido consentimento.

Importa ressaltar que esse tipo de discussão quanto ao uso de dados sensíveis de usuários de redes digitais também ocorreu no Brasil, conforme será demonstrado a seguir.

2.1 A DISSEMINAÇÃO DE NOTÍCIAS FALSAS NO BRASIL NO CONTEXTO POLÍTICO

O popular aplicativo *WhatsApp*, muito embora seja um facilitador de comunicação à distância, foi apontado como uma importante ferramenta na disseminação de notícias falsas, revelando-se, também como um obstáculo para a gestão da Justiça Eleitoral.

Notícias falsas não são um problema recente, o que se discute atualmente está mais relacionado à forma como elas são disseminadas. Ainda assim, no que diz respeito ao termo *fake news*, é preciso realizar um importante recorte, haja vista a utilização constante do termo para designar apenas uma versão diferente da que é contada por um interlocutor.

Conforme Frias Filho (2018, p. 43), a ideia de *fake news* está ligada à informação que, apesar de comprovadamente falsa, é capaz de prejudicar terceiros, tendo sido possivelmente forjada e/ou posta em circulação por negligência ou má-fé – ela pode visar ao lucro ou à manipulação política.

São os dados pessoais sensíveis que permitem a rede algorítmica a disseminar as informações falsas nas redes das mais diversas plataformas. Já é conhecida a possibilidade de construção de modelos de predição com a finalidade de análise de tendências de comportamentos individuais e de grupos. Muito embora essa estratégia pode estar relacionada a propagandas comerciais direcionadas, a mesma tecnologia pode vir a afetar o processo eleitoral.

Há estudos que demonstram a utilização de técnicas de propaganda computacional para os referidos fins eleitorais. Daniel Arnaudo, *Research Fellow* do Instituto Igarapé (2017, p. 20), aponta que essas técnicas incluem o microdirecionamento de mensagens de maneira individualizada (a grupos de eleitores) por meio da coleta de seus dados pessoais, o que leva à divulgação de *fake news* através da utilização de contas automatizadas.

Nesse sentido, foi ingressada, no ano eleitoral de 2018, uma ação judicial eleitoral por abuso de poder econômico e uso indevido de meios de comunicação. A ação

(BRASIL, 2018, p. 2) foi ajuizada pela Coligação “O Povo Feliz de Novo” (que envolvia os partidos políticos PT, PCdoB e PROS) contra o então candidato Jair Messias Bolsonaro e seu vice Antônio Hamilton Martins Mourão, além do empresário Luciano Hang e as pessoas jurídicas de direito privado *Quick Mobile* Desenvolvimento e Serviços Ltda., *Yacows* Desenvolvimento de *Software* Ltda., *Croc* Services Soluções de Informática Ltda., *SMSMarket* Soluções Inteligentes Ltda., além do *Facebook* Serviços Online do Brasil Ltda. (responsável pelo aplicativo WhatsApp).

Em especial, é preciso mencionar mais uma vez que o *WhatsApp* foi apontado como uma importante ferramenta para a disseminação de *fake news*, o que muito provavelmente decorre do fato de que, não havendo cobrança pelas mensagens ou controle de conteúdo, não há que se falar em prestação de quaisquer tipos de contas em relação ao que é enviado pelo aplicativo (tendo ou não cunho político).

A ação em estudo, em sua petição inicial (BRASIL, 2018, p. 3), relata uma reportagem publicada pelo Jornal Folha de São Paulo (MELLO, 2018) na qual há documentação comprobatória de irregularidades na contratação do serviço de realização de disparos massivos de mensagens de contexto eleitoral pelo *WhatsApp*. A petição ainda menciona uma rede de empresas que fez uso fraudulento de nomes e CPF de pessoas idosas para o registro de chips de celular com uma relação de 10 mil nomes de pessoas nascidas entre 1932 e 1953 (BRASIL, 2018, p. 3). Tal como destacado, as empresas *Quickmobile*; *Croc Services*; *SMS Market*; e *Yacows* são colocadas como perpetradoras do sistema de propagação financiado por empresários.

