

O Enfrentamento Das *Fake News* No Processo Eleitoral A Partir Das Leis De Proteção De Dados

Outros temas relacionados a administração da justiça

Caroline Coradassi Almeida Santos (Universidade Positivo); Ana Claudia de Batista Fernandes (Universidade Positivo)

RESUMO

É evidente que o planejamento, a organização e a execução de uma eleição em um país envolvem desafios e responsabilidades, como política de privacidade de dados, sistemas seguros contra ataques cibernéticos, monitoramento de campanhas e veiculação de *fake news*. Para reduzir tais inseguranças, com a vigência da *General Data Protection Regulation (GDPR)*, foi promulgada a Lei Geral de Proteção de Dados (LGPD), visando à adequação do contexto normativo à globalização das novas tecnologias e serviços pautados no uso da internet para suas operações. Assim, o estudo tem por objetivo discutir aspectos das legislações de proteção de dados que viabilizem o combate às *fake news* no processo eleitoral. De forma a compreender quais os aspectos da lei favorecem a gestão dos dados no processo eleitoral, propõe-se relacionar, por meio de pilares devidamente conceituados, um conjunto de fatores que possibilitam a adoção de medidas legais e preventivas, para conferir segurança jurídica ao processo eleitoral em meio ao cenário das *fake news*. Trata-se de um ensaio teórico de abordagem qualitativa e natureza descritiva, com intenção em avançar no entendimento legal e de governança, por meio dos pilares norteadores: a) ético; b) legal; c) cultural; d) tecnológico; e) social; f) econômico; e g) estratégico, a fim de apresentar um modelo que favoreça a gestão do processo eleitoral no que tange às *fake news*, trazendo maior credibilidade aos partidos políticos e confiança pela sociedade no uso dos seus dados.

Palavras-Chave: Processo eleitoral; *fake news*; lei de proteção de dados; governança.

Introdução

Os processos eleitorais democráticos dependem da cultura e das tecnologias disponíveis e temos acompanhado essa mutação de forma enérgica a nível mundial (Bennett & Livingston, 2018). As tecnologias modernas nos sistemas de gestão eleitoral geraram interesse e preocupações entre eleitores, instituições, organizações, profissionais do sistema eleitoral e políticos. É evidente que o planejamento, a organização e a execução de uma eleição em um país envolvem desafios e responsabilidades, entre os quais política de privacidade de dados, sistemas seguros contra ataques cibernéticos, monitoramento de campanhas e possível uso de *fake news*, entre outros.

No uso da tecnologia, tem-se dado um destaque especial nas últimas eleições para o uso das redes sociais e, também, do WhatsApp, que de certo modo estão abarcados e enquadrados nas normas de proteção da LGPD (Tanner, Fishman, Horton & Sheth, 2017). Quando se trata desse assunto, a Resolução número 23.610/2019 do Tribunal Superior Eleitoral (TSE) define, por exemplo, no artigo 41 que, no que couber a lei geral de proteção de dados, será aplicável às normas, às regras nas eleições, ou seja, o envio de mensagens de WhatsApp ou até de SMS,

principalmente, sem autorização, é uma das principais questões a serem analisadas neste contexto de proteção de dados e de aplicação da LGPD.

Para reduzir as incertezas quanto à proteção de dados, em 25 de maio de 2018, entrou em vigor a GDPR que avançou para além das fronteiras europeias, inspirando iniciativas nacionais na busca da proteção de dados pessoais, tanto na esfera pública como na esfera privada, passíveis de identificação no ciberespaço. Após a vigência da GDPR, foi promulgada a LGPD, Lei Ordinária nº. 13.709/2018, visando à adequação do contexto normativo à globalização das novas tecnologias e serviços pautados no uso da internet para suas operações.

No cenário nacional, os direitos e garantias fundamentais preconizadas na Constituição da República Federativa do Brasil (CRFB), em especial, o direito à privacidade, intimidade e liberdade de expressão, chamam a atenção aos impactos ocasionados pela disseminação das *fake news* no processo eleitoral e a necessidade da proteção dos dados.

Em que pese inexistir no ordenamento jurídico brasileiro regulamentação normativa acerca das *fake news*, legislações eleitorais e de matérias esparsas, apresentam dispositivos legais que remetem a circulação de desinformação, dentre eles, o artigo 58 da Lei das Eleições (Lei n. 9.504/1997), que versa sobre o direito de resposta a candidato, partido ou coligações políticas, no tocante à propaganda política e a vedação da exposição de fato sabidamente inverídico.

A consciência dos próprios partidos políticos em relação à proteção de dados é algo que vem sendo questionado, considerando que o sistema jurídico já possui e ressalta a necessidade de proteção de dados mediante a LGPD, então, a dúvida está no preparo e adequação dos envolvidos no processo eleitoral para atender aos requisitos da lei. Portanto, o objetivo do estudo consiste em analisar aspectos das legislações de proteção de dados que viabilizem o combate às *fake news* no processo eleitoral.

Muitos casos envolvendo o uso de dados pessoais por empresas terceirizadas, contratadas por partidos políticos, trabalham no refinamento de informações sobre as pessoas e acabam tendo acesso não só aos gostos, como também, técnicas de *target* e *profile*, mas inclusive aos medos, com facilidade de manipulação de seus interesses. Por isso, a LGPD pode auxiliar na redução de problemas de desinformação, não sendo a única ferramenta para combater esse cenário, permitindo aliar a educação digital às demais ferramentas de controle em relação à veiculação de *fake news* e, conseqüentemente, propagação da desinformação.

A relação com as informações, tanto ao acesso quanto ao repasse, por parte da população deve ser consciente, ou seja, as pessoas antes de encaminhar uma mensagem pelo WhatsApp, por exemplo, ou qualquer rede social não devem apenas ler a manchete, mas a matéria na íntegra, inclusive, recorrendo aos instrumentos de checagem dos fatos, o que fortalece o combate às *fake news*, e atua como forma de medida educativa (Tanner *et al*, 2017). O comportamento ético é um importante fator na conscientização do usuário no uso das redes no Brasil e os fatores culturais se somam a fatores éticos e aos aspectos regulatórios da LGPD.

Mediante ao exposto, o estudo tem por objetivo discutir aspectos das legislações de proteção de dados que viabilizem o combate às *fake news* no processo eleitoral. De forma a compreender quais os aspectos da lei favorecem a gestão dos dados no processo eleitoral, propõe-se relacionar, por meio de pilares devidamente conceituados, um conjunto de fatores que possibilitam a adoção de medidas legais e preventivas, para conferir segurança jurídica ao processo eleitoral em meio ao cenário das *fake news*.

Trata-se de um ensaio teórico, de abordagem qualitativa e natureza descritiva, com intenção em avançar no entendimento legal e de governança, por meio dos pilares norteadores: a) ético; b) legal; c) cultural; d) tecnológico; e) social; f) econômico; e g) estratégico, a fim de

apresentar um modelo que favoreça a gestão do processo eleitoral no que tange às *fake news*, trazendo maior credibilidade aos partidos políticos e confiança pela sociedade no uso dos seus dados.

Leis internacionais e legislação sobre proteção de dados

Com a revolução tecnológica iniciada em 1990, a informação assumiu papel de grande relevância, sobretudo, quando se fala em política, tecnologia e as novas tecnologias. Sabe-se que a informação cresce a nível exponencial, na qualidade e na celeridade de seu acesso e compartilhamento. Com isso, formou-se um relacionamento social no meio digital, pelo qual é possível transmitir informações, independente do espaço físico e, como exemplo, pode-se citar a criação de movimentos e protestos por meio das redes sociais.

Isso é o que se chama de Sociedade da Informação, vez que “a informação avoca um papel central e adjetivante da sociedade: sociedade da informação” (Bioni, 2019, p. 34). De fato, a organização da sociedade leva em consideração a informação gerada pelos mecanismos de comunicação e sistemas ligados à informática, a coleta, uso e compartilhamento de dados e, no que diz respeito ao período eleitoral, tal mecanismo se torna valioso para o estudo de perfil e tendências de grupos eleitorais e, conseqüentemente, confecção de *fake news* para tumultuar as campanhas e agir (des)favoravelmente a determinado candidato, partido ou coligação.

De acordo com Doneda (2011, p. 91), “o dado apresenta conotação um pouco mais primitiva e fragmentada”. É o que ele chama de “pré-informação”, porquanto se apresenta anteriormente à interpretação e ao processo de elaboração do saber.

Por sua vez, a informação “alude a algo além da representação contida no dado, chegando ao limiar da cognição” (Doneda, 2011, p. 91). Segundo o autor, “na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega também um sentido instrumental, no sentido da redução de um estado de incerteza”. Simplificadamente, dados são aqueles que descrevem e qualificam determinada coisa, enquanto a informação representa o significado dos dados combinados e a posterior transmissão de seu teor, formador do conhecimento, que, por sua vez, constitui informação organizada e aplicada ao respectivo contexto. Com isso, observa-se a necessidade de assegurar, dentre outros, os princípios da privacidade e da proteção dos dados.

Para reduzir as incertezas quanto à proteção de dados, em 25 de maio de 2018, entrou em vigor a GDPR, ou, em português, Regulamento Geral de Proteção de Dados, que avançou para além das fronteiras europeias, inspirando iniciativas de nacionais na busca da proteção de dados pessoais, tanto na esfera pública como na esfera privada, passíveis de identificação no ciberespaço.

De fato, importante ressaltar que a preocupação no cenário brasileiro já se encontrava cunhada desde o Marco Civil da Internet (Lei nº. 12.965 de 23 de abril de 2014), com a previsão da proteção de dados pessoais dentre os seus princípios, como uma lacuna normativa, em razão da ausência de regulamentação normativa correspondente para perfectibilizar a previsão legal. Dentre os princípios elencados, o Marco Civil da Internet dispõe, também, da proteção da privacidade, garantia da liberdade de expressão, funcionalidade e neutralidade de rede, segurança e boas práticas no ambiente cibernético, responsabilização dos agentes, dentre outros (artigo 3º da Lei nº. 12.965/2014).

Não se pode olvidar que, com a vigência da GDPR e os escândalos internacionais envolvendo a *Cambridge Analytica* e a manipulação dos dados pessoais de milhões de pessoas e a indevida utilização durante as eleições americanas e, também, a votação do *British exit* - ou

Brexit -, no Reino Unido, com repercussão global, contribuíram para a rápida adequação normativa no Brasil.

Assim, a Lei Geral de Proteção de Dados (LGPD), Lei Ordinária nº. 13.709, promulgada em 14 de agosto de 2018, pelo Presidente da República, à época, Michel Temer, originou-se de maneira conturbada, porquanto criada a partir do Projeto de Lei da Câmara nº. 53/2018 e aprovada, com unanimidade, pelo Plenário do Senado, no mês de julho de 2018, devido a urgência do tema, isto é, adequação do contexto normativo à globalização das novas tecnologias e serviços pautados no uso da internet para suas operações.

Ocorre que a LGPD foi alterada pela Medida Provisória nº. 869/2018 e pela Lei nº. 13.853/2019, sofrendo longo período de *vacatio legis*, com vigência prorrogada em virtude da Medida Provisória nº. 959/2020, tendo sido finalmente sancionada pelo Presidente da República, com início de sua vigência em 18 de setembro de 2020.

Neste sentido, importante destacar que o artigo 1º da LGPD tem por finalidade a proteção dos direitos fundamentais da liberdade, privacidade e livre desenvolvimento da pessoa natural, especialmente, no que toca à importância do tratamento de dados pessoais, no ambiente digital, por pessoas físicas ou jurídicas e estas, de direito público ou privado. Destaca-se, ainda, que o tratamento dos dados deve se atentar ao objetivo e aos fundamentos delineados pela legislação, porém, desde que a operação tenha se dado em território nacional (artigo 3º da LGPD), com exceção àquele:

provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (inciso IV do artigo 4º da LGPD).

Denota-se que a legislação apresenta a conceituação sobre o que se compreende por dados, de modo amplo, aplicabilidades no meio virtual e, também, de agentes envolvidos na proteção de dados. A inquietação do presente estudo se relaciona ao tema afeto aos dados pessoais, especialmente, os dados pessoais sensíveis e anonimizados, porquanto, consoante a própria legislação ensina, tais dados são todas as informações reunidas que possibilitam não somente a identificação geral, mas de determinada pessoa.

Os dados sensíveis extrapolam qualquer limitação, pois reúne um conjunto de fatores relacionados à intimidade individual e, portanto, passíveis de discriminação, caso sejam publicizados. Ou seja, “quando se pensa em dados que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade” (Bioni, 2019, p. 118).

Paralelamente, encontra-se o conceito de dado anonimizado e que, igualmente, interfere esfera individual da pessoa natural. Neste sentido, importante frisar que “algoritmos que mineram dados anonimizados podem esconder práticas discriminatórias em prejuízo de uma coletividade e de pessoas singulares” (Bioni, 2019, p. 112-113). Com a migração das relações pessoais, profissionais, atividades ligadas ao exercício da cidadania e democracia do meio físico ao meio digital, resta presente a participação do interesse público, o qual deve regular as relações no ambiente cibernético, notadamente, diante da necessidade de garantia de direitos fundamentais, previstos constitucionalmente, a exemplo, defesa à privacidade, intimidade e liberdade de expressão.

A LGPD, portanto, enaltece a necessidade de proteção de dados pessoais, em especial, por intermédio da adoção de medidas preventivas, exigindo uma ação multidisciplinar dos atores indicados na legislação, tanto na iniciativa privada, como na pública, no tocante à gestão e governança de dados pessoais, nos moldes do artigo 6º, inciso VIII, por exemplo.

Na Europa existem estudos e diretrizes sobre como aplicar o GDPR em campanhas eleitorais, no entanto o Brasil ainda está começando a entender a importância desse complexo problema, o processo de adequação é lento, robusto e envolve diversas áreas e profissionais. Assim, ter o esforço e entender como será a aplicação direta da LGPD nos processos eleitorais, campanhas e, também, os partidos políticos individualmente possibilita a compreensão não só da proteção de dados pessoais, mas os direitos digitais como um todo.

Importante ressaltar que a LGPD não dispõe necessariamente sobre *fake news* e formas de tratamento de tal problema. Ambos não estão diretamente relacionados, mas indiretamente. Nota-se maior atenção às mídias digitais do que às mídias tradicionais e essa alteração repercute também na disseminação de *fake news*, pois através de uma base de dados dos eleitores é possível a mineração dos dados para a disseminação *fake news*.

O TSE, por exemplo, como instituição, possui papel fundamental na adequação dos processos, *compliance* e prevenção de riscos, ou seja, há uma relação direta entre campanhas eleitorais e adequação à LGPD e, embora o TSE ainda esteja tímido como instituição em alinhar estratégias, ferramentas e métodos de atuação.

Por fim, importante ressaltar que a adoção da LGPD no Brasil visou, além de cunhar uma regulamentação normativa no país, adequar-se aos requisitos para o ingresso na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), manifestada pelo Governo Federal anteriormente à vigência da LGPD, já que a ausência de tal legislação foi considerada uma lacuna e obstáculo a esse intento, notadamente, porque tal organização “exige, como boa prática, a regulamentação de uso de dados pessoais, assim como um órgão supervisor independente e autônomo” (Observatório Privacidade, 2018).

A preocupação com as normas de proteção de dados pessoais pela OCDE e no âmbito internacional é latente desde a década de 1980, de modo que a LGPD, na seara nacional, externaliza essa convergência regulatória para a proteção dos dados pessoais e, sobretudo, da movimentação e fluxo internacional de dados (Mendes & Bioni, 2019, p. 161).

Portanto, observa-se que a LGPD se afigura a primeira legislação brasileira a tratar da proteção dos dados no país, com a apresentação de conceitos genéricos e estabelecimento de princípios norteadores de tal disciplina e técnicas de segurança da informação. Ademais, os temas relativos à mencionada legislação se encontram em consonância com os princípios que regem a matéria em ordem transnacional, a exemplo da GDPR e, conseqüentemente, abarcados na recomendação da OCDE.

O tratamento legal das *fake news* no processo eleitoral

Na tradução literal, *fake news* significa notícia falsa e, ainda que a expressão falsa desperte interesse, notadamente, em virtude da discussão acerca da pós-verdade e do que é considerado mentira, por exemplo. No entanto, é importante concentrar-se rapidamente no entendimento do conceito do que é notícia. A notícia, por sua vez, é a expressão da verdade obtida no momento, sem olvidar da possibilidade de retratação e retificação posterior. Ou seja, se a notícia pressupõe que seja verdadeira, ela não pode ser falsa.

De acordo com Wardle (2017), existem sete tipos distintos de *fake news* que podem ser identificados nas plataformas digitais, são eles: sátira ou paródia, conteúdo enganoso, falso

contexto, falsa conexão, conteúdo impostor, conteúdo manipulado e conteúdo fabricado (Wardle, 2017). Por isso, talvez as melhores expressões empregadas sejam desinformação ou notícia fraudulenta (Rais, 2018).

Em relação ao adjetivo falso empregado nas “notícias falsas”, para analisar a veracidade de um fato divulgado, é necessário analisar o seu contexto, vez que o teor da informação difundida, para ser verdadeira e, portanto, notícia, deve estar associada ao contexto. Assim, o termo falso pode ser caracterizado por sua inclusão no contexto desassociado de um fato informativo e, da mesma forma, o inverso, por exemplo, sem considerar conteúdos fraudulentos e dotados de desinformação, fabricados para gerar clamor social, discursos de ódio e violência digital.

Os mecanismos de disseminação, com as novas tecnologias, ocorrem majoritariamente nas redes sociais, onde são amplamente difundidos e compartilhados, sem a devida observação acerca da veracidade dos fatos pelos usuários.

A incapacidade de interpretar conteúdos ou a confiabilidade cega nas chamadas “notícias” circuladas nas mídias sociais, sem qualquer exercício de checagem dos fatos, permite influenciar a opinião pública sobre temas importantes, em especial, ligados à cidadania e processo democrático. Nas palavras de Allcott e Gentzkow (2017, p. 213, tradução nossa) “fake news são notícias verificáveis e intencionalmente falsas e que podem enganar os leitores”.

Existe um impacto pernicioso porque afeta a capacidade das pessoas de fazer um voto consciente e embasado em informações reais (Cheeseman, Lynch & Willis, 2018). A decisão de voto se é feita com base em informações falsificadas, fraudulentas, torna-se prejudicial e compromete a lisura do processo eleitoral e do processo democrático, pois as eleições representam a base de escolha de governantes, sobretudo da continuidade da democracia. Como nos Estados Unidos, França, Espanha e no Brasil, são exemplos de democracias que assistiram as notícias falsas se espalharem durante os processos eleitorais.

O problema das *fake news* acabou nivelando a democracia como um todo, democracias já estabelecidas e as recentes, como o Brasil, se viram abaladas pelo fenômeno das *fake news*, ou seja, um problema transversal (Jang & Kim, 2018). A desinformação com a intenção de prejudicar o contexto eleitoral.

No processo eleitoral brasileiro, o qual é regido pelo Código Eleitoral e Lei das Eleições, com poder normativo, isto é, dotado de função típica para a edição de resoluções pelo TSE, nos termos do artigo 105 da Lei 9.504/97, bem como função julgadora para a resolução de controvérsias eleitorais, tais como as propagandas eleitorais.

Com a migração das propagandas eleitorais para o meio digital, o enfrentamento de questões normativas e jurisdicionais pela Justiça Eleitoral passou a ser mais desafiador, notadamente, porque antes da era da internet, tais conteúdos eram predominantes em veículos de imprensa vistos como tradicionais, como rádio e televisão.

Ainda que a Lei das Eleições estabeleça a permissão para a veiculação de propaganda eleitoral até o dia 15 de agosto do ano da eleição (artigo 36), sabe-se que a *internet* viabiliza a troca de informações com maior rapidez e de forma instantânea entre os usuários. Ademais, é comum que os próprios candidatos ou assessoria de comunicação dos partidos e coligações se utilizem de tal facilidade para promover campanhas eleitorais, ou que candidatos, a qualquer tempo, circule nas redes sociais informações próprias ou de concorrentes, valendo-se, assim, da propaganda positiva e/ou negativa (Borba, 2015), para atingir aos milhões de cidadãos e eleitores em potencial, com acesso à internet e, assim, exercer influência na escolha e decisão do eleitor.

Por propaganda eleitoral positiva, entende-se que são aquelas que “fazem referência à autopromoção dos candidatos, como a apresentação de propostas, o currículo administrativo e a biografia política” (Borba, 2015, p. 280). De outro lado, a propaganda eleitoral negativa é entendida como “qualquer crítica direcionada por um candidato aos seus adversários” (Borba, 2015, p. 280).

E, a propósito, destaca-se que, de acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), em Pesquisa Nacional por Amostra de Domicílios (PNAD) no ano 2019, “82,7% dos domicílios nacionais possuem acesso à internet, um aumento de 3,6 pontos percentuais em relação a 2018” (Governo Federal, 2021).

Assim, diante do novo cenário apresentado a partir da era da *internet*, novas regras foram adotadas pela Justiça Eleitoral, para a interromper a circulação de propagandas eleitorais irregulares e, conseqüentemente, conteúdo eivado de desinformação e práticas de *fake news* durante o período eleitoral. Como resultado, a Lei nº. 13.488/2017 alterou a Lei das Eleições para incluir o capítulo referente à propaganda na internet, do artigo 57-A ao 57-J.

A Resolução nº. 23.610, de 18 de dezembro de 2019 do Tribunal Superior Eleitoral, menciona a lei geral de dados especificamente com relação à propaganda eleitoral na *internet*. Ao artigo 28 desta resolução, destaca:

Art. 28. A propaganda eleitoral na internet poderá ser realizada nas seguintes formas (Lei nº 9.504/1997, art. 57-B, I a IV):

- I - em sítio do candidato, com endereço eletrônico comunicado à Justiça Eleitoral e hospedado, direta ou indiretamente, em provedor de aplicação de internet estabelecido no país;
- II - em sítio do partido político ou da coligação, com endereço eletrônico comunicado à Justiça Eleitoral e hospedado, direta ou indiretamente, em provedor de aplicação de internet estabelecido no país;
- III - por meio de mensagem eletrônica para endereços cadastrados gratuitamente pelo candidato, pelo partido político ou pela coligação, observadas as disposições da Lei Geral de Proteção de Dados quanto ao consentimento do titular;
- IV - por meio de blogs, redes sociais, sítios de mensagens instantâneas e aplicações de internet assemelhadas, dentre as quais aplicativos de mensagens instantâneas, cujo conteúdo seja gerado ou editado por:
 - a) candidatos, partidos políticos ou coligações, desde que não contratem disparo em massa de conteúdo (Lei nº 9.504/1997, art. 57-J); ou
 - b) qualquer pessoa natural, vedada a contratação de impulsionamento e de disparo em massa de conteúdo (Lei nº 9.504/1997, art. 57-J).

Sabe-se que a liberdade de expressão e o acesso à informação são fatores de sustentação de um Estado democrático de direito.

Assim, a regulamentação acerca da veiculação de propaganda eleitoral, em especial, aquelas de conteúdos irregulares ou mesmo de conteúdo eivado de desinformação, pelo Poder Legislativo ou pela Justiça Eleitoral, por meio de resoluções, torna-se demasiadamente necessária, especialmente, nos períodos eleitorais, a fim de evitar a propagação de *fake news* e gerar influência na tomada de decisão por parte de eleitores, em decorrência do uso indevido ou irregulares de dados pessoais, sem incorrer na supressão dos princípios que garantem a livre expressão e informação.

4. As leis de proteção de dados como mecanismo de enfrentamento às *fake news*

Muitos casos envolvendo o uso de dados pessoais por empresas terceirizadas contratadas por partidos políticos trabalham no refinamento de informações sobre as pessoas e acabam tendo acesso não só aos gostos das pessoas com técnicas de *target* e *profile*, mas inclusive aos medos, e é fácil manipular pessoas através dos medos, por isso a LGPD pode auxiliar na redução de problemas de desinformação, mas ela não é a única ferramenta para combater esse cenário e, por isso, a educação digital se soma às demais ferramentas de controle de desinformação.

A relação com às informações, tanto ao acesso quanto ao repasse, por parte da população, deve ser consciente, ou seja, as pessoas antes de passar uma mensagem pelo *WhatsApp*, por exemplo, ou qualquer rede social não devem apenas ler a manchete, mas a matéria na íntegra, além de checar a fonte (Tanner et al, 2017). Nesse pilar cultural, o comportamento ético é um importante fator na conscientização do usuário no uso das redes no Brasil. Os fatores culturais se somam a fatores éticos e aos aspectos regulatórios da LGPD.

Resolver problemas complexos como a desinformação envolve uma série de recursos, instituições e profissionais. Por isso a solução não é simples e depende de mudanças estruturais e sociais, assim como há expectativa em acoplar na proteção de dados a possibilidade de resolução do problema, embora seja notório que tem uma interface interessante, mas não vai resolver todo o problema (Marwick, 2018), a começar pela falta de técnica no tratamento conceitual e prático, pois ainda há divergências sobre o que se configura como uma notícia falsa. Além disso, envolve diversos temas e a própria terminologia que pode afetar desde instituições, organizações, candidatos e eleitores, também a liberdade de expressão e acesso à informação dependendo como esse conteúdo será moderado (Mckelvey, Ordeshook & Mckelvey, 1986).

Tem-se dado um destaque especial nas últimas eleições para o uso das redes sociais, especialmente, ao uso do *WhatsApp*, deparando-se com as normas de proteção da LGPD (Tanner et al, 2017). Quando se trata desse assunto, a Resolução número 23.610/ 2019 define, no artigo 41, por exemplo, que no que couber a lei geral de proteção de dados será aplicável às normas, às regras nas eleições. Isso quer dizer que o envio de mensagens de *WhatsApp* ou até de SMS, principalmente, sem autorização é uma das principais questões a serem analisadas neste contexto de proteção de dados e de aplicação da LGPD.

Para as eleições, posto que as resoluções do TSE têm caráter permanente e uma das previsões, inclusive, é de que este envio não autorizado de SMS ou de *WhatsApp* podem gerar multas, caso tenha havido um disparo em massa de maneira indevida o valor dessas multas pelo que está previsto nas resoluções é destinado ao fundo partidário e o dinheiro é revertido em favor dos próprios partidos. Os candidatos e partidos políticos podem ajuizar ações e o eleitor pode denunciar ao Ministério Público e à Justiça Federal pelos meios digitais, caso constate o uso de irregularidades.

Outra questão a ser analisada é a possibilidade de que candidatos de partidos políticos podem ser punidos pelo descumprimento da legislação eleitoral em relação ao envio de mensagens em massa, mas as empresas que forem contratadas eventualmente para fazer esse tipo de serviço também podem ser punidas na esfera cível. Mas o fato é que as campanhas eleitorais como controladoras de dados em potencial e algumas empresas e profissionais que prestam serviços para as campanhas se caracterizam como controladores e processadores no tratamento de dados nas campanhas eleitorais, podem sim, seguir ao enquadramento das normas previstas na LGPD. Neste ponto, importante destacar que o disparo automático em massa de

mensagens ele está proibido e que as empresas podem até ser contratadas para fazer esse tipo de serviço, desde que não haja impulsionamento irregular, não previsto nas próprias plataformas e na própria legislação eleitoral, ou seja é permitido, porém, caso esteja em conformidade com a resolução do TSE.

É proibido, por exemplo, que estas empresas utilizem tráfego de bases de dados para o envio de mensagens ou encaminhamento sem autorização do eleitor. O eleitor quando desejar receber algum material de campanha deverá voluntariamente se cadastrar nessas vias de transmissão, para ter acesso aos conteúdos conforme for disponibilizado pelas campanhas.

Conforme dispõe a LGPD e a Resolução do TSE, há possibilidade de solicitação de exclusão de cadastro da lista para que não receba mais informações e, também, a exclusão dos dados a qualquer tempo. Além disso, empresas que trabalham com pesquisas de opinião precisam se adequar às regras e normas, pois, às vezes, nessas pesquisas é feita uma análise do perfil dos eleitores para extração de dados quantitativos e qualitativos sobre intenções de voto,

No entanto, uma vez coletados, os dados podem ser utilizados como forma de discriminar pessoas e extrair informações de redes sociais, o que deve ser feito com o consentimento do eleitor. Por exemplo, grupos em redes sociais e as pessoas que fazem parte de forma voluntária terão seus dados coletados, desde que se cadastrem voluntariamente e permitam a extração desses dados, da mesma forma é importante alertar e destacar o uso desses dados nas políticas de privacidade, assim assegurados os direitos válidos para cidadão através da LGPD.

Cabe a ressalva de que a coleta e uso dos dados pessoais, mesmo que seja uma coleta feita de maneira consentida, é de que esses dados coletados sejam captados para a finalidade destinada à autorização do eleitor. A LGPD, assim como a legislação eleitoral afirmam que o eleitor tem o direito de saber como o controlador, no caso, a campanha, teve acesso aos seus dados pessoais, principalmente, caso ele comece a receber materiais não solicitados, considerando que é seu direito saber de onde vieram os dados e quais são todos os dados físicos e digitais que o partido ou empresas possuem.

A Resolução 23.624 de 2020 do TSE, que procurou adequar a questão dos prazos dos procedimentos eleitorais, também trata do envio em massa de mensagens no *WhatsApp* junto a questão do abuso do poder econômico que conforme a Lei Complementar nº 64 de 18 de maio 1990, que prevê como conduta de abuso de poder econômico, o envio em massa de mensagens e o tráfego de dados pessoais, para o fim de aliciamento eleitoral, uma vez que esse tipo de prática abusiva pode afetar o resultado das eleições.

No item 4 desta resolução, nos artigos 27 até o 41, a questão da propaganda na internet é tratada de maneira específica, incluindo a situação da questão da proteção de dados. O artigo 28, inciso III, por exemplo, permite que a propaganda seja feita por meio de aplicativos de mensagens voluntariamente, observando o consentimento do titular e tal inciso menciona as próprias normas da LGPD. O inciso IV cita que é permitido o envio de mensagens em grupos do *Facebook* e *WhatsApp*, por exemplo, desde que os participantes permaneçam e que o impulsionamento seja de forma natural ou normal, ou seja, de acordo com o parágrafo terceiro desse mesmo artigo, em funcionamento normal seriam aquelas formas de funcionamento que não estão previstas no próprio funcionamento das plataformas como promoções do *Facebook*.

Deve-se coletar o que precisa e certificar-se de que é destinado para uma finalidade legítima. Outro compromisso é estar aberto à transparência, além de que manter dados pessoais é um compromisso contínuo com esses dados enquanto os guardar. Se precisar mantê-lo, deve ser atualizado regularmente. Se não precisar mais dele, deverá excluí-lo. É inegável que a

utilização dos dados é necessária para a realização de negociações contratuais e tomada das melhores decisões.

Na tabela 1, pretende-se apresentar as definições constitutivas e operacionais referentes aos pilares definidos.

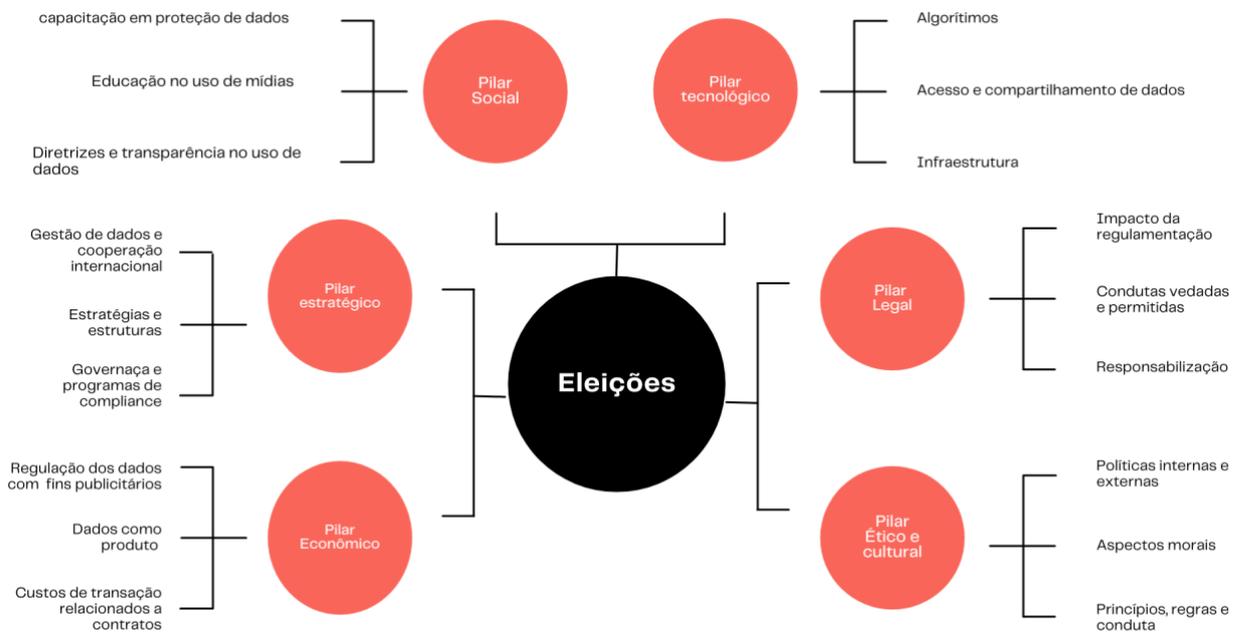
Tabela 1. Pilares norteadores

Pilar	Definição Constitutiva	Definição Operacional
Estratégico	Diretrizes estratégicas e subsídios ao planejamento com medidas de controle e prevenção.	<ul style="list-style-type: none"> - Governança em organizações públicas e privadas. - Presença de barreiras à entrada. - Políticas internas. - Mecanismos internos de supervisão e previsão.
Econômico	As informações coletadas para vender o melhor produto para usuários individuais. Com isso, o titular dos dados passou a ser o foco do processo e as informações pessoais adquiriram valor econômico e comercial, atendendo ao seu papel nas vendas. Economia baseada em dados.	<ul style="list-style-type: none"> - Regulação direcionada a comunicação e uso compartilhado de dados com objetivo de vantagem econômica. - Sanções dependem de condições econômicas. - Direito de personalidade menos orientado à exploração mercadológica.
Social	Diretrizes vinculadas ao uso de informações, bem como a clareza e transparência no uso de dados. Aplicada a usuários e organizações.	<ul style="list-style-type: none"> - Ações de curto e longo prazo voltadas à capacitação em proteção de dados para organizações. - Ações direcionadas a conscientização do público em geral.
Tecnológico	Desenvolvimento tecnológico e tecnologias disponíveis para coleta e processamento de dados.	- Instrumentos: Big Data; Data Warehouse; Data Mining; BI.
Legal	Condutas passíveis de sanções cível, administrativa e penal.	Condutas vedadas, permitidas, responsabilização, abrangência nacional ou internacional.
Ético e Cultural	Tem origem do grego <i>ethos</i> e orienta um conjunto de regras de conduta de um indivíduo ou grupo, estendendo-se à cultura, porquanto esta é valorada a partir de preceitos éticos e morais em prol da coletividade, de modo que uma não existe sem a outra.	Ações internas pautadas em governança e fortalecimento de políticas internas voltadas para a compreensão da importância de princípios orientados pelas organizações públicas e privadas.

Fonte: adaptado de Mantelero, 2014.

A partir da elaboração das definições constitutivas e operacionais de cada pilar previamente definido como norteadores do presente estudo – a dizer: estratégico, econômico, social, tecnológico, legal e ético/cultural –, visando à implementação da LGPD como mecanismo de enfrentamento das *fake news* no âmbito do processo eleitoral, torna-se essencial a construção de esquema para a apresentação das sugestões dos elementos dos respectivos pilares.

Para tanto, a título ilustrativo, sugere-se o esquema abaixo delineado.



Conclusão

O presente artigo teve como escopo abordar a legislação de proteção de dados nacional e internacional e, com base na extração de elementos correlatos, estruturar modelo ideal para o enfrentamento das *fake news* no processo eleitoral.

Assim, para a consecução do trabalho, revelou-se de extrema importância traçar um panorama acerca da legislação internacional, a dizer, GDPR, e nacional de proteção de dados pessoais, qual seja, a Lei nº. 13.709/2018, então conhecida como LGPD, a fim de ponderar as recomendações da OCDE, com a transformação digital com base na supressão da lacuna normativa e alinhamento da LGPD com as estratégias perquiridas internacionalmente, com a priorização de princípios como da privacidade e transparência, por exemplo.

Na Europa a preocupação com a proteção de dados é muito anterior à LGPD, isto é, pelo menos desde a década de 1980. Hoje, a política é feita de dados e existe muita manipulação com o uso não autorizado de dados pessoais e, para ajudar no controle destes dados pessoais é comum a criação de sistemas robustos de governança de big data.

Neste contexto, surgem as *fake news*, que se tornou fenômeno e centro das discussões de discursos midiáticos que culminaram para a escolha da palavra *post-truth*, isto é, “pós-verdade”, como palavra do ano de 2016, pelo Dicionário Oxford, notadamente, diante da crescente onda de reportagens falsas e mensagens de ódio na *internet*, durante as eleições de 2016 nos Estados Unidos e, no âmbito nacional, com as eleições presidenciais de 2018, posteriormente, reproduzidas para as eleições municipais. No Brasil, para fazer cessar a reprodução de fake news e propagandas irregulares durante o período eleitoral, a Justiça Eleitoral se esmera na publicação de resoluções no âmbito de sua competência, as quais parecem não acompanhar a avalanche de desinformação na *internet*, fundamentalmente, pelo fato de inexistir uma normatização do uso das redes sociais e plataformas digitais durante as eleições.

Inegável que toda a utilização irregular ou indevida de dados pessoais para manipular eleitores e as respectivas tomadas de decisões manipulam, conseqüentemente, o processo eleitoral e a escolha dos representantes de uma nação, interferindo na esfera democrática do país. No entanto, o Poder Legislativo e o TSE devem se atentar para respeitar os princípios e garantias fundamentais.

Com isso, no centro das atenções de uma eleição e, com a atenção às garantias constitucionais, sugere-se a observância de pilares norteadores para o enfrentamento das *fake news*, baseada na adoção de condutas transcritas nos respectivos elementos, para que se obtenha um processo eleitoral idôneo e em respeito às normas de proteção de dados pessoais. Os pilares norteadores: a) social; b) tecnológico; c) legal; d) ético e cultural; e) econômico; e f) estratégico. Cada um desses pilares identificados e conceituados apresenta um conjunto de elementos que orientam a boas práticas institucionais e organizacionais e passíveis de adoção por todos os envolvidos, isto é, desde a Justiça Eleitoral, até os atores em destaque – candidatos e partidos políticos –, eleitores e cidadãos de forma geral.

Importante mencionar que não se pretende, com a implementação de tal estruturação conceitual e dos pilares e elementos identificados, resolver de forma incontestável o problema ligado à disseminação de *fake news*, principalmente, durante o período eleitoral, mas sim, apresentar um modelo que favoreça a gestão do processo eleitoral no que tange às *fake news*, como mecanismo de enfrentamento, utilizando-se das legislações de proteção de dados, conferindo, assim, maior credibilidade aos atores públicos e confiança no uso dos seus dados pela sociedade.

Referências

- Allcott, H. & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, v. 31, n. 2, p. 211–236.
- Bennett, W. L. & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, v. 33, n. 2, p. 122–139, 2 abr. 2018.
- Bioni, B. R. (2019). Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense. p. 34.
- Borba, F. (2015). *Propaganda negativa nas eleições presidenciais brasileiras*. Opinião Pública [online]. v. 21, n. 02, pp. 268-295. Disponível em: <<https://doi.org/10.1590/1807-01912015212268>>. ISSN 1807-0191. <https://doi.org/10.1590/1807-01912015212268>).
- Bragatto, R. C. (2011). Democracia e internet: apontamentos para a sistematização dos estudos da área. *Compólitica*, v. 1, n. 2, p. 131, 24 out.
- Brasil. Lei nº. 4.737, de 15 de julho de 1965. *Institui o Código Eleitoral*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/14737compilado.htm> Acesso em 20 set. 2021.

Brasil. *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em 21 jun. 2021.

Brasil. Lei Complementar nº. 64, de 18 de maio de 1990. *Estabelece, de acordo com o art. 14, § 9º da Constituição Federal, casos de inelegibilidade, prazos de cessação, e determina outras providências*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp64.htm> Acesso em: 20 set. 2021.

Brasil. *Lei n. 9.504, de 30 de setembro de 1997*. Estabelece normas para as eleições. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/19504.htm> Acesso em 21 jun. 2021.

Brasil. Lei nº. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm> Acesso em 20 set. 2021.

Brasil. Lei n. 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados (LGPD)*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm> Acesso em 21 jun. 2021.

Brasil. Medida Provisória nº. 869, de 27 de dezembro de 2018. *Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm> Acesso em 20 set. 2021.

Brasil. Lei nº. 13.853, de 8 de julho de 2019. *Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm> Acesso em 20 set. 2021.

Brasil. Tribunal Superior Eleitoral. *Resolução nº. 23.610, de 18 de dezembro de 2019*. Relatoria Min. Luís Roberto Barroso. Publicado no DJE-TSE, nº 249, de 27.12.2019, p. 156-184. Disponível em: <<https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>> Acesso em 20 set. 2021.

Brasil. Medida Provisória nº. 959, de 29 de abril de 2020. *Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm> Acesso em: 20 set. 2021.

- Brasil. Tribunal Superior Eleitoral. Resolução nº. 23.634, de 13 de agosto de 2020. Relatoria Min. Luís Roberto Barroso. Publicado no DJE-TSE, nº 166, de 20.8.2020, p. 310-320. Disponível em: <<https://www.tse.jus.br/legislacao/compilada/res/2020/resolucao-no-23-624-de-13-de-agosto-de-2020>> Acesso em: 20 set. 2021.
- Cheeseman, N., Lynch, G., & Willis, J. (2018) Digital dilemmas: the unintended consequences of election technology, *Democratization*, 25:8, 1397-1418, DOI: [10.1080/13510347.2018.1470165](https://doi.org/10.1080/13510347.2018.1470165)
- Dawson, A. & Innes, M. (2019). How Russia's Internet Research Agency Built its Disinformation Campaign. *The Political Quarterly*, v. 90, n. 2, p. 245–256, 6 jun.
- Del Rowe, Sam. "Businesses Need to Know GDPR: Companies worldwide--and marketers in particular--need to prepare for the regulation, which takes full effect in May." *CRM Magazine*, vol. 22, no. 1, Jan.-Feb. 2018, p. 14. *Gale Academic OneFile*, link.gale.com/apps/doc/A525003835/AONE?u=capes&sid=bookmark-AONE&xid=1a229d4d. Accessed 30 May 2021.
- Doneda, D. (2011). a proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. v. 12, n. 2, p. 91-108.
- Europe. *General Data Protection Regulation (GDPR)*. Disponível em: <<https://gdpr-info.eu/>> Acesso em 21 jun. 2021.
- Governo Federal. *Ministério das Comunicações*. Disponível em <<https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet>> Acesso em 18 set. 2021.
- Hladick, B. (2018). "Elections Technology, Aging in Place." *State Legislatures*, vol. 44, no. 2, Feb. p. 10. *Gale Academic OneFile*.
- Jang, S. M. & Kim, J. K. (2018). Third person effects of fake news: Fake news regulation and media literacy interventions. *Computers in Human Behavior*, v. 80, p. 295–302, mar.
- Laybats, C. & Davies, J. GDPR: Implementing the regulations. *Business Information Review*. 2018, Vol. 35(2) 81–83. DOI: 10.1177/0266382118777808 journals.sagepub.com/home/birlink.gale.com/apps/doc/A523920107/AONE?u=capes&sid=bookmark-AONE&xid=1c640700. Accessed 13 May 2021.
- Mantelero, A. (2014). The future of consumer data protection in the E.U. Re-thinking the “notice and consent” paradigm in the new era of predictive analytics. *Computer Law & Security Review*, Volume 30, Issue 6.
- Marwick, A. (2018). Why do people share fake news? A sociotechnical model of media effects. *Journalism: Theory, Practice & Criticism*, v. 2.2, p. 474–512.

- McKelvey, R. D., Ordeshook, P. C. & McKelvey, R. D. (1986). Information, Electoral Equilibria, and the Democratic Ideal. *The Journal of Politics*, v. 48, n. 4, p. 909–937.
- Mendes, L. S., Bioni, B. R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. *Revista de Direito do Consumidor*. vol. 124. ano 28. p. 157-180. São Paulo: Ed. RT, jul.-ago. 2019.
- Observatório Privacidade. 2018: Uma conjunção astral. Memória do Observatório: Episódio 3/5. Por Data Privacy BR. Disponível em: <<https://www.observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/>> Acesso em: 18 set. 2021.
- RAIS, Diogo. A melhor tradução para fake news não é notícia falsa, é notícia fraudulenta. In: Entrevista concedida a Pedro Canário. *Revista Consultor Jurídico*, São Paulo, ago. 2018. Disponível em: <<https://www.conjur.com.br/2018-ago-12/entrevista-diogo-rais-professor-direito-eleitoral>> Acesso em 20 set. 2021.
- Tanner, C., Fishman, E. K., Horton, K. M. & Sheth, S. (2017). How Technology Is Changing News and Our Culture: Lessons From Elections 2016 and Davos 2017: Tech, Media, and the Newsroom of the Future. *Journal of the American College of Radiology*, Volume 14, Issue 12, Pages 1632-1634.e1, <https://doi.org/10.1016/j.jacr.2017.06.025>.
- Wardle, C. (2017). Fake news. It's complicated. First Draft, 2017. Disponível em: <<https://firstdraftnews.org/fake-news-complicated/>>. Acesso em: 18 de maio. 2021.