COORDENAÇÃO:
Ana Paula Canto de Lima
Newton Moraes

ELEIÇÕES NA ERA DIGITAL: DESAFIOS E REGULAMENTAÇÃO NO SÉCULO XXI

EDITORA IMPÉRIO

EDITORA
IMPÉRIO

Eleições na Era Digital
Desafios e Regulamentação no Século XXI

COORDENADORES

ANA PAULA CANTO DE LIMA
NEWTON MORAES

Eleições na Era Digital
Desafios e Regulamentação no Século XXI

Ana Paula Canto de Lima
Adrianne Lima
Beatriz de Andrade Junque
Camila Henning Salmoria
Carolina Elisa Margonari
Caroline Vivas Gonçalves
Daiana Allessi Nicoletti Alves
Eloá de Azevedo Caixeta
Érica Costa
Flavia Alcassa
Geysa Camara
Gisele Truzzi
Iasmin Palotta
João Victor Barcellos Machado Correia
Letícia Zampieri
Mariana Gomes Lopes
Newton Moraes
Oscar Valente Cardoso
Rafael A. Carneiro de Castilho
Silvio Maciel e Silva Junior

EDITORA IMPÉRIO

Direção Executiva: Eduardo Cavalcante de Almeida Costa
Direção Editorial: Ana Paula Moraes Canto de Lima
Conselho Editorial: Ana Paula Moraes Canto de Lima
Anne Cristine Silva Cabral
Cristiano Carrilho Silveira Medeiros
Ingrid Zanella Andrade Campos
Isabela Lessa de Azevedo Pinto Ribeiro
Maria Emília Miranda de Oliveira Queiroz
Schamkpou Bernardo Bezerra

Capa: Editora Império

Projeto Gráfico e Diagramação: Editora Império

Revisão: Do autor

Relacionamento com o cliente via WhatsApp: (81) 3203-6469

ISBN 978-65-89291-34-3

Printed in Brazil - Impresso no Brasil

APRESENTAÇÃO

A era digital trouxe novas dinâmicas para o cenário eleitoral, revolucionando tanto a forma de fazer campanha quanto desafiando o ordenamento jurídico. O livro "Eleições na Era Digital: Desafios e Regulamentação no Século XXI" explora questões atuais relacionadas ao pleito eleitoral na sociedade contemporânea.

A obra lança luz sobre a necessidade de regras claras, equânimes e transparentes capazes de trazer direcionamento, sanções e responsabilização aos atores que impactam o processo eleitoral, de maneira equilibrada, em conformidade com os princípios, a Carta Magna e o ordenamento jurídico como um todo. E dessa maneira, resgatar a confiança no processo e na paridade de armas que deve permear um pleito eleitoral.

É indispensável enfrentar os desdobramentos do ambiente digital que impactam na democracia, seja na escolha dos candidatos, nas responsabilidades de cada ator, ferramentas, plataformas e todas as nuances que impactam o pleito eleitoral, sendo indispensável um ambiente neutro, com a devida sanção àqueles que excederem os limites legais.

É preciso empreender esforços para que os cidadãos/eleitores aumentem o nível de consciência, possibilitando que sejam capazes de questionar e criticar o que observam na internet. Cabe aos legisladores, educadores, à sociedade civil organizada, ao estado e às plataformas digitais a postura de disseminar informação e educação digital evoluindo a compreensão do cenário e a proteção da integridade democrática.

O livro está repleto de temas atuais como a inclusão digital, a propaganda eleitoral online e os riscos de manipulação por deepfakes, entre outros excelentes que são abordados, evidenciando os dilemas que cada vez mais afetam as eleições.

Com uma abordagem clara e atual, esta obra é essencial para todos que buscam entender as transformações, o cenário atual e os riscos envolvidos na era digital.

Aproveite sem moderação!
Os coordenadores.

PREFÁCIO

A era digital redefiniu os contornos do processo eleitoral, introduzindo desafios sem precedentes e transformando radicalmente a dinâmica entre candidatos, eleitores e plataformas digitais. O livro "Eleições na Era Digital: Desafios e Regulamentação no Século XXI" se debruça sobre as implicações dessa revolução tecnológica no âmbito democrático, oferecendo uma análise crítica e aprofundada sobre os principais temas que emergem desse novo cenário. Ao intercalar tecnologia, regulação e democracia, esta obra ilumina as questões mais prementes e as soluções necessárias para garantir a integridade e transparência do processo eleitoral no mundo digital.

A obra investiga o delicado equilíbrio entre a liberdade de expressão e a responsabilidade das plataformas de mídias sociais, analisando o papel crucial que desempenham na moderação de conteúdo durante as campanhas eleitorais. A crescente violência política de gênero, exacerbada no ambiente virtual, é abordada de forma contundente, destacando a urgência de mecanismos de proteção eficazes e políticas de conscientização. Esse fenômeno não pode ser subestimado, visto que o ambiente digital não só reflete como amplifica práticas de opressão e exclusão.

Outro ponto fundamental explorado é a inclusão digital e sua relevância para a participação cidadã plena. Garantir que a tecnologia seja uma ponte, e não um obstáculo, para o exercício da cidadania é um dos grandes desafios do século XXI. O impacto devastador das fake news e a manipulação de informações digitais também são temas centrais da obra, que propõe políticas robustas e educação digital como as principais ferramentas para combater a desinformação.

A obra não se limita a tratar das nuances legislativas, mas traz um estudo aprofundado sobre crimes eleitorais digitais e suas implicações, ressaltando a importância da

cibersegurança na preservação da integridade do processo democrático. Analisam-se as ameaças tecnológicas, como a proliferação de deepfakes e a manipulação de conteúdo audiovisual, que representam riscos imensuráveis para a autenticidade das campanhas eleitorais.

Além disso, o livro examina o impacto do Marco Civil da Internet sobre o contexto eleitoral, traçando um panorama das regras de propaganda eleitoral digital e suas limitações, visando sempre a transparência e justiça no pleito. A responsabilidade das plataformas digitais é tema recorrente, especialmente no que tange à moderação de conteúdos sensíveis e à garantia de um ambiente eleitoral equânime e democrático.

Por fim, "Eleições na Era Digital: Desafios e Regulamentação no Século XXI" é leitura indispensável para juristas, especialistas em tecnologia e todos aqueles que buscam entender as novas fronteiras que a tecnologia impõe ao sistema democrático. Este livro é mais do que uma reflexão; é um guia para a compreensão e enfrentamento dos novos paradigmas impostos pela era digital.

Parabenizo os coordenadores Ana Paula Canto de Lima e Newton Moraes, assim como os demais autores, que, com precisão e clareza, trazem reflexões contemporâneas e necessárias para os profissionais do Direito, Tecnologia e demais interessados. A leitura atenta dos artigos aqui presentes enriquecerá o debate e fornecerá respostas às questões complexas que emergem no ambiente digital.

Coriolano Camargo Ph.d.

Advogado e Doutor em Direito com certificação internacional em Direito Digital. Conselheiro Estadual da OAB/SP em seu terceiro mandato, Presidente da Digital Law Academy, Coordenador do curso de Proteção de Dados da ESA Nacional e Diretor Jurídico do CIESP. Integra o Conselho Superior de Direito da FecomercioSP e a Comissão Nacional de Inteligência Artificial do Conselho Federal da OAB. Professor de universidades europeias e convidado de diversas instituições nacionais e internacionais, com atuação focada em Ciberlaw e Proteção de Dados.

SUMÁRIO

MÍDIAS SOCIAIS E LIBERDADE DE EXPRESSÃO NAS ELEIÇÕES: LIMITES E RESPONSABILIDADE DOS CANDIDATOS E ELEITORES

Ana Paula Canto de Lima[1]
Érica Costa[2]

1. INTRODUÇÃO

Podemos afirmar que não existe tema mais em voga no Brasil do que a regulação das redes sociais no geral, bem como, questões que envolvam redes sociais em épocas de eleitorais.

Antes de se iniciarmos qualquer breve estudo sobre a as Mídias Sociais e Liberdade de Expressão nas Eleições, em que se possam ser atribuídos limites e responsabilidade dos candidatos e eleitores, devemos entender o cenário Legislativo, Executivo e Judicial relativo à esta temática.

Em um primeiro momento, vale destacar que o binômio "liberdade de expressão" e "censura" sempre andaram

1 Advogada, sócia fundadora do escritório Canto de Lima Advocacia, mestre (UFRPE), LLM em proteção de dados com dupla certificação Brasil/Portugal (LGPD--RGPD); Conselheira no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD); Membro do Observatório Nacional de Cibersegurança, Inteligência Artificial e Proteção de Dados – ONCiber; Membro da Comissão de Proteção de Dados da OAB Nacional; Conselheira Estadual da OAB/PE, Vice-presidente da Comissão de Proteção de Dados da OAB/PE; Presidente da Comissão de Crimes Cibernéticos da ABCCRIM. Fundadora do LGPD Learning Edutech e do Cadê meu dado?

2 Advogada, 15 anos OAB/SP. Formada em Direito pela Universidade Católica de Pernambuco (2009), pós-graduada em Direito Constitucional PUC/SP, MBA em gestão empresarial pela FGV, LLM em Proteção de dados e Privacidade pela Universidade de Lisboa e FMP. Certificada TOLES legal English. Advogada Itaú Unibanco (2010), Advogada Villemor & Amaral advogados (2011), Advogada Sênior in house Mercado Livre (2011-2015), Coordenadora Jurídica Nacional Walmart (2015-2018Fundadora da DPO Society Consultoria, Privacy Counsel Americas OneTrust (2020 - 2022), Global Privacy Manager AB-InBev (2023), fundadora da DPO Society Consultoria.

de mãos dadas, unidos ou como forma de manipulação social, assim, a temática sobre mídias sociais e liberdade de expressão é e sempre será um tema complexo e em constante evolução, especialmente no contexto brasileiro.