Importa destacar, nesse momento, os argumentos jurídicos realizados pela parte autora, embasados especialmente na lei 9.504/97, que estipula em seu art. 57-E: “São vedadas às pessoas relacionadas no art. 24 a utilização, doação ou cessão de cadastro eletrônico de seus clientes, em favor de candidatos, partidos ou coligações” (BRASIL, 1997). O art. 24 apontado no dispositivo diz respeito a, entre outros entes, órgãos da administração pública direta ou indireta; concessionários ou permissionários de serviço público; entidade de direito privado recebedora de contribuição em virtude de disposição legal; e organizações da sociedade civil de interesse público.

Dessa maneira, a parte autora buscou caracterizar a ocorrência de abuso de poder, o que faz em conjunto com a alegação da existência de doação realizada por pessoa jurídica.

Entretanto, no que pese os argumentos oferecidos, o Tribunal Superior Eleitoral, por meio da decisão do Min. Jorge Mussi, negou o pedido cautelar realizado sob a

orientação pré-existente da jurisprudência do tribunal "[...] no sentido de prestigiar a liberdade de manifestação do pensamento, de expressão e de informação" (BRASIL, 2018).

Apesar da decisão, é importante ressaltar que o caso mencionado lida com uma dupla complexidade: 1) a alegação de doação de campanha por empresas, o que é vedado pela legislação eleitoral; 2) a alegação de empresas apoiadoras do então candidato Jair Bolsonaro (PSL) que compraram o serviço de "disparo em massa", o que foi feito a partir de uma base de dados de usuários vendidas por agências de estratégia digital (MELLO, 2018).

Conforme será demonstrado, há uma série de limites no uso de informações sensíveis, o que faz com que a decisão proferida pelo TSE esteja em completo equívoco, com base nas informações que serão apresentadas em relação a atual legislação de proteção de dados.

É importante mencionar que o uso (indevido) de dados pessoais para disseminação desse tipo de informação extrapola não apenas a LGPD, mas a própria liberdade de expressão. Isso se torna ainda mais complexo quando são criados grupos que repassam as notícias falsas. Conforme a reportagem mencionada (MELLO, 2018), há uma estimativa que vai de 20 a 300 mil pessoas que estavam lidando diretamente no setor de grupos de *WhatsApp* para disparos de mensagens contra partidos políticos específicos.

O presente trabalho não busca atacar a decisão proferida pelo TSE, mas prestar-se-á demonstrar como a legislação atual pode ser utilizada como base de responsabilização do uso indevido de dados.

3 A NECESSIDADE DE UMA LEI GERAL DE PROTEÇÃO DE DADOS

O tratamento de dados sensíveis tem sido discutido para muito além do campo eleitoral e não somente no Brasil. A produção massificada de dados, mencionada no tópico anterior, fez com que os Estados nacionais se preocupassem com o tema e, na Europa, o Regulamento Geral de Proteção de Dados (UE, 2016), surgiu com o intuito de tornar o continente Europeu um exemplo para a proteção de dados sensíveis.

Em 2018 o Brasil aprovou lei com objetivo similar, a lei 13.709/18. A legislação nacional busca assumir um papel de protagonista na temática em questão, apresentando fundamentos e princípios que extrapolam a própria legislação, no intuito de esclarecer o pensamento jurídico (COTS; OLIVEIRA, 2019, p. 38-39).

Importa ressaltar que os dados pessoais e sensíveis abordados pela legislação mencionada dizem respeito à necessidade de proteção da pessoa natural. O eventual tratamento ilegal desses dados, contudo, poderão ser realizados por qualquer pessoa física ou jurídica, seja ela de direito público ou privado (COTS; OLIVEIRA, 2019, p. 42).

É preciso mencionar o que a legislação compreende como dado pessoal, o que consta em seu art. 5º, I (BRASIL, 2018): "[...] dado pessoal: informação relacionada a pessoa natural identificada ou identificável". Dessa maneira, exclui-se do âmbito de proteção da LGPD os chamados dados anonimizados (em consonância com o art. 5º, III, da legislação, sendo aqueles que passam por um processo que impossibilite a reversão e eventual identificação do usuário).

O que interessa a esse trabalho é principalmente o que diz respeito aos chamados dados pessoais sensíveis. Conforme estabelece o art. 5º, II, da LGPD:

> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

É o uso desses dados a razão das discussões relacionadas à disseminação de *fake news* para fins de ingerência no processo eleitoral. A partir de um banco de dados de pessoas que se inserem dentro de um mesmo espectro político (entre outras particularidades) utilizados por determinadas pessoas físicas e jurídicas, foi possível determinar que tipo de conteúdo seria direcionado. No caso mencionado em tópico anterior, houve um espalhamento de mensagens falsas a respeito de um partido político rival, o que pode ter impactado o resultado das votações no ano de 2018.

Esses dados merecem especial proteção justamente porque podem ser utilizados não apenas para fins políticos, mas também discriminatórios. São informações relacionadas a aspectos extremamente particulares da vida privada de uma pessoa.

algumas informações ainda merecem destaque no presente tópico: 1) o que se entende por tratamento; 2) que tipo de tratamento pessoal é permitido pela legislação; 3) se é possível a manipulação dos dados considerados sensíveis; e 4) quem são os diferentes atores envolvidos no tratamento de dados e quais são suas responsabilidades.

3.1 O TRATAMENTO DE DADOS PESSOAIS

A partir do momento em que se compreende o dado pessoal como toda informação capaz de individualizar seu titular, é preciso apontar o que deve ser entendido por tratamento.

Trata-se de qualquer atividade que faça uso de um dado não anonimizado. As atividades englobam (mas não se limitam) as descritas abaixo (SILVA, 2020, p. 16):

1) Armazenamento, como possibilidade de manutenção de um dado; 2) Avaliação, como análise de um dado com o escopo de produzir algum tipo de informação; 3) Classificação, como forma de ordenação de dados seguindo algum critério pré-estabelecido; 4) Coleta, que se trata do recolhimento propriamente dito de algum dado pessoal para uma dada finalidade; 5) Difusão, como a divulgação ou disseminação de um dado; 6) Extração, como a possibilidade de se copiar ou retirar dados do local em que este era mantido; 7) Processamento, que engloba o uso de dados pessoais organizados para que se obtenha um certo resultado; 8) Produção, vista como a criação de determinado bem ou serviço a partir de um tratamento já realizado com a informação obtida; 9) Transferência, como a mudança de dados para terceiro, que também poderá realizar determinado tratamento; 10) Transmissão, vista como a movimentação de dados entre pontos por meio de ferramentas eletrônicas, telegráficas ou similares.

A Lei Geral de Proteção de Dados será aplicada a qualquer operação de tratamento como as mencionadas feita em território nacional, ou por meio de dados que foram coletados em território nacional, ou que pertençam a titular localizado em território nacional, o que independe se essas informações foram colhidas *online* ou *offline* (SILVA, 2020, p. 16).

Nota-se que a lei está restrita a esses usos, além de estipular de maneira clara, em seu art. 4º (BRASIL, 2018), que não será aplicada nas seguintes situações: 1) quando o tratamento é feito por pessoa natural para finalidades exclusivamente particulares (sem cunho econômico); 2) quando é feito para fins jornalísticos, artísticos ou acadêmicos; 3) com finalidade exclusiva voltada à segurança pública, defesa nacional, segurança do Estado, além de atividades de investigação e repressão de infrações criminais; 4) quando o tratamento for proveniente de fora do campo territorial nacional, não sendo objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou que tenha sido objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione algum grau de proteção de dados pessoais adequado ao que é previsto na legislação.

Conforme essa análise preliminar, é possível demonstrar que o uso de dados alcançados sem consentimento prévio para fins de repasse de notícias falsas de cunho político não se insere em nenhuma das exceções legais, muito embora esse uso esteja evidenciado nas ações de tratamento as quais a lei se destina, como coleta, difusão, processamento e transmissão.

3.2 TRATAMENTOS PESSOAIS PERMITIDOS PELA LGPD

Se o tópico anterior deixou claro quais os tipos de tratamento estão sujeitos à legislação, é preciso mencionar quais dessas hipóteses a LGPD trata como lícitas. Uma leitura do art. 23 permite a compreensão de que os entes responsáveis pelo tratamento poderão fazê-lo somente para o atendimento de uma finalidade específica que tenha como objetivo a execução de competências legais ou cumprimento de atribuições que sejam contratualmente ajustadas. É imperativo que essas hipóteses estejam previamente tratadas e informadas ao titular (BRASIL, 2018).

Conforme Silva (2020, p. 18-19), as bases legais que legitimam o tratamento são: 1) O consentimento do titular: tendo em vista que a LGPD exige essa confirmação por escrito ou por outro meio idôneo, manifestando sua inequívoca vontade; 2) O cumprimento de obrigação legal ou regulatória pelo controlador: de modo a impedir que a LGPD entre em conflito com outras leis; 3) Para execução de políticas públicas: hipótese voltada aos órgãos públicos que também estão obrigados ao cumprimentos das diretrizes da legislação; 4) Para a realização de estudo de órgão de pesquisa: sendo garantida, sempre que possível, a anonimização dos dados; 5) Necessidade para execução de contrato: referindo-se à necessidade do tratamento para que seja executado um contrato ou procedimento preliminar; 6) Exercício regular de direito: ocorre quando o tratamento acontece para fins específicos decorrentes de ordem judicial ou alguma imposição legal; 7) Proteção da vida ou tutela da saúde: admite-se o tratamento para proteção de vida ou incolumidade física do titular ou de terceiros; 8) Interesse legítimo do controlador ou de terceiros: trata-se da autorização do controlador a tratar os dados pessoais para diversos fins, mas é preciso que sejam considerados legítimos, como no caso de apoio ou promoção de atividades que beneficiem o titular de dados, respeitando-se os direitos, suas liberdades fundamentais e a devida proteção; 9) Proteção ao crédito: ocorre quando o tratamento serve como garantia ao controlador no recebimento do crédito que lhe é devido.

Essas hipóteses se fundam em determinados princípios que são previstos na própria LGPD em seu art. 6º (BRASIL, 2018): 1) Finalidade; 2) Adequação; 3) Necessidade; 4) Segurança; 5) Prevenção; 6) Responsabilização e prestação de contas; 7) Livre Acesso; 8) Qualidade dos dados; 9) Transparência; 10) Não discriminação.

É importante ressaltar que o exemplo citado em tópico anterior também não se insere dentro das bases legais mencionadas, principalmente no que diz respeito à ausência de consentimento do titular. Não obstante, nota-se uma inobservância a princípios, tais como finalidade e transparência.

3.3 A MANIPULAÇÃO DE DADOS SENSÍVEIS

Conforme já explicitado, a definição de dado pessoal se encontra no art. 5º, I, da LGPD (BRASIL, 2018), o que abarca "[...] toda informação relacionada à pessoa natural identificada ou identificável". Ocorre que nem todo dado pessoal deve ser tratado da mesma maneira, haja vista que algumas informações possam vir a causar maior dano ao indivíduo caso sejam tratadas de maneira incorreta.

Algumas informações mais convencionais (tais como nome ou endereço do indivíduo) podem ser utilizadas de maneira fácil para que o titular seja identificado. Conforme consta no dispositivo mencionado, também é objeto de proteção da lei toda informação capaz de tornar seu titular identificável, ainda que de maneira indireta. Nesse patamar, é possível mencionar informações como dados de geolocalização (de um aparelho celular, por exemplo), ou o *Internet Protocol* (ou IP), pelo qual é possível se conectar à *internet*.

No que pese a legislação trazer a necessidade de proteção de dados que identifiquem direta ou indiretamente um titular, há informações de cunho extremamente pessoal, chamados dados pessoais sensíveis. Consoante Silva (2020, p. 15), são aquelas informações que podem levar a atos de caráter discriminatórios contra os titulares de determinados dados. Merecem especial atenção e proteção e englobam informações como origem étnica, convicção religiosa ou filosófica, além de opinião e filiação política. Essas últimas características, de grande importância para o presente estudo.

O tratamento de tais dados sensíveis segue a mesma lógica de proteção que a RGPD na União Europeia (nos arts. 4º e 9º), que submete tais informações (o que engloba também dados genéticos e biométricos) a regras específicas de tratamento (UNIÃO EUROPEIA, 2016).

Nota-se que algumas pessoas também merecem maiores cuidados no tratamento de seus dados pessoais. É o caso de crianças e adolescentes, que devem ser feitos em seu melhor interesse, da forma estabelecida no art. 14, da legislação (BRASIL, 2018).

Quanto ao tratamento de tais dados, o art. 11 define seus limites, sendo possível a manipulação apenas quando o titular ou responsável legal der o consentimento de forma específica e destacada, desde que para finalidades específicas; ou quando não houver consentimento, mas apenas nos seguintes casos (BRASIL, 2018):

> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

É preciso deixar claro, portanto, que não há possibilidade de uso de dados pessoais sensíveis caso não haja consentimento para específica finalidade ou nos casos elencados (quando não houver consentimento), sendo necessário também apontar o que consta no art. 12, §2º, da legislação (BRASIL, 2018), ao determinar que são também considerados dados pessoais aqueles que são utilizados para a formação de perfil comportamento de pessoa natural identificada.

3.4 OS DIFERENTES ATORES NA LGPD

O presente artigo, além de ter a necessidade de abordar os conceitos elementares do tópico passado, também precisa definir os diferentes atores no contexto da lei geral de proteção de dados. Trata-se de uma tarefa de relevância, haja vista que é preciso saber qual o grau de responsabilidade desses indivíduos em caso de tratamento ilegal de dados pessoais.

O ator mais relevante é certamente o titular, o sujeito protegido pela legislação e a quem se referem os dados coletados e tratados, conforme definido pelo art. 5º, V, da LGPD (BRASIL, 2018). Como mencionado em tópico anterior, fala-se apenas em pessoa natural.

O controlador, por outro lado, pode ser tanto pessoa física ou jurídica, também poderá ser pessoa jurídica de direito público ou privado. Trata-se de quem coleta os dados pessoais e quem toma decisões tocantes ao procedimento de tratamento de dados, definindo questões como finalidade da manipulação e tempo de manutenção de armazenamento. Sua definição se encontra no inciso VI do já referido dispositivo.

Enquanto o controlador toma as decisões, o tratamento dos dados é efetivamente feito pelo operador, que poderá ser tanto pessoa física quanto jurídica. A manipulação é feita em nome do controlador (art. 5º, VII). Tanto o controlador quanto o operador são considerados agentes de tratamento, nos termos do inciso IX (BRASIL, 2018).

Os três atores mencionados são aqueles que lidam diretamente com os dados pessoais, mas não são os únicos protagonistas da legislação. Silva (2020, p. 17) aponta ainda a figura do encarregado (ou DPO: *Data Protection Officer*), que também deve ser uma pessoa natural – indicada pelo controlador – que atuará como responsável pela comunicação entre o próprio controlador, os titulares e a Autoridade Nacional de Proteção de Dados. O DPO deve orientar o controlador a respeito de quais são as melhores práticas quanto ao tratamento dos dados em sua posse. O encarregado é definido no inciso VIII e possui suas atividades listadas no art. 41, §2º, da legislação e englobam: 1) a aceitação de reclamações e comunicações dos titulares, devendo prestar esclarecimentos; 2) o recebimento de comunicações da autoridade nacional; 3) a orientação dos funcionários e contratados da entidade no que diz respeito às práticas que devem ser adotadas para a proteção de dados; e 4) a execução de outras atribuições que são determinadas pelo controlador ou estabelecidas em outras normas (BRASIL, 2018).

Por fim, a Autoridade Nacional de Proteção de Dados (ou ANPD) foi devidamente incluída na LGPD por alteração feita pela lei 13.853/19. Trata-se de um órgão da Administração Pública Federal, integrante na Presidência da República. Sua definição se encontra no art. 55-A e sua composição no art. 55-C (BRASIL, 2018). Sendo um recente órgão, será responsável pela implementação e fiscalização do cumprimento da lei, podendo aplicar sanções em caso de ilegalidades, o que será feito por meio de processo administrativo (SILVA, p. 17).

Uma vez definidos os atores da LGPD, o trabalho buscará apontar as eventuais ilegalidades e responsabilidades pelo uso indevido de dados pessoais para fins eleitorais, o que contará também com uma análise de instrumentos normativos eleitorais.

4 O TRATAMENTO DE DADOS SENSÍVEIS PARA FINS ELEITORAIS

Apesar da Lei Geral de Proteção de Dados ter sido pensada no contexto da regulamentação geral de dados, certamente se trata de uma legislação de análise obrigatória no assunto do aumento da manipulação da opinião pública por meio de redes sociais digitais. Muito embora essas redes (como *Facebook* e *Twitter*) possam parecer, em um primeiro momento, verdadeiros instrumentos de participação popular na democracia, também vem sendo utilizados como um palco para a violação de direitos.

Isso permite a conclusão de que a mesma tecnologia que permitiria a facilitação do alcance ao conhecimento também permite a difusão de conteúdo inverídico. Em períodos de alta polarização política, a informação disseminada por empresas que fazem uso desses dados tem sido utilizada para a formação de opinião de usuários de certas mídias, o que possui direta implicação no próprio processo eleitoral.

A LGPD, entretanto, não pode ser lida de forma isolada, haja vista a existência de instrumentos normativos no campo eleitoral que têm sido constantemente atualizados no intuito de coibir práticas de ilícitos eleitorais na seara virtual, conforme será demonstrado no tópico seguinte.

4.1 A REGULAMENTAÇÃO DA REDE POR MEIO DAS NORMAS ELEITORAIS

A chamada Lei das Eleições (lei 9.504/97) surgiu em um momento no país no qual a rede mundial de computadores ainda não era muito difundida. Entretanto, por meio de atualizações, a legislação passou a tratar do uso de aparatos tecnológicos de comunicação e informação (para além do rádio e TV) para fins eleitorais.

Certos dispositivos da mencionada legislação se referem diretamente ao envio de conteúdo por mensagens eletrônicas. Eles se encontram nos arts. 57-A a 57-J, alguns dos quais devem ser analisados no presente tópico. Vale ressaltar que tais artigos foram incluídos por meio de legislações posteriores, quais sejam: a lei 12.034/2009; a lei 12.891/13; e lei 13.488/17 (BRASIL, 1997).

O primeiro dispositivo a ser mencionado é o art. 57-B, que trata da propaganda eleitoral na *internet*. Observa-se, inicialmente, que essa modalidade de publicidade não é vedada pela legislação eleitoral, entretanto, ela não pode ocorrer de maneira livre. Os incisos do dispositivo citado dispõem a respeito das possibilidades e limitações à conduta abordada.

Os incisos I e II tratam da propaganda em páginas específicas, como aquelas relacionadas ao candidato e ao seu partido. O inciso IV, por sua vez, trata da propaganda que é veiculada, em regra, em *blogs* e redes sociais vinculadas aos candidatos, partidos ou coligações. O que merece maior destaque é a possibilidade do inciso III, que diz respeito à publicidade por meio de mensagem eletrônica enviada a endereços cadastrados gratuitamente pelo candidato, partido ou coligação (BRASIL, 1997).

Trata-se de evidente possibilidade de tratamento de dados pessoais. Pode-se, nesse caso, ocorrer o envio de mensagens a determinados grupos. Há duas considerações relevantes para esse inciso: A) o tratamento de dados nesse caso deve obedecer aos princípios e normas relacionados à LGPD (já mencionados); B) o envio não pode ser utilizado para fins ilícitos, incluindo ilícitos eleitorais, tais como o delito de divulgação de fatos inverídicos previsto no art. 323, do Código Eleitoral (BRASIL, 1965).

Outro dispositivo de considerável interesse é o art. 57-C, incluído pela lei 13.488/17. Muito embora em sua primeira parte aponte para a impossibilidade de veiculação de propaganda eleitoral paga na *internet*, torna lícito o impulsionamento de conteúdo, desde que, conforme a letra da lei: "[...] identificado de forma inequívoca como tal e contratado exclusivamente por partidos, coligações e candidatos e seus representantes" (BRASIL, 1997).

Menciona-se, ainda, o disposto no art. 57-D, da mesma legislação. O artigo menciona a livre manifestação do pensamento consagrada originalmente na Constituição Federal em seu art. 5º, IV (BRASIL, 1988). Apesar de não abordar necessariamente o tratamento de dados de eleitores eventuais, assegura o direito de resposta às afirmações feitas na rede mundial de computadores e também permite que o ofendido solicite a retirada de publicação que contenha agressão ou ataques, conforme o §3º (BRASIL, 1997).

Por fim, é preciso ressaltar o que dispõem os arts. 57-E e 57-G. Enquanto o primeiro veda a doação ou cessão de cadastro eletrônico em favor de candidatos, partidos ou coligações (o que inclui a venda de cadastro de endereços eletrônicos), o último estabelece que as mensagens eletrônicas enviadas por candidato, partido ou coligação

devem dispor de ferramentas capazes de realizar o descadastramento do destinatário, caso este assim o deseje, no prazo de quarenta e oito horas (BRASIL, 1997).

É importante notar que a Lei das Eleições não aborda de maneira pormenorizada o processo em geral do tratamento dos dados pessoais ou sensíveis no contexto das campanhas eleitorais, muito embora, conforme demonstrado, permita tal tratamento em determinados casos. É imperativo, portanto, que a legislação eleitoral e a LGPD sejam igualmente observadas para que sejam evitados abusos durante a veiculação de propaganda eleitoral.

5 CONCLUSÃO

Percebe-se, diante do que foi exposto, que a Lei das Eleições e a Lei Geral de Proteção de Dados não foram pensadas no tratamento e regulamento da disseminação de desinformação. Contudo, por tratarem e, de certa maneira, se complementarem no que diz respeito à proteção de dados pessoais, são marcos importantíssimos para a compreensão dos limites que um dado pessoal ou sensível poderá ser utilizado.

Conforme abordado em tópico próprio, a LGPD tem como um de seus marcos o consentimento do titular para a realização de qualquer tratamento de dados. É preciso que esse consentimento ocorra de maneira expressa, o que veda a aquisição de dados de maneira indevida, tal como ocorreu no uso fraudulento de informações do caso *Yacows* e *Cambridge Analytica*.

É importante também fazer menção ao que consta no Marco Civil da Internet (BRASIL, 2014), que já mencionada o direito ao consentimento livre, expresso e informado (art. 7º) na ocorrência de fornecimento de dados pessoais a terceiros.

Nota-se também uma necessidade de cooperação entre o próprio Tribunal Superior Eleitoral e a Autoridade Nacional de Proteção de dados no intuito de haver um maior controle do uso de informações para fins políticos.

Dessa maneira, sabe-se que não são poucos os candidatos e partidos que contratam empresas de *marketing* para a realização do gerenciamento de sua campanha eleitoral. Conforme estipulado, é preciso que sejam definidos, conforme a estrutura da LGPD, a posição e o protagonismo de cada um desses atores no contexto do uso dos dados de eleitores.

Assim, um partido político ou candidato pode muito bem atuar na pessoa do controlador, decidindo pelo tratamento dos dados (conforme a lei estabelece em seu art.

5º, VI). A empresa que efetivamente realiza o tratamento atua, dessa forma, como operador (Art. 5º, VII), desde que essa atuação ocorra em nome do controlador previamente mencionado.

Importa ressaltar que, conforme estabelece o art. 42, da própria LGPD (BRASIL, 2018), tanto o controlador quanto o operador dos dados são responsáveis pela reparação dos danos causados, sejam eles de cunho patrimonial, moral, individual ou coletivo.

De maneira mais específica, nos termos do art. 42, §1º (BRASIL, 2018), a responsabilidade do operador será solidária no que diz respeito aos danos causados pelo tratamento dos dados quando houver o descumprimento de obrigações da LGPD ou quando as instruções lícitas do uso de dados não forem seguidas. Por sua vez, o controlador que esteja diretamente envolvido no tratamento no qual ocorrer algum dano ao titular dos dados responderá de forma solidária.

Tanto os controladores quanto os operadores não responsabilizados apenas nas hipóteses previstas no art. 43, quando provarem (BRASIL, 2018):

> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

É também preciso identificar o encarrego que foi indicado (art. 5º, VIII), além de se saber exatamente que dados serão utilizados e para quais fins. Essa transparência é fundamental e também deve ser acompanhada de relatório de impacto à proteção de dados pelo controlador (art. 5º, XVII), como uma necessária garantia de proteção.

Nota-se, por fim, que muito embora não haja uma legislação específica para o caso de utilização ilícita de dados para disseminação de *fake news*, o que pode se mostrar necessário, a legislação brasileira, ao seguir as diretrizes internacionais, tem buscado trazer um maior rigor no uso e tratamento de dados, notadamente aqueles coletados na rede mundial de computadores.

6 REFERÊNCIAS

ARNAUDO, Dan. **Computational Propaganda in Brazil**: Social Bots during Elections. Samuel Woolley and Philip N. Howard, Working Paper 2017.8. Oxford, UK: Project on

Computational Propaganda. Disponível em: < https://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Brazil-1.pdf>. Acesso em: 16 jul. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 jul. 2021.

BRASIL**. Lei 4.737, de 15 de julho de 1965**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4737compilado.htm. Acesso em: 16 jul. 2021.

BRASIL. **Lei nº. 9.504, de 30 de setembro de 1997**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 29 jun. 2021.

BRASIL. **Lei nº. 12.965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 jul. 2021.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 jul. 2021.

BRASIL. Superior Tribunal Eleitoral. **Ação de Investigação Judicial Eleitoral nº. 11.527**: Decisão. Relator: Min. Jorge Mussi. Publicado em: 19 out. 2018. Disponível em: https://www.conjur.com.br/dl/decisao-mussi-pt-bolsonaro-esquema.pdf. Acesso em: 29 jun. 2021.

BRASIL. Superior Tribunal Eleitoral. **Ação de Investigação Judicial Eleitoral nº. 11.527**: Petição inicial. Relator: Min. Jorge Mussi. Publicado em: 19 out. 2018. Disponível em: https://static.poder360.com.br/2018/12/acao-0601968-80-2018-6-00-0000-protocolo.pdf. Acesso em: 29 jun. 2021.

COTS, Márcio; Oliveira, Ricardo. **Lei Geral de Proteção de dados pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

FRIAS FILHO, Otávio. O que é falso sobre fake news. *In*: **Revista USP**. São Paulo, n. 116, p. 29-44, jan., fev., mar., 2018. Disponível em: https://jornal.usp.br/wp-content/uploads/4-Otavio-Frias.pdf. Acesso em: 06 jul. 2021.

MELLO, Patrícia Campos. Empresários bancam campanha contra o PT pelo WhatsApp. *In*: **Folha de São Paulo**. 18 out. 2018. Disponível em: https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml. Acesso em: 29 jun. 2018.

MOREIRA JÚNIOR, Ronaldo Félix; LOPES, Jaime. O poder dos fluxos de informação: análise sociológica do exercício político pela rede mundial de

computadores. *In*: **Revista da Semana Discente de Sociologia Política do Instituto Universitário de Pesquisas do Rio de Janeiro**, v. 2, p. 33-35, 2019.

OLIVEIRA, Bruno. Como eram feitas as análises do Cambridge Analytica. *In*: **Medium**. Disponível em: https://medium.com/internet-das-coisas/tic-02-como-eram-feitas-as-análises-do-cambridge-analytica-42235dea12d5. Acesso em: 11. out. 2020.

SILVA, Daniel Cavalcante. **Manual da Lei Geral de Proteção de Dados para Instituições de Ensino**. Brasília: Covac, 2020.

SOARES, Ana Thereza Nogueira. Epistemologia, métodos e teorias da comunicação na era do Big Data: panorama crítico da pesquisa em mídias sociais. *In*: **Comunicação e Sociedade**, vol. 33, 2018, pp. 151 – 166.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 06 jul. 2021.