Para iniciar este breve artigo, vale mencionar alguns dos principais pontos e desafios atuais relacionados a esse assunto, sendo eles:

> **a) Supremo Tribunal Federal (STF):** A atuação do STF que vem desempenhando um papel central em decisões sobre a liberdade de expressão nas redes sociais. O tribunal máximo do país, enfrenta o desafio de equilibrar a proteção ao direito de livre manifestação com a necessidade de combater discursos de ódio e garantir a segurança e dignidade dos indivíduos.
>
> **b) Marco Civil da Internet[3]:** é imprescindível pontuar a Marco Civil da Internet (MCI) de 2014 surgiu de forma inovador para disciplinar o uso da internet no Brasil. O diploma legal trata desde então acerca da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros, com consequências e responsabilidades para os provedores de conexão e provedores de aplicações. Além de regular como se daria a requisição judicial de registros de acesso às aplicações de internet, tempo de guarda e outras informações relevantes.
>
> **c) Regulamentação das Mídias Sociais:** Até recentemente, a legislação brasileira possuía poucas leis que regulamentassem as redes, no entanto, mudanças começaram a ocorrer com a implementação da Lei Geral de Proteção de Dados (LGPD)[4], que estabele-

3 BRASIL. MCI - LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 05 out. 2024.

4 BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 05 out. 2024.

ce diretrizes para o tratamento de dados pessoais nas plataformas digitais. Bem como, aperfeiçoamento dos regulamentos, diretrizes, manuais para que estejam em conformidade e modernidade para esta questão das redes sociais que estão a cada dia se modernizando mais e mais.

d) Projeto de Lei 2630/2020[5]: Conhecido como a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, este projeto estabelece normas para a transparência de redes sociais e serviços de mensagens privadas, focando na responsabilidade dos provedores em combater a desinformação. (Ainda não aprovado).

e) Cartilhas e Manuais: O Tribunal Superior Eleitoral (TSE) disponibiliza cartilhas interativas e manuais que esclarecem as regras de campanha eleitoral na internet, incluindo o uso de redes sociais. Esses materiais são desenvolvidos para ajudar candidatos e partidos a compreenderem as normas e evitarem infrações durante a campanha eleitoral.

f) Lei das Eleições (Lei nº 9.504/1997)[6]: Esta é a principal lei que regula as eleições no Brasil, estabelecendo normas sobre propaganda eleitoral, financiamento de campanhas, entre outros aspectos.

g) Código Eleitoral (Lei nº 4.737/1965)[7]: Embora mais antigo, este código ainda contém disposições re-

5 CÂMARA DOS DEPUTADOS. PL 2630/2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735> Acesso em: 05 out. 2024.

6 BRASIL. LEI Nº 9.504, DE 30 DE SETEMBRO DE 1997 -Estabelece normas para as eleições. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9504.htm> Acesso em: 05 out. 2024.

7 TSE. Código Eleitoral - Lei nº 4.737, de 15 de julho de 1965. Disponível em: <https://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb0-4.737-de-15-de-julho-de-1965> Acesso em: 05 out. 2024.

levantes sobre o processo eleitoral.

h) Lei nº 13.488/2017[8]: Alterou a Lei das Eleições para incluir disposições sobre propaganda eleitoral na internet.

i) Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018)[9]: Embora não seja específica para eleições, a LGPD é relevante para o uso de dados pessoais em campanhas eleitorais.

j) Resolução nº 23.610/2019[10]: Esta resolução dispõe sobre a propaganda eleitoral, utilização e geração do horário gratuito e as condutas ilícitas em campanha eleitoral nas eleições. Ela aborda a propaganda na internet e o combate à desinformação.

k) Resolução nº 23.671/2021[11]: Trata das regras para as eleições de 2022, incluindo disposições sobre propaganda eleitoral e desinformação, com atenção especial ao uso de mídias sociais.

l) Resolução nº 23.608/2019[12]: Estabelece normas para a fiscalização e auditoria do sistema eletrônico de votação, incluindo medidas para combater a desinformação sobre o processo eleitoral.

---

8 BRASIL. LEI Nº 13.488, DE 6 DE OUTUBRO DE 2017. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13488.htm> Acesso em: 05 out. 2024.

9 BRASIL. CÓDIGO CIVIL. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 05 out. 2024.

10 TSE. RESOLUÇÃO Nº 23.610, DE 18 DE DEZEMBRO DE 2019.Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019> Acesso em: 05 out. 2024.

11 TSE. RESOLUÇÃO Nº 23.671, DE 14 DE DEZEMBRO DE 2021. Disponível em: Acesso em: <https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-671-de-14-de-dezembro-de-2021> Acesso em: 05 out. 2024.

12 TSE. RESOLUÇÃO Nº 23.608, DE 18 DE DEZEMBRO DE 2019. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-608-de-18-de-dezembro-de-2019> Acesso em: 08 out. 2024.

Esses materiais são fundamentais para garantir que o processo eleitoral ocorra de maneira justa e transparente, prevenindo abusos e garantindo a integridade das eleições. Se precisar de mais informações ou acesso a algum desses documentos, recomendo visitar o site oficial do Tribunal Superior Eleitoral (TSE) ou dos Tribunais Regionais Eleitorais (TREs).

Todavia a narrativa de censura e perseguição política é frequente, destacando a necessidade de um equilíbrio entre a liberdade de expressão e a regulação das plataformas para prevenir abusos e proteger os direitos humanos.

2. CONTEXTUALIZAÇÃO DE LIBERDADE DE EXPRESSÃO, CENSURA E NARRATIVA

> a) Liberdade de Expressão: A liberdade de expressão é um dos direitos fundamentais garantidos pela Constituição Federal do Brasil de 1988. Este direito está consagrado no artigo 5º, inciso IV, que assegura a livre manifestação do pensamento, vedado o anonimato. A liberdade de expressão é essencial para o funcionamento de uma democracia, pois permite que indivíduos expressem suas opiniões, ideias e críticas sem medo de censura ou represálias. Este direito abrange não apenas a fala, mas também outras formas de comunicação, como a arte, a imprensa e as mídias sociais.

Além de garantir a liberdade de expressão, a Constituição Federal[13] também estabelece limites para esse direito. O inciso X do artigo 5º protege a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua

13 BRASIL.CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 08 out. 2024.

violação. Isso significa que, embora as pessoas tenham o direito de se expressar livremente, elas também devem respeitar os direitos dos outros e podem ser responsabilizadas por discursos que causem danos a terceiros.

A liberdade de expressão também está ligada à liberdade de imprensa, que é fundamental para a transparência e a fiscalização dos poderes públicos. A Constituição, em seu artigo 220, garante que a manifestação do pensamento, a criação, a expressão e a informação não sofrerão qualquer restrição, observando os limites previstos na própria Constituição. Isso assegura que os meios de comunicação possam operar sem censura, mas dentro dos limites legais, promovendo um fluxo livre de informações que é crucial para uma sociedade informada.

No entanto, a liberdade de expressão no Brasil enfrenta desafios, especialmente em tempos de polarização política e desinformação. O Supremo Tribunal Federal (STF) tem desempenhado um papel crucial na interpretação dos limites e na proteção desse direito, buscando equilibrar a liberdade de expressão com outros direitos fundamentais. Casos emblemáticos têm sido julgados para definir até onde vai o direito de expressar opiniões sem que isso resulte em discursos de ódio ou incitação à violência. Contudo, em que pese o papel relevante do STF, é preciso cautela para que, ao buscar equalizar tais diretos e garantias, não exceder os limites e competências do próprio Tribunal.

Em suma, a liberdade de expressão é um pilar da democracia brasileira, protegida pela Constituição, mas que deve ser exercida com responsabilidade. Ela permite que os cidadãos participem ativamente do debate público, contribuindo para o desenvolvimento social e político do país. No entanto, é essencial que esse direito seja exercido de maneira que respeite os direitos dos outros, garantindo um ambiente de respeito e diálogo construtivo.

O ordenamento jurídico brasileiro estabelece

critérios, regras e possui leis que orientam como exercer tais direitos e como os excessos podem ser penalizados, conforme determinação legal, respeitando o devido processo legal e o contraditório.

> b) Censura: A censura é um tema complexo e controverso, especialmente quando se trata de personagens fundamentais a qualquer tipo e democracia: políticos, eleitores, apoiadores e a imprensa. No contexto político, a censura pode ser vista como uma ferramenta para controlar narrativas e limitar a divulgação de informações que possam ser prejudiciais à imagem de um governo ou de um partido específico.

Historicamente, regimes autoritários têm utilizado a censura para silenciar opositores e manter o controle social. No entanto, mesmo em democracias, a censura pode ocorrer de maneiras mais sutis, como através de pressões econômicas ou políticas sobre veículos de comunicação.

Para os eleitores e apoiadores, a censura pode se manifestar na forma de restrições ao acesso à informação ou na manipulação de conteúdos disponíveis, o que afeta a capacidade de formar opiniões informadas. Em muitos casos, a censura direcionada a esses grupos visa moldar percepções e influenciar resultados eleitorais. Isso pode ocorrer por meio de desinformação ou da supressão de vozes dissidentes em plataformas de mídia social, impactando o debate público e a participação democrática.

A imprensa, como guardiã da liberdade de expressão e da informação, frequentemente enfrenta censura quando suas reportagens desafiam interesses de figuras poderosas. A censura à imprensa pode assumir várias formas, desde a intimidação de jornalistas até a imposição de restrições legais que limitam a cobertura de determinados assuntos. Em muitos países, jornalistas enfrentam ameaças, violência e até mesmo prisão por seu trabalho investigativo, o que represen-

ta um ataque direto ao direito do público de ser informado.

Os desafios da censura são amplificados no ambiente digital, onde a disseminação rápida de informações e a presença de grandes plataformas tecnológicas criam novas dinâmicas de controle e influência.

A censura online pode ser exercida por governos, mas também por empresas privadas que gerenciam plataformas de comunicação. A moderação de conteúdo, embora necessária para prevenir abusos, pode resultar em censura se não for conduzida de maneira transparente e justa, levantando questões sobre quem decide o que pode ou não ser dito.

Em suma, a censura afeta profundamente a dinâmica política e social, limitando a liberdade de expressão e o direito à informação. É essencial que sociedades democráticas estabeleçam mecanismos eficazes para proteger esses direitos fundamentais, garantindo que a censura não seja utilizada como ferramenta de opressão. O equilíbrio entre a proteção contra abusos e a garantia de liberdade de expressão é um desafio contínuo que exige vigilância e compromisso com os princípios democráticos.

> c) Narrativas: A narrativa é o ato de contar uma história, real ou fictícia, por meio de uma sequência de eventos interligados, envolvendo personagens em determinados tempos e espaços. Elementos essenciais de uma narrativa incluem o narrador, personagens, enredo, tempo e espaço.[14]

No âmbito eleitoral, a narrativa diz respeito à construção de histórias e discursos que candidatos e partidos utilizam para persuadir e mobilizar o eleitorado. O storytelling, em suma, é a arte de falar sobre um assunto por meio de uma história. Portanto, narrar um fato ocorrido dentro de um

14 SIGNIFICADOS. Narrativa. Disponível em: <https://www.significados.com.br/narrativa/> Acesso em: 08 out. 2024.

determinado contexto. Essa estratégia, frequentemente denominada **storytelling eleitoral**, envolve a criação de uma narrativa política que conecta emocionalmente os eleitores à candidatura, destacando valores, experiências e propostas de maneira envolvente.[15]

A narrativa que provoca percepções diferentes da mesma história, dependendo do lado que a conta, está relacionada ao conceito de narrativas alternativas ou moldagem de realidade. Esse fenômeno ocorre quando um mesmo evento ou situação é contado de maneiras diferentes por grupos ou indivíduos, destacando certos elementos, omitindo outros e, às vezes, interpretando os fatos sob ângulos específicos. Segundo McIntyre "a pós-verdade não é tanto afirmar que a verdade não existe, como é afirmar que os fatos importam menos que nosso ponto de vista político".[16] Ou seja, o fato em si passa a não importar, mas apenas quem o está protagonizando ou proferindo.

As narrativas podem levar a grupos opostos a desenvolverem percepções divergentes sobre a mesma questão, cada lado utilizando uma narrativa oposta para justificar de forma que fique melhor para seus interesses. Essa polarização pode ser exacerbada pela disseminação de desinformação e fake news, que frequentemente acompanham essas narrativas.

3. ESCÂNDALOS INTERNACIONAIS E NACIONAIS SOBRE MANIPULAÇÃO DE MÍDIAS SOCIAIS A FAVOR OU CONTRA CANDIDATOS

O escândalo da empresa *Cambridge Analytica*, que veio à tona em 2018, revelou práticas controversas de coleta e uso de dados pessoais de milhões de usuários do Facebook

15 COUTO, Mari. O storytelling eleitoral e seus segredos. Disponível em: <https://blog.alcateiapolitica.com.br/segredos-storytelling-eleitoral/> Acesso em: 08 out. 2024.

16 MCINTYRE, L. Post-truth. Cambridge: MIT Press, 2018. p. 32.

sem seu consentimento explícito. A *Cambridge Analytica*, uma empresa de consultoria política, utilizou esses dados para criar perfis psicológicos detalhados dos eleitores, com o objetivo de influenciar suas decisões de voto em várias campanhas políticas, incluindo a eleição presidencial dos Estados Unidos em 2016 e o referendo do Brexit no Reino Unido.[17]

A coleta dos dados foi realizada por meio de um aplicativo de teste de personalidade chamado "*thisisyourdigitallife",* desenvolvido por Aleksandr Kogan, um pesquisador da Universidade de Cambridge. Embora apenas cerca de 270.000 usuários tenham baixado o aplicativo, ele foi projetado para coletar dados não apenas dos usuários, mas também de seus amigos no Facebook, alcançando assim cerca de 87 milhões de perfis. Esses dados foram então vendidos para a *Cambridge Analytica*, violando as políticas de privacidade do Facebook.

O impacto do escândalo foi significativo, gerando um intenso debate sobre privacidade de dados e o papel das redes sociais na manipulação política. Revelou-se que a *Cambridge Analytica* utilizava os dados para criar anúncios políticos altamente segmentados e personalizados, explorando vulnerabilidades emocionais dos usuários para influenciar suas opiniões e comportamentos de voto. Isso levantou preocupações sobre a integridade dos processos democráticos e a capacidade das plataformas digitais de proteger suas informações pessoais.

Em resposta ao escândalo, o Facebook enfrentou escrutínio global, resultando em investigações por parte de reguladores em vários países e uma queda significativa no valor de mercado da empresa. Mark Zuckerberg, CEO do Facebook, foi convocado a testemunhar perante o Congresso

17 BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751> Acesso em: 08 out. 2024.

dos Estados Unidos e o Parlamento do Reino Unido, onde admitiu falhas na proteção dos dados dos usuários e se comprometeu a implementar medidas mais rigorosas de segurança e transparência.[18]

O escândalo da *Cambridge Analytica* destacou a necessidade urgente de regulamentações mais robustas sobre a coleta e uso de dados pessoais na era digital. Ele impulsionou mudanças significativas na legislação de proteção de dados, como a implementação do Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia. Além disso, aumentou a conscientização pública sobre a importância da privacidade online e incentivou uma discussão global sobre ética, responsabilidade e direitos dos usuários na internet.

Já no cenário nacional, a manipulação de votos no contexto brasileiro é um tema complexo que envolve diversas práticas e desafios históricos. Desde o período colonial, o Brasil enfrentou problemas relacionados à corrupção eleitoral, como o uso do "*voto de cabresto*", onde eleitores eram coagidos ou comprados para votar em determinados candidatos. Essa prática era comum durante a República Velha e foi facilitada pela falta de um sistema eleitoral transparente e confiável.

Nos últimos anos, a manipulação de informações nas redes sociais emergiu como uma preocupação central. Durante as eleições presidenciais de 2018, por exemplo, houve relatos de campanhas de desinformação disseminadas por meio de plataformas como WhatsApp e Facebook. Essas campanhas tinham o potencial de distorcer fatos e influenciar as percepções dos eleitores sobre candidatos e suas propostas, afetando o resultado eleitoral de maneira significativa.

Para mitigar esses riscos, o Tribunal Superior Eleito-

18 G1. Em depoimento de 5 horas ao Senado americano, Mark Zuckerberg admite erros do Facebook. <https://g1.globo.com/economia/tecnologia/noticia/mark-zuckerberg-depoe-ao-senado-sobre-uso-de-dados-pelo-facebook.ghtml> Acesso em: 08 out. 2024.

ral (TSE) tem implementado medidas para combater a desinformação, incluindo parcerias com empresas de tecnologia e campanhas de conscientização pública sobre a importância de verificar a veracidade das informações antes de compartilhá-las. Além disso, o TSE promoveu ações para aumentar a transparência e a segurança do processo eleitoral, assegurando que o sistema de votação eletrônica permaneça confiável.

A manipulação de votos no Brasil, portanto, evoluiu de práticas diretas de coerção para estratégias mais sutis de influência através da informação. Embora o país tenha feito progressos significativos na proteção da integridade eleitoral, a batalha contra a manipulação, fake News, narrativas e a desinformação continua a ser um desafio crucial para a democracia brasileira. A educação dos eleitores e a regulamentação eficaz das plataformas digitais são essenciais para garantir eleições justas e transparentes no futuro.

4. LEGISLAÇÃO VIGENTE PARA AS CAMPANHAS ELEITORAIS EM 2024

A legislação vigente para campanhas eleitorais no Brasil em 2024 aborda diversos aspectos relacionados ao uso de mídias sociais, *fake news* e desinformação, refletindo a crescente importância dessas plataformas no cenário político. Com o avanço da tecnologia e o impacto das redes sociais na formação da opinião pública, o Tribunal Superior Eleitoral (TSE) tem intensificado seus esforços para regulamentar e fiscalizar o ambiente digital durante o período eleitoral.

Um dos principais focos da legislação é o combate à disseminação de *fake news*. As campanhas eleitorais estão sujeitas a regras rigorosas para evitar a propagação de informações falsas que possam influenciar o resultado das eleições. Há penalidades para candidatos e partidos que se beneficiem direta ou indiretamente de campanhas de desinformação.

A legislação também estabelece limites claros para a

propaganda eleitoral nas mídias sociais. Os candidatos podem utilizar suas contas oficiais para promover suas campanhas, mas devem respeitar as regras de transparência e identificação de conteúdo patrocinado. Qualquer anúncio pago deve ser claramente identificado como tal, e os gastos com publicidade digital devem ser devidamente registrados na prestação de contas da campanha.

Além disso, a legislação proíbe o uso de robôs e perfis falsos para manipular o debate público nas redes sociais. O uso de tecnologia para criar interações artificiais e aumentar o alcance de determinadas mensagens é considerado uma prática ilegal e antiética. As plataformas são incentivadas a desenvolver mecanismos para detectar e eliminar esses perfis, garantindo um ambiente mais autêntico e transparente para o debate eleitoral.

O TSE também promove campanhas de conscientização pública para educar os eleitores sobre os riscos da desinformação. A ideia é capacitar os cidadãos para que possam identificar notícias falsas e verificar a veracidade das informações antes de compartilhá-las. Essa iniciativa é crucial para reduzir o impacto das *fake news* e fortalecer a confiança no processo eleitoral.

Outro ponto importante é a regulamentação do impulsionamento de conteúdo. As campanhas podem pagar para aumentar o alcance de suas postagens, mas devem seguir regras específicas sobre segmentação de público e transparência. As plataformas são obrigadas a manter um banco de dados público com informações sobre todos os anúncios políticos, incluindo quem pagou por eles e quanto foi gasto.

A legislação também aborda a proteção de dados pessoais. Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), as campanhas devem garantir que o uso de dados dos eleitores para fins de segmentação e marketing esteja em conformidade com as normas de privacidade. Isso inclui obter consentimento explícito dos usuários e garantir

que seus dados sejam usados de maneira responsável e segura.

Em relação à fiscalização, o TSE conta com um sistema de denúncias para que os eleitores possam reportar irregularidades nas campanhas digitais. As denúncias são investigadas e, se comprovadas, podem resultar em multas e outras sanções para os responsáveis. Essa medida visa garantir que as regras sejam efetivamente aplicadas e que haja consequências para aqueles que tentam burlar o sistema.

A legislação também incentiva a colaboração internacional no combate à desinformação. O TSE tem buscado parcerias com órgãos eleitorais de outros países para compartilhar experiências e boas práticas. Essa cooperação é essencial para enfrentar um problema que é global e que exige uma resposta coordenada entre diferentes nações e plataformas.

Por fim, a legislação para as campanhas na atualidade reflete um esforço contínuo para adaptar o processo eleitoral às novas realidades tecnológicas. A evolução das normas busca equilibrar a liberdade de expressão com a necessidade de proteger a integridade das eleições, garantindo que o ambiente digital seja um espaço seguro e justo para o debate democrático.

5. CONSIDERAÇÕES FINAIS

A liberdade de expressão é um dos pilares fundamentais de uma sociedade democrática, permitindo que indivíduos e grupos manifestem suas opiniões e ideias sem medo de represálias. Quando cidadãos evitam se manifestar por temer as consequências e represálias, há que se repensar o rumo que a sociedade está tomando.

No cenário eleitoral brasileiro, essa liberdade é crucial para garantir um debate público robusto e informado. No entanto, o exercício dessa liberdade não é absoluto e enfrenta limites, especialmente quando confrontado com a

disseminação de informações falsas e discursos de ódio. A linha tênue entre liberdade de expressão e censura se torna ainda mais complexa durante períodos eleitorais, quando a influência sobre o eleitorado pode determinar o futuro político do país.

Um dos principais desafios no contexto eleitoral é a propagação de *fake News e narativas*, que podem distorcer o processo democrático ao influenciar as decisões dos eleitores com base em informações falsas ou enganosas.

O Tribunal Superior Eleitoral (TSE) tem buscado medidas para combater essa prática, equilibrando a necessidade de proteger a integridade das eleições com a garantia da liberdade de expressão. Essas medidas incluem parcerias com plataformas de mídias sociais para identificar e remover conteúdos falsos, além de campanhas educativas para conscientizar o público sobre a importância de verificar informações.

Entretanto, a implementação de medidas contra *fake news* levanta preocupações sobre censura. Há um debate contínuo sobre até que ponto o Estado ou empresas privadas devem intervir na moderação de conteúdo online. A censura, mesmo que bem-intencionada, pode facilmente se transformar em um instrumento de controle excessivo, suprimindo vozes críticas e limitando o debate público. Portanto, há uma linha tênue e qualquer excesso é temerário, ademais, qualquer ação nesse sentido deve ser transparente, proporcional e sujeita a mecanismos de responsabilização. O ponto de atenção é que, não se deve pender para nenhum partido ou lado político, tendo em vista a subjetividade do assunto, eis onde está o maior desafio, pois lidamos com pessoas que possuem lado e preferência política.

Além das *fake news*, o discurso de ódio é outro aspecto que desafia os limites da liberdade de expressão durante as eleições. Mensagens que incitam violência ou discriminação contra grupos específicos podem ameaçar a coesão social e a segurança pública.

Noutro giro, as narrativas ganham espaço e dificultam a transparência e a equidade do pleito eleitoral, uma vez que, a depender do lado, o mesmo fato e acontecimento pode ser percebido de maneiras diversas, a depender de quem o praticou, o que impacta na neutralidade e na equidade das eleições.

O TSE e outras entidades têm a responsabilidade de atuar contra as manifestações ilícitas visando proteger os direitos fundamentais de todos os cidadãos. No entanto, definir o que constitui discurso de ódio pode ser subjetivo e controverso, exigindo critérios claros e objetivos para evitar abusos das autoridades e manipulações político-partidárias.

O papel das plataformas de mídias sociais é central nesse debate. Empresas como Facebook, Twitter e YouTube têm implementado políticas próprias para lidar com desinformação e discurso de ódio, mas enfrentam críticas tanto por não fazerem o suficiente, quanto por irem longe demais. A autorregulação dessas plataformas é vista por alguns como insuficiente, enquanto outros argumentam que a intervenção estatal pode comprometer a neutralidade da rede e a liberdade de expressão, e por consequência impondo censura.

A educação midiática emerge como uma solução potencial para mitigar os efeitos negativos da desinformação e do discurso de ódio. Ao capacitar os cidadãos para avaliar criticamente as informações que consomem, é possível fortalecer a resiliência da sociedade contra tentativas de manipulação. Iniciativas educacionais podem complementar as medidas regulatórias, promovendo uma cultura de responsabilidade e engajamento cívico.

O equilíbrio entre liberdade de expressão e censura também está ligado à confiança nas instituições democráticas. A transparência nas ações do governo e das plataformas de mídias sociais é crucial para manter a confiança do público. Processos claros com o objetivo de contestar decisões de remoção de conteúdo e garantir a proteção dos direitos

dos usuários são fundamentais para um ambiente digital saudável. Não se pode relativizar o devido processo legal, o contraditório e a ampla defesa, garantias constitucionais que tanto se lutou para conquistar.

A participação ativa da sociedade civil é igualmente importante na definição dos limites da liberdade de expressão. Organizações não governamentais, acadêmicos e defensores dos direitos humanos desempenham um papel vital na fiscalização das ações do governo e das empresas, garantindo que as medidas adotadas respeitem os princípios democráticos, estes devem representar todos os lados envolvidos no processo eleitoral.

Finalmente, o diálogo contínuo entre todas as partes interessadas — governo, sociedade civil, setor privado e cidadãos — é essencial para encontrar soluções equilibradas. O cenário eleitoral brasileiro, com sua diversidade e complexidade, exige abordagens que respeitem a pluralidade de vozes enquanto protegem a integridade do processo democrático.

Em resumo, os limites da liberdade de expressão no cenário eleitoral brasileiro são um campo de tensão entre garantir um debate público livre e proteger o processo democrático de influências negativas. A busca por esse equilíbrio requer vigilância constante, transparência e a participação ativa de toda a sociedade.

REFERÊNCIAS

BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751> Acesso em: 08 out. 2024.

BRASIL. MCI - LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 05 out. 2024.

CÂMARA DOS DEPUTADOS. PL 2630/2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735> Acesso em: 05 out. 2024.

BRASIL. LEI Nº 9.504, DE 30 DE SETEMBRO DE 1997 -Estabelece normas para as eleições. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9504.htm> Acesso em: 05 out. 2024.

TSE. Código Eleitoral - Lei nº 4.737, de 15 de julho de 1965. Disponível em: <https://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb-0-4.737-de-15-de-julho-de-1965> Acesso em: 05 out. 2024.

BRASIL. LEI Nº 13.488, DE 6 DE OUTUBRO DE 2017. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13488.htm> Acesso em: 05 out. 2024.

BRASIL. CÓDIGO CIVIL. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 05 out. 2024.

BRASIL.CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 05 out. 2024.

G1. Em depoimento de 5 horas ao Senado americano, Mark Zuckerberg admite erros do Facebook. <https://g1.globo.com/economia/tecnologia/noticia/mark-zuckerberg-depoe-ao-senado-sobre-uso-de-dados-pelo-facebook.ghtml> Acesso em: 08 out. 2024.

TSE. RESOLUÇÃO Nº 23.610, DE 18 DE DEZEMBRO DE 2019.Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezem-

bro-de-2019> Acesso em: 05 out. 2024.

TSE. RESOLUÇÃO Nº 23.671, DE 14 DE DEZEMBRO DE 2021. Disponível em: Acesso em: <https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-671-de-14-de-dezembro-de-2021> Acesso em: 05 out. 2024.

TSE. RESOLUÇÃO Nº 23.608, DE 18 DE DEZEMBRO DE 2019. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-608-de-18-de-dezembro-de-2019> Acesso em: 05 out. 2024.

SIGNIFICADOS. Narrativa. Disponível em: <https://www.significados.com.br/narrativa/> Acesso em: 08 out. 2024.

COUTO, Mari. O storytelling eleitoral e seus segredos. Disponível em: <https://blog.alcateiapolitica.com.br/segredos-storytelling-eleitoral/> Acesso em: 08 out. 2024.

VIOLÊNCIA POLÍTICA DE GÊNERO E O PAPEL POTENCIALIZADOR DO AMBIENTE DIGITAL

Camila Henning Salmoria[1]
Daiana Allessi Nicoletti Alves[2]

1. INTRODUÇÃO

A equidade de gênero no ambiente político ainda é um desafio significativo. Mulheres candidatas enfrentam uma forma específica de resistência: a violência política de gênero. Esse fenômeno inclui ataques verbais, simbólicos e, em alguns casos, até físicos, cujo objetivo é desqualificar, intimidar e silenciar mulheres em posições de poder. Tais ações prejudicam suas candidaturas e desencorajam futuras participações femininas na política, comprometendo a diversidade e a representatividade nos espaços de decisão.

O ambiente digital, que poderia ampliar a visibilidade e engajamento político, tem se tornado um terreno fértil para a propagação dessa violência. Plataformas de redes sociais e fóruns online facilitam a disseminação em massa de

1 Juíza de Direito do Tribunal de Justiça do Paraná, titular junto a 5ª Turma Recursal, especialista em Direito Digital pela ENFAM, graduada em Inteligência Artificial pela Universidade Positivo, integrante dos coletivos Todas da Lei e Antígona. Endereço eletrônico: chsa@tjpr.jus.br

2 Advogada. Doutoranda em Tecnologia e Sociedade pela Universidade Tecnológica Federal do Paraná (UTFPR). Mestra em Direitos Humanos e Políticas Públicas pela Pontifícia Universidade Católica do Paraná (PUCPR). Pós-graduada pela Escola da Magistratura do Paraná com especialização em Direito Aplicado e pela Escola da Magistratura Federal com especialização em Direito Público. Professora da Especialização em Direitos Humanos e Políticas Públicas da Pontifícia Universidade Católica do Paraná. (PUCPR) e da graduação em Direito da Uninter. Autora de diversos artigos relacionados aos direitos humanos das mulheres. Integrante do Coletivo Todas da Lei. Palestrante. Colunista. Endereço eletrônico: daianaallessi@gmail.com

discursos de ódio e ataques misóginos, muitas vezes realizados de forma anônima. Essa anonimidade dificulta a identificação dos agressores, ampliando o impacto negativo sobre as mulheres que se aventuram na política.

Estudos como o realizado pelo InternetLab evidenciam a gravidade da situação. Na pesquisa "Louca, Doida e Maluca: Misoginia Domina Ofensas a Candidatas Nessas Eleições" (Belin, 2022), foram coletados dados sobre as agressões direcionadas a candidatas durante as eleições brasileiras, revelando que as ofensas mais comuns são de cunho misógino e desqualificam as mulheres com base em estereótipos de instabilidade emocional. A maioria dos ataques analisados continha termos como "louca", "doida" e "maluca", minando a credibilidade das candidatas.

Além das ofensas verbais, muitas candidatas relatam ameaças de violência física e sexual, que, embora mais privadas, têm impacto psicológico profundo. Esses ataques se intensificam em momentos de maior visibilidade midiática, como debates e entrevistas, sugerindo que a exposição pública, essencial para o sucesso eleitoral, também aumenta a vulnerabilidade à violência de gênero.

Outro desafio enfrentado pelas mulheres na política são as campanhas de desinformação. Mensagens distorcidas e narrativas falsas são amplamente disseminadas nas redes, prejudicando a imagem pública das candidatas. Isso cria um ambiente de hostilidade e desconfiança que afeta negativamente suas chances de sucesso, além de gerar impactos emocionais e sociais duradouros.

Com base nos dados coletados e na análise de casos recentes, este artigo examina como o ambiente digital tem potencializado a violência política de gênero e suas implicações jurídicas. A partir de uma revisão bibliográfica e documental, busca-se compreender melhor esse fenômeno e discutir formas eficazes de enfrentá-lo no Brasil.

2. VIOLÊNCIA POLÍTICA DE GÊNERO NO BRASIL: UMA ANÁLISE CRÍTICA

A violência política de gênero é uma realidade crescente no Brasil, que se manifesta como um obstáculo significativo à participação plena das mulheres nos espaços de poder e decisão política. Embora conquistas importantes tenham sido alcançadas e implementadas com intuito de fomentar a igualdade entre os gêneros, a exemplo das cotas de candidaturas femininas e a promulgação de leis voltadas à proteção dos direitos das mulheres, a política institucional ainda se apresenta como um espaço predominantemente masculino, no qual mulheres enfrentam resistência, discriminação e violência direta.

O fenômeno da violência política de gênero consiste em ações, omissões ou comportamentos que têm como objetivo ou efeito prejudicar, impedir ou restringir a participação das mulheres na política em razão de seu gênero. Tais práticas podem ser manifestadas de várias formas, incluindo violência verbal, psicológica, física, sexual e institucional.

A promulgação da Lei nº 14.192/2021(Brasil, 2021) que tipifica e pune condutas que visam inibir, restringir ou impedir a participação de mulheres na seara eleitoral e decisória, foi uma política pública necessária para conter, ou pelo menos, minimizar a hegemonia violenta e patriarcal que insiste em ignorar e hostilizar o feminino nas esferas de poder e decisão.

De acordo com Alves (2023), as mulheres, mesmo com a conquista do voto e da possibilidade de serem votadas, ainda não conseguiram adentrar no espaço político eleitoral ante a pouca permeabilidade que um território tão masculino e patriarcal apresenta. O machismo, a dominação masculina, a violência estrutural do Estado são, em grande parte, responsáveis por esses baixos índices de participação das mulheres na política e vem ganhando espaço com as violências perpetradas inclusive, virtualmente, em desfavor de

candidatas e de eleitas.

É bastante crível e, portanto, nada falacioso, afirmar que a violência política é a gênese de todas as demais violências de gênero que perpetuam estereótipos de dominação, hegemonia androcêntrica e exclusão, pois, afastar as mulheres dos espaços de poder e decisão, das esferas nas quais se realiza a política institucional e a gestão social é uma maneira de garantir salvo-conduto para abusos, ferocidade e a ausência programada de perspectiva de gênero no processo democrático e eleitoral.

No contexto brasileiro, essa violência ocorre tanto dentro dos partidos políticos, como durante campanhas eleitorais, ou após a ocupação de cargos políticos. O principal foco é a intimidação, exclusão ou desmoralização das mulheres, muitas vezes levando à retirada de candidaturas, à renúncia de cargos ou à desistência de futuros envolvimentos políticos.

Os partidos políticos são, muitas vezes, ambientes hostis para as mulheres. Elas enfrentam dificuldades na obtenção de recursos para campanhas, são colocadas em posições menos competitivas e, em muitos casos, são vítimas de candidaturas fraudulentas, como o caso das chamadas candidaturas-laranja, nas quais mulheres são registradas apenas para cumprir as cotas mínimas sem qualquer apoio real para suas candidaturas. Esse tipo de fraude configura uma forma de violência política institucional, uma vez que essas mulheres são usadas como ferramentas políticas sem autonomia ou apoio.

Na esteira das facetas da violência política de gênero no Brasil, o abuso verbal e psicológico tem sido constante durante o processo eleitoral e, após a eleição, na condução dos mandatos, sessões, apartes e falas, violência que é perpetrada por adversários políticos, colegas de partido ou até mesmo eleitores e eleitoras. Mulheres que ocupam cargos de destaque ou que buscam uma carreira política frequente-

mente são alvo de insultos misóginos, ataques pessoais que se concentram em sua aparência, comportamento ou vida privada, em vez de suas capacidades ou propostas políticas.

As causas da violência política de gênero no Brasil estão enraizadas em fatores culturais, sociais e estruturais. A política, historicamente dominada por homens, é permeada por normas e práticas que excluem as mulheres ou as colocam em posições subordinadas, decorrentes da cultura colonial e patriarcal, que ainda predomina na sociedade brasileira e reforça a ideia de que o espaço público é um território masculino.

Outro fator importante é a percepção de ameaça que as mulheres representam para os homens que detêm o poder. À medida que as mulheres se tornam mais presentes e visíveis na política, aqueles que se beneficiam do status quo muitas vezes recorrem à violência e intimidação para manter sua posição de privilégio, pois não há vácuo no poder e para que uma mulher se sente na mesa das decisões institucionais, um homem precisará levantar e ceder seu lugar.

No entanto, a aplicação da lei ainda enfrenta desafios, pois, embora existam mecanismos legais, a subnotificação de casos de violência política de gênero permanece alta, e muitas mulheres continuam a sofrer com a falta de apoio institucional adequado. A implementação de medidas preventivas e punitivas ainda é limitada, com a responsabilização insuficiente dos perpetradores dessa violência que prevalecem sua conduta abusiva na forte tessitura social preconceituosa e patriarcal.

A jurisprudência brasileira começa a incorporar a questão da violência política de gênero, com o Tribunal Superior Eleitoral (TSE) atuando de forma mais assertiva na punição de práticas que violam os direitos das mulheres na política. Casos de candidaturas-laranja, em especial, têm sido alvo de maior escrutínio judicial, com partidos sendo penalizados pela utilização de candidaturas fictícias de mu-

lheres para burlar a legislação eleitoral.[3]

Outro caso emblemático foi o julgamento de agressões verbais dirigidas a parlamentares mulheres, em que o TSE considerou essas agressões como violência política de gênero. Essas decisões marcam um avanço no reconhecimento do direito das mulheres à participação política em condições de igualdade e segurança. Em decorrência da tipificação como crime da prática de atos de violência política de gênero, o Tribunal Superior Eleitoral tem protagonizado julgamentos que reconhecem esses abusos, inclusive quando concretizados por meio da comunicação de massa, como se depreende da seguinte ementa:

> ELEIÇÕES 2022. REPRESENTAÇÃO. PROPAGANDA ELEITORAL IRREGULAR. VIOLÊNCIA POLÍTICA DE GÊNERO. MEIOS DE COMUNICAÇÃO DE MASSA. EXPLORAÇÃO DE PRECONCEITOS. DEMOCRACIA PARITARIA. COMPETÊNCIA DA JUSTIÇA ELEITORAL. RECURSO A QUE SE DÁ PROVIMENTO. REPRESENTAÇÃO JULGADA

3 De acordo com a Súmula 73 do TSE, a fraude a cota de gênero consistente no que diz respeito ao percentual mínimo de 30% de candidaturas femininas, nos termos do artigo 10, parágrafo 3º, da Lei nº 9.504/1997, configura-se com a presença de um ou alguns dos seguintes elementos, quando os fatos e as circunstâncias do caso concreto assim permitirem concluir: votação zerada ou inexpressiva; prestação de contas zerada, padronizada ou ausência de movimentação financeira relevante; ausência de atos efetivos de campanha, divulgação ou promoção da candidatura de terceiros. Frisa-se que o reconhecimento do ilícito acarretará as seguintes consequências: cassação do Demonstrativo de Regularidade de Atos Partidários (Drap) da legenda e dos diplomas das candidatas e dos candidatos a ele vinculados, independentemente de prova de participação, ciência ou anuência deles; inelegibilidade daqueles que praticaram a conduta ou anuíram a ela, nas hipóteses de Ação de Investigação Judicial Eleitoral (Aije); nulidade dos votos obtidos pelo partido, com a recontagem dos quocientes eleitoral e partidário (artigo 222 do Código Eleitoral), inclusive para fins de aplicação do artigo 224 do Código Eleitoral, se for o caso. Ressalta-se que somente em 2023, nas sessões ordinárias presenciais, os ministros confirmaram a prática desse crime ao julgar 61 recursos. Em 2024, esse número ultrapassou mais de 20. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Julho/tse-tem-jurisprudencia-pacificada-sobre-fraude-a-cota-de-generopara-as-eleicoes-2024, Acesso em: 24 set. 2024.

> PROCEDENTE. 1. Compete à Justiça Eleitoral processar e julgar representação envolvendo declarações com conteúdo discriminatório, veiculadas contra mulheres ou quaisquer minorias, com reflexos no processo eleitoral, especialmente quando divulgadas em concessionária de serviço público. 2. Os meios de comunicação de massa, enquanto concessionários de serviço público, não podem ser agentes de discriminação e violência de qualquer natureza. 3. A veiculação de mensagens que explorem preconceitos, sobretudo contra determinada pessoa ou coletividade, compromete os princípios democráticos, desvirtuando o debate político e favorecendo a violência de gênero.4. Recurso a que se dá provimento. Representação julgada procedente. (Brasil, 2024)

A interseccionalidade também deve ser uma consideração central nas políticas de enfrentamento da violência política de gênero. Mulheres negras, indígenas, LGBTQIAPN+ e aquelas de classes sociais menos favorecidas estão particularmente vulneráveis a essa violência e devem ser foco de iniciativas específicas de proteção e empoderamento.

Cabe menção a esse excerto muito bem fundamentado que escancara o racismo, a misoginia e os múltiplos preconceitos que permeiam a sociedade brasileira e surtem efeitos deletérios em ambiente decisório institucional:

> **O racismo no Brasil é estrutural.** Isso significa que, mais do que um problema individual, o racismo está inserido nas estruturas políticas, sociais e econômicas e no funcionamento das instituições, o que permite a reprodução e perpetuação da desigualdade de oportunidades da população negra. A desigualdade racial é escancarada por diversas estatísticas, que demonstram que, em todos os campos, desde o acesso à educação até a segurança pública, negros são desfavorecidos e marginalizados. (...) **Como fenômeno intrinsecamente relacionado às relações de poder e dominação, o racismo se manifesta especialmente no âmbito político–eleitoral.** Nas eleições gerais de 2018, embora 47,6% dos candidatos que concorreram fossem negros, entre os eleitos, estes representaram apenas 27,9%. Um dos principais fatores

que afetam a viabilidade das candidaturas é o financiamento das campanhas. Quanto ao tema, verifica–se que, em 2018, houve efetivo incremento nos valores absolutos e relativos das receitas das candidatas mulheres por força das decisões do STF e do TSE. Enquanto em 2014 a receita média de campanha das mulheres representava cerca de 27,8% da dos homens, em 2018, tal receita representou 62,4%. No entanto, ao se analisar a intersecção entre gênero e raça, verifica–se que a política produziu efeitos secundários indesejáveis. Estudo da FGV Direito relativo à eleição para Câmara dos Deputados apontou que mulheres brancas candidatas receberam percentual de recursos advindos dos partidos (18,1%) proporcional às candidaturas (também de 18,1%). No entanto, candidatos negros continuaram a ser subfinanciados pelos partidos. Embora mulheres negras representassem 12,9% das candidaturas, receberam apenas 6,7% dos recursos. Também os homens negros receberam dos partidos recursos (16,6%) desproporcionais em relação às candidaturas (26%). Apenas os homens brancos foram sobrefinanciados (58,5%) comparativamente ao percentual de candidatos (43,1%). No mundo contemporâneo, a igualdade se expressa particularmente em três dimensões: a igualdade formal, que funciona como proteção contra a existência de privilégios e tratamentos discriminatórios; a igualdade material, que corresponde às demandas por redistribuição de poder, riqueza e bem-estar social; e a igualdade como reconhecimento, significando o respeito devido às minorias, sua identidade e suas diferenças. **A ordem constitucional não apenas rejeita todas as formas de preconceito e discriminação, mas também impõe ao Estado o dever de atuar positivamente no combate a esse tipo de desvio e na redução das desigualdades de fato. Sob o prisma da igualdade, há um dever de integração dos negros em espaços de poder, noção que é potencializada no caso dos parlamentos.** E que a representação de todos os diferentes grupos sociais no parlamento é essencial para o adequado funcionamento da democracia e para o aumento da legitimidade das decisões tomadas. Quando a representação política é excludente, afeta–se a capacidade de as decisões e políticas públicas refletirem as vontades e necessidades das minorias sub–representadas. Para além do impacto na agenda públi-

> ca, o aumento da representatividade política negra tem o efeito positivo de desconstruir o papel de subalternidade atribuído ao negro no imaginário social e de naturalizar a negritude em espaços de poder. (...) A violência política de gênero no Brasil é um desafio persistente que impede a plena realização da igualdade de gênero na política. Embora leis como a Lei nº 14.192/2021 representem um avanço significativo, é essencial que o país continue a desenvolver políticas públicas eficazes, promover mudanças culturais e fortalecer as instituições para garantir que as mulheres possam participar da política em condições de igualdade. Somente com a superação dessas barreiras estruturais será possível construir um sistema político verdadeiramente inclusivo e democrático. (Brasil, 2020. Grifamos)

Verifica-se que a violência de gênero performa várias nuances que inflacionam a nocividade dos abusos intencionados a afastar as mulheres do espaço público político brasileiro, e muito embora não seja uma exclusividade do nosso país, vivenciamos uma realidade na qual a violência material e concreta assume contornos ainda mais perigosos quando reproduzida em ambiente virtual com o auxílio da internet e de todos os artefatos tecnológicos dela decorrentes, sem filtros potencial ainda mais excludente em relação ao gênero e as interseccionalidades decorrentes e desconsideradas pela cultura patriarcal imposta e ainda vigente.

3. POTENCIALIDADE DO AMBIENTE DIGITAL NA AMPLIFICAÇÃO DA VIOLÊNCIA

O ambiente digital, com suas características intrínsecas de conectividade, instantaneidade e anonimato, exerce um papel central na amplificação da violência política de gênero. Embora a internet e as redes sociais ofereçam ferramentas poderosas para promover a inclusão e a participação política, elas também se tornaram espaços propícios para a reprodução e intensificação de comportamentos misóginos e violentos. Como salientado por Vint Cerf (Salmoria, 2022), um dos fundadores da internet, a realidade online reflete a

sociedade como um todo. Com a disseminação dos celulares e das redes sociais, a violência, antes restrita ao mundo offline, passou a manifestar-se no ambiente virtual, adquirindo novos contornos e formatos.

Nesse contexto, a impossibilidade de violência física é compensada pela proliferação de formas de violência psicológica e emocional. O anonimato, a velocidade de transmissão, a amplitude de propagação e a permanência dos conteúdos não só facilitam a frequência dos abusos, mas também aumentam sua gravidade. O universo online, sendo um reflexo da realidade offline, deveria ser um espaço de fortalecimento do diálogo e do pluralismo de ideias em uma sociedade democrática.

Contudo, quando condutas buscam silenciar ou reprimir a livre manifestação do pensamento das mulheres, retirando-lhes espaço de fala ou reduzindo-as à condição de meros objetos de discussão, o próprio alicerce social é comprometido. A replicação das práticas machistas do mundo offline no ambiente online não apenas perpetua a opressão, mas também atenta contra a construção da identidade individual das mulheres.

O ambiente digital é marcado por fatores que facilitam a rápida e ampla disseminação de conteúdos, incluindo discursos de ódio e ataques pessoais. O anonimato oferecido pelas plataformas digitais protege a identidade dos agressores, permitindo que atuem sem medo de retaliação ou punição, expressando comportamentos que dificilmente manifestariam em interações presenciais. A viralidade inerente ao ambiente digital permite que conteúdos misóginos sejam disseminados em velocidade e escala inigualáveis, atingindo uma audiência significativamente maior do que seria possível em contextos offline. Comentários, memes e montagens que desqualificam candidatas mulheres podem ser compartilhados milhares de vezes em questão de horas, perpetuando estereótipos e contribuindo para uma cultura de deslegitima-

ção e silenciamento das vozes femininas na política.

A violência política de gênero não se manifesta apenas em atos isolados, mas se materializa através de um conjunto de práticas discursivas que se amplificam no ambiente digital, revelando uma vulnerabilidade linguística que coloca as mulheres em situações de risco contínuo (Vallada, 2023).

Essa vulnerabilidade linguística das mulheres em ambientes digitais é crucial para compreender como essas ameaças se enraízam e se expandem. A estrutura dessas ameaças é reforçada pela citacionalidade dos enunciados, onde frases ameaçadoras são repetidas e recontextualizadas em diferentes plataformas, criando um efeito de eco que multiplica o impacto da violência original. Essa citacionalidade não apenas amplia o alcance das ameaças, mas também perpetua um ciclo de violência que torna a vítima ainda mais vulnerável a novas agressões (Vallada, 2023).

A citacionalidade e a repetição desempenham um papel central nesse processo. No ambiente digital, as ameaças são reproduzidas em uma escala antes inimaginável, circulando através de postagens, comentários, memes e outras formas de conteúdo digital. Esse fenômeno, denominado "legado citacional", transforma os enunciados ameaçadores em elementos que, ao serem repetidos e transformados, adquirem uma nova força. Cada repetição não só reafirma a ameaça, mas também a potencializa, criando um cenário em que a violência linguística se aproxima perigosamente de se transformar em violência física. A repetição incessante dessas ameaças serve como um lembrete constante da vulnerabilidade da vítima, intensificando o impacto psicológico e social das agressões (Vallada, 2023).

A visibilidade proporcionada pelo ambiente digital é uma faca de dois gumes para as mulheres na política. Por um lado, as redes sociais e outras plataformas online oferecem uma vitrine para que candidatas possam se comunicar diretamente com o público, mobilizar apoiadores e promover suas

agendas. No entanto, essa visibilidade também as torna alvos fáceis para ataques misóginos, uma vez que suas aparições públicas e declarações são frequentemente distorcidas e usadas como munição por aqueles que desejam deslegitimá-las.

Essa dinâmica de poder é exacerbada pela cultura de "trollagem" e pela presença de comunidades online que se organizam em torno da prática de assediar figuras públicas, especialmente mulheres. Essas comunidades, frequentemente operando com base em ideologias extremistas ou machistas, utilizam o poder coletivo para lançar campanhas coordenadas de ódio e desinformação. As candidatas mulheres são particularmente vulneráveis a esses ataques, que não apenas buscam humilhá-las, mas também intimidar outras mulheres que possam estar considerando entrar na política.

3.1. Exemplos de Agressões Online

A pesquisa conduzida pelo InternetLab oferece uma análise detalhada sobre a natureza e a intensidade das agressões direcionadas a mulheres candidatas durante os períodos eleitorais. Ela revela que o ambiente digital não só facilita a propagação da violência política de gênero, mas também a intensifica, criando uma atmosfera de hostilidade contínua para as mulheres que se aventuram na política.

O caso de Manuela d'Ávila durante as eleições municipais de 2020 em Porto Alegre ilustra de forma emblemática os desafios enfrentados por mulheres na política, especialmente no ambiente virtual. Manuela, candidata à prefeitura, foi alvo de uma série de ataques no segundo turno da eleição, que não se limitaram à sua atuação política, mas também invadiram aspectos de sua aparência, personalidade e vida pessoal. Esses ataques foram amplamente disseminados nas redes sociais e em outras plataformas digitais, ampliando os danos à sua imagem pública (De Souza, 2023).

Entre as acusações infundadas, circularam mentiras de que Manuela teria feito compras milionárias em Miami,

junto com outras histórias fabricadas com o objetivo claro de desmoralizá-la perante o público. Além disso, ela foi vítima de montagens fotográficas indecentes e de difamações constantes em redes sociais, onde foi retratada de forma pejorativa e vinculada a estereótipos negativos (De Andrade, 2023).

A violência virtual contra Manuela foi caracterizada principalmente pela disseminação de desinformação e fake news, usadas como armas para minar sua credibilidade e criar uma narrativa negativa que visava desqualificá-la perante o eleitorado. A circulação dessas fake news foi intensa, com milhares de compartilhamentos em plataformas digitais, o que distorceu a percepção pública de sua candidatura. Esses ataques não apenas afetaram a campanha de Manuela, mas também contribuíram para perpetuar estereótipos de gênero, reforçando a ideia de que as mulheres na política são menos competentes ou legítimas do que seus colegas homens.

Os espaços de comentários nas notícias publicadas sobre Manuela no portal UOL tornaram-se terreno fértil para a expressão de ódio e preconceito. Muitos comentários desconsideraram a gravidade da violência política de gênero, relativizando os ataques com declarações como: "A UOL tem provas de que as notícias são falsas? Apresente-as por favor," ou "Se essa defensora de coisas podres ganhar, o que acho impossível, Porto Alegre está perdida!" Outros reforçavam os insultos e ofensas, atacando não apenas sua posição política, mas também aspectos pessoais, como no comentário: "Fingir ser católica e se vestir igual a uma dama não é fake news??? Fora esquerda!!!!!" (De Souza, 2023). Nesse ambiente, os leitores não apenas consumiam a desinformação, mas também a reproduziam e amplificavam, criando um ciclo contínuo de violência simbólica e psicológica contra a candidata.

Outro exemplo significativo é o de Isa Penna, deputada estadual pelo PSOL-SP, que também foi alvo de ataques no ambiente virtual. Após sofrer um episódio de assédio

dentro da Assembleia Legislativa de São Paulo, onde foi tocada indevidamente por um colega parlamentar, Isa enfrentou uma nova onda de violência online. Nas redes sociais, a deputada foi alvo de ofensas sexistas e ameaças, numa tentativa clara de silenciá-la e minimizar o gravíssimo episódio de assédio que havia sofrido (De Andrade, 2023).

Ficou famoso ainda o caso de Talíria Petrone, deputada federal, que recebeu inúmeras ameaças de morte e mensagens racistas, forçando-a a aumentar sua segurança pessoal (Costa, 2023).

Uma pesquisa adicional com dados históricos demonstra que a violência política de gênero no ambiente virtual tem se intensificado, especialmente contra mulheres negras, durante os períodos eleitorais no Brasil entre 2016 e 2022 (Costa, 2023). Dados indicam que cerca de 60% das candidatas negras que participaram das eleições em 2018 relataram ter sofrido algum tipo de violência online, seja por meio de ameaças, difamações ou assédio. Quando se considera o fator interseccionalidade, os números se tornam ainda mais expressivos. Por exemplo, 70% das mulheres negras que se candidataram a cargos públicos em 2020 foram alvo de campanhas de difamação online, evidenciando um aumento significativo em comparação com as eleições anteriores.

O caso da vereadora Marielle Franco, assassinada em 2018, é emblemático, pois continuou a ser alvo de ataques digitais mesmo após sua morte. As campanhas contra ela incluíam a disseminação de fake news e discursos de ódio, amplamente compartilhados em redes sociais e fóruns online.

3.2 Aspectos jurídicos, legislação e jurisprudência

Em termos legislativos, a promulgação da Lei 14.192/2021 representa um marco significativo na luta contra a violência política de gênero no Brasil. Esta lei foi criada para prevenir, reprimir e combater a violência política con-

tra as mulheres durante as eleições e no exercício de seus direitos políticos e funções públicas. A lei estabelece que toda ação, conduta ou omissão com a finalidade de impedir, obstaculizar ou restringir os direitos políticos das mulheres constitui violência política de gênero. Além disso, a lei tipifica como crime eleitoral atos como assediar, constranger, humilhar, perseguir ou ameaçar candidatas ou detentoras de mandatos eletivos, utilizando-se de discriminação relacionada ao gênero, raça ou etnia.

Um aspecto inovador da Lei 14.192/2021 é a sua aplicação ao ambiente virtual. A legislação prevê o aumento das penas para crimes de calúnia, difamação e injúria quando praticados por meio da internet ou redes sociais, especialmente se envolverem discriminação contra a condição de mulher. Isso é particularmente relevante no contexto atual, onde o ambiente virtual é um dos principais espaços de manifestação política e, infelizmente, também de ataques misóginos e preconceituosos.

O pioneirismo na aplicação deste conceito foi evidenciado em um julgamento do Tribunal Regional Eleitoral do Rio de Janeiro (TRE-RJ) durante as eleições de 2020. Neste caso, uma candidata à Prefeitura do Rio de Janeiro foi alvo de uma intensa campanha de desinformação, com ataques voltados à sua vida pessoal, especialmente em relação ao seu passado amoroso. Esses ataques foram considerados um exemplo claro de violência política de gênero, já que visavam descredibilizar a candidata explorando aspectos de sua vida íntima, com o objetivo de influenciar negativamente a opinião pública (Aieta, 2023).

A Procuradoria Regional Eleitoral do Rio de Janeiro desempenhou um papel crucial ao construir e argumentar o conceito de violência política de gênero nesse julgamento. O parecer da Procuradoria ressaltou que a exploração da vida íntima de mulheres em campanhas eleitorais, especialmente em plataformas digitais, é uma forma de violência que

perpetua a desigualdade de gênero e dificulta a participação feminina na política. Esse julgamento não apenas aplicou a nova legislação, mas também estabeleceu um precedente importante para futuras interpretações judiciais sobre a violência política de gênero no ambiente virtual.

4. CONSIDERAÇÕES FINAIS

A violência política de gênero é um desafio complexo que persiste no cenário brasileiro, e seu impacto é exacerbado pela amplificação no ambiente digital. As plataformas online, inicialmente vistas como espaços de democratização e promoção de vozes marginalizadas, tornaram-se também terrenos férteis para a proliferação de discursos de ódio e ataques misóginos. O anonimato e a rapidez com que informações, ou desinformações, se espalham nas redes sociais aumentam a vulnerabilidade das mulheres que se candidatam ou ocupam cargos públicos, afetando negativamente suas campanhas e suas experiências no espaço político.

Os dados revelados pelo InternetLab demonstram a magnitude dessa violência, com uma concentração expressiva de ataques misóginos dirigidos às candidatas mulheres durante o período eleitoral. Termos desqualificadores baseados em estereótipos de gênero são amplamente utilizados para minar a credibilidade e a legitimidade dessas mulheres, reforçando preconceitos enraizados em uma sociedade patriarcal. Além dos insultos verbais, a disseminação de desinformação e as ameaças de violência física e sexual geram um ambiente de constante intimidação, que afeta não apenas a saúde mental das candidatas, mas também sua vontade de permanecer no cenário político.

O avanço legislativo no Brasil, com a promulgação da Lei nº 14.192/2021, é um passo importante na tentativa de coibir essa violência. No entanto, a aplicação dessa lei ainda enfrenta desafios, especialmente no que diz respeito à responsabilização dos agressores no ambiente digital. Em-

bora a legislação represente um marco significativo, é essencial que haja um fortalecimento das instituições e uma maior regulamentação das plataformas digitais para garantir que os espaços online se tornem ambientes seguros e inclusivos para a participação política das mulheres.

Para superar esse quadro, é necessária uma combinação de políticas públicas eficazes, iniciativas de conscientização social e maior rigor na aplicação das leis. Apenas com a integração de ações preventivas, punitivas e educativas será possível reduzir os efeitos da violência política de gênero e promover a participação plena e igualitária das mulheres na política. A construção de um ambiente político inclusivo depende não apenas de esforços legislativos, mas também de uma transformação cultural que repudie a misoginia e celebre a diversidade nas esferas de poder.

REFERÊNCIAS

AIETA, Vânia Siciliano. A construção do conceito de violência política de gênero nas campanhas eleitorais. Revista Científica do CPJM, v. 2, n. Especial, p. 115-126, 2023. Disponível em: https://rcpjm.cpjm.uerj.br/revista/article/view/174. Acesso em: 26 ago. 2024.

ALVES, Daiana Allessi Nicoletti. As lutas feministas e o enfrentamento à desigualdade de gênero na política institucional brasileira. São Paulo: Dialética, 2023.

BELIN, L. Louca, doida e maluca: misoginia domina ofensas a candidatas nessas eleições | InternetLab. 6/09/2022. Disponível em: <https://internetlab.org.br/pt/noticias/louca-doida-e-maluca-misoginia-domina-ofensas-a-candidatas-nessas-eleicoes/>. Acesso em: 27 set. 2024.

BRASIL. Tribunal Superior Eleitoral. Recurso Em Representação 060128334/DF, Relator(a) Min. Kassio Nunes Marques, Acórdão de 07/03/2024, publicado no(a) Diário de Justiça Eletrônico 96, data 06/06/2024. Disponível em: https://jurisprudencia.tse.jus.br/#/jurisprudencia/pesquisa?expressaoLivre=viol%C3%AAncia%20pol%C3%ADtica%20de%20

g%C3%AAnero%20&tipoDecisao=Ac%25C3%25B3rd%-25C3%25A3o%252CResolu%25C3%25A7%25C3%25A3-o%252CDecis%25C3%25A3o%2520sem%2520resolu%-25C3%25A7%25C3%25A3o&params=s Acesso em 25 set. 2024.

BRASIL. Tribunal Superior Eleitoral. Consulta 060030647/DF, Relator(a) Min. Luís Roberto Barroso, Acórdão de 25/08/2020, publicado no(a) Diário de Justiça Eletrônico 199, data 05/10/2020, pag. 0 Disponível em: https://jurisprudencia.tse.jus.br/#/jurisprudencia/pesquisa?expressaoLivre=viol%C3%AAncia%20pol%C3%ADtica%20de%20g%C3%AAnero%20&tipoDecisao=Ac%25C3%25B3rd%-25C3%25A3o%252CResolu%25C3%25A7%25C3%25A3-o%252CDecis%25C3%25A3o%2520sem%2520resolu%-25C3%25A7%25C3%25A3o&params=s Acesso em 26 set. 2024.

BRASIL. Tribunal Superior Eleitoral. TSE tem jurisprudência pacificada sobre fraude à cota de gênero para as Eleições 2024. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2024/Julho/tse-tem-jurisprudencia-pacificada-sobre-fraude-a-cota-de-generopara-as-eleicoes-2024>.

BRASIL. Lei 14.192 de 04 de agosto de 2021.Estabelece normas para prevenir, reprimir e combater a violência política contra a mulher; e altera a Lei nº 4.737, de 15 de julho de 1965 (Código Eleitoral), a Lei nº 9.096, de 19 de setembro de 1995 (Lei dos Partidos Políticos), e a Lei nº 9.504, de 30 de setembro de 1997 (Lei das Eleições), para dispor sobre os crimes de divulgação de fato ou vídeo com conteúdo inverídico no período de campanha eleitoral, para criminalizar a violência política contra a mulher e para assegurar a participação de mulheres em debates eleitorais proporcionalmente ao número de candidatas às eleições proporcionais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14192.htm Acesso em 26 ago. 2024.

COSTA, Lorraina Silva; LEÃO, Ingrid Viana. Violência Política nas Redes Sociais Contra Mulheres Negras nas Eleições Brasileiras entre 2016 a 2022. Universidade Estadual de Mato Grosso do Sul (UEMS). Seminário em Políticas Públicas e Direitos Humanos: Pesquisa e Interdisciplinaridade, Paranaíba, 10 e 11 de março de 2023.

DE ANDRADE LIMA, Elizabeth Christina; DO NASCIMENTO COSTA, Ana Paula Guedes. À flor da pele: sofrimento, misoginia e violência política de gênero no Brasil. Thelma Maria Grisi Velôso (Organizadoras), p. 65-107. Disponível em: <https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Genero-diversidade-e-relacoes-de-poder.pdf#page=65>. Acesso em: 26 ago. 2024.

DE SOUZA, Caroline et al. Violência Política de Gênero: A Circulação de Sentidos em Episódios Comunicacionais das Eleições de 2020. Revista Comunicando, v. 12, n. 1, p. e023005-e023005, 2023. Disponível em: https://doi.org/10.58050/comunicando.v12i1.314. Acesso em: 26 ago. 2024.

SALMORIA, Camila Henning; ALVES, Daiana Allessi Nicoletti; BAZZO, Mariana Seifert. Violência de Gênero e Crimes Cometidos no Mundo Virtual Contemporâneo. Revista CEVID, v. 2, n. 3, p. 1-15. Disponível em: https://revistacevid.tjpr.jus.br/documents/d/revista-cevid/revista-eletronica-cevid-v2-n3-atualizada-1. Acesso em: 26 ago. 2024.

VALLADA, Amanda Diniz; PINTO, Joana Plaza. Vulnerabilidade linguística em ambientes digitais e as forças escalares da ameaça contra mulheres. Cadernos de Linguagem e Sociedade**,** Brasília, v. 24, n. 2, p. 326-340, jul./dez. 2023. DOI: 10.26512/les.v24i2.50742. Disponível em: https://doi.org/10.26512/les.v24i2.50742. Acesso em: 26 ago. 2024.

INCLUSÃO DIGITAL E PARTICIPAÇÃO ELEITORAL: PERSPECTIVAS E DESAFIOS

Carolina Elisa Margonari[1]

1. CULTURA DIGITAL E AS NOVAS TECNOLOGIAS DIGITAIS E A SOCIEDADE.

O modo de explorar e vivenciar a cultura no país passou por transformações significativas, impulsionadas principalmente pela adoção de novas tecnologias, que alteraram profundamente a dinâmica social. A noção de espaço e tempo foi reconfigurada pelas múltiplas formas de acessar conteúdo, como música, filmes e séries. E assim como pela facilidade de obter informações, adquirir conhecimento, se comunicar e interagir com o governo. Essa transformação digital possibilitou o surgimento de novas práticas, comportamentos e valores, resultantes do uso contínuo das tecnologias digitais, por meio do acesso à internet, redes sociais, dispositivos móveis e outras formas de comunicação online.

Essas mudanças moldaram o novo conceito de cultura, a cultura digital, cujos principais elementos incluem a democratização da informação, a criação de novas formas de expressão cultural e artística, e a transformação das relações sociais e econômicas.[2]

A cultura digital pode ser considerada uma expressão da atualidade, que surge com o advento das novas tecnologias e resulta em novas formas de interação pessoal, cultural

1 Advogada com atuação na área de Propriedade Intelectual, Contratos e Proteção de Dados, atuante no Terceiro Setor, com certificação Data Privacy Brasil, e autora de diversos artigos.

2 Cultura digital. Disponível em: https://pt.wikipedia.org/wiki/Cultura_digital. Acesso em: 24 set. 2024.

e política, todas vivenciadas e mediadas no ambiente virtual. Nesse contexto, ela vai além do conceito tradicional de cultura vinculada à tecnologia, evoluindo como uma extensão da cibercultura, com o potencial de impulsionar a criatividade, a produtividade e a liberdade.[3]

A transformação digital remodelou profundamente a maneira como a cultura é vivenciada e explorada no Brasil, redefinindo também as interações sociais, culturais e econômicas. As mudanças ao acesso à informação e o surgimento de novas formas de expressão trouxeram tanto oportunidades quanto desafios. Nesse contexto, a conectividade e a tecnologia passam a desempenhar papéis centrais na construção de uma cultura.

2. INCLUSÃO DIGITAL E CONECTIVIDADE SIGNIFICATIVA

O tema da inclusão digital tem sido amplamente debatido nas organizações da sociedade civil, e, nos últimos anos, estudos têm enfatizado a crescente necessidade de aprofundar a compreensão sobre o assunto, dada a sua complexidade. A edição do Caderno NIC.br de Estudo Setorial associa a inclusão digital à "conectividade significativa", destacando que "nos últimos anos, a literatura sobre inclusão digital tem incorporado o debate sobre a relação da conectividade significativa com o empoderamento de indivíduos e comunidades socialmente marginalizados, além de sua importância na redução das desigualdades digitais (Alliance for Affordable Internet [A4AI], 2022a; Radhakrishnan et al., 2023; Katz & Gonzalez, 2016)".[4]

3 AMARAL, Vinícius R. A. (2012). Os caminhos da cultura digital: a emergência de novas práticas e enunciados políticos. 2012. 108 f. Dissertação (Mestrado) – Mestrado em Ciências Sociais, Pontifícia Universidade Católica de São Paulo, São Paulo.

4 Núcleo de Informação e Coordenação do Ponto BR. Conectividade significativa [livro eletrônico]: propostas para medição e o retrato da população no Brasil.

No mesmo material, é destacado que o conceito de inclusão digital vai além do simples acesso à internet, abrangendo diversos obstáculos enfrentados pelos usuários, como a qualidade do acesso e da conexão, os dispositivos utilizados para acessar a rede, o custo das franquias de dados, as habilidades digitais, além da segurança e privacidade no ambiente virtual. Seguindo essa mesma linha de pensamento, a conectividade significativa se concentra em um tipo de acesso que não se limita à presença online, mas que promove um uso efetivo e produtivo da internet, permitindo que as pessoas participem de forma ativa e obtenham benefícios concretos nos âmbitos social, econômico e educacional.[5]

A definição de conectividade significativa pode, portanto, ser considerada abrangente, já que envolve diversos aspectos que auxiliam na compreensão de como as pessoas interagem com o mundo digital.

Fica cada vez mais claro que o simples uso da internet não basta para entender plenamente o conceito de inclusão digital. Como consequência, essa limitação afeta diretamente o entendimento de conectividade, pois não é mais viável associar o nível de conectividade de um país focando apenas ao número de usuários conectados.[6]

Ficou evidente que a inclusão digital vai além do simples acesso à internet, envolvendo a qualidade do acesso, a frequência de uso, a capacidade de realizar atividades online de forma fluida e a relevância do conteúdo para a vida dos

Tradução Ana Zuleika Pinheiro Machado. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2024. PDF.

5 Núcleo de Informação e Coordenação do Ponto BR. Conectividade significativa [livro eletrônico]: propostas para medição e o retrato da população no Brasil. Tradução Ana Zuleika Pinheiro Machado. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2024. PDF.

6 Núcleo de Informação e Coordenação do Ponto BR. Conectividade significativa [livro eletrônico]: propostas para medição e o retrato da população no Brasil. Tradução Ana Zuleika Pinheiro Machado. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2024. PDF.

usuários. E a conectividade significativa considera como a tecnologia possibilita uma participação mais ativa e produtiva na sociedade digital, promovendo não apenas a conexão, mas também o pleno uso dos recursos digitais disponíveis. A associação entre esses dois temas contribui para a redução das desigualdades, promovendo a diminuição da exclusão digital.

3. INFORMATIZAÇÃO ELEITORAL

Para acompanhar todo esse avanço tecnológico, muitos órgãos públicos tiveram que atualizar seus modelos de atuação para proporcionar uma melhor conexão com os seus cidadãos. A Justiça Eleitoral seguiu o mesmo caminho, informatizando a sua estrutura para melhorar o exercício da democracia brasileira, através da utilização de urnas eletrônicas, cadastramento da biometria facial dos eleitores e eleitoras, a criação de canais de comunicação em aplicativos de mensagens instantâneas e em diversas redes sociais.[7]

A informatização traz benefícios ao facilitar um contato mais direto entre o órgão eleitoral e os eleitores. No entanto, essa facilidade esbarra com a realidade do país. Conforme pesquisa realizada pelo NIC.br, em 2023, apenas "84% da pessoas no Brasil são usuárias de Internet", apesar de estarmos próximos de uma "universalidade do acesso à Internet", ainda existem pessoas que estão offline.[8] Do outro lado, temos aqueles que estão online, mas não dispõem de uma conectividade significativa, comprometendo seu direito de votar ou de acessar informações que auxiliem no exercício consciente desse direito.

---

7 BRASIL. Tribunal Superior Eleitoral. Portal da Justiça Eleitoral. Disponível em: https://www.justicaeleitoral.jus.br/. Acesso em: 25 set. 2024.

8 Núcleo de Informação e Coordenação do Ponto BR. Conectividade significativa [livro eletrônico]: propostas para medição e o retrato da população no Brasil. Tradução Ana Zuleika Pinheiro Machado. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2024. PDF.

Embora a informatização da justiça eleitoral seja essencial, ela pode acabar excluindo certos cidadãos de participarem do debate eleitoral.

4. DESAFIOS DA DEMOCRACIA DIGITAL

"Um Estado proativo tem a capacidade de implantar procedimentos e instrumentos de participação popular que levarão a uma substancial participação política dos cidadãos."[9]

Com as novas formas de interações digitais, o exercício da democracia passa a ter um novo ambiente de aplicação.

Esse novo contexto social, impulsionado pela tecnologia, coloca o indivíduo e suas capacidades cognitivas no centro do processo, evidenciando a necessidade de adquirir conhecimento e compreensão desse fenômeno. Com isso, surge a busca por equilíbrio dentro da sociedade informacional, desafiando a democracia digital a enfrentar as complexidades que emergem dessa nova interação entre tecnologia e práticas democráticas.[10] Nesse sentindo, Castells reforça essa visão, afirmando que a base dessa relação está fundamentada na capacidade das pessoas de gerar e processar informações, bem como de transformar esses dados em conhecimento.[11]

Essa nova configuração de democracia traz desafios significativos para os governos, ao criar responsabilidades no sentido de garantir o acesso à informação de forma segura, transparente e abrangente para toda a população. Além

9 PINHO, José A. G. et al. (2012). Limites e possibilidades da política e da democracia na Internet: um olhar a partir da realidade brasileira. In: PINHO, José A. G. (org.). Estado, sociedade e interações digitais: expectativas democráticas. Salvador: EDUFBA.

10 ELEUTÉRIO, Kênia I. P. et al. (2021). O meme político: Uma análise na perspectiva tecnológica e democrática. Research, Society and Development. Paraná Eleitoral.

11 CASTELLS, Manuel. O Poder da Identidade. São Paulo: Paz e Terra, 1999.

disso, impõe a obrigação de proteger os dados pessoais dos usuários, assegurando o respeito aos direitos fundamentais dos cidadãos e fortalecendo a confiança nas instituições democráticas.

Em contrapartida, a democracia digital proporciona aos cidadãos a chance de participar ativamente do processo democrático no espaço virtual. Ela possibilita uma troca diversificada de ideias, conhecimentos, vivências e práticas tanto políticas quanto culturais. Com o apoio de tecnologias de comunicação e informação fornecidas pelas instituições democráticas, essa modalidade estabelece uma nova forma de entender a democracia, referida como democracia digital.[12]

5. IMPACTOS DO AMBIENTE DIGITAL NAS ELEIÇÕES

O primeiro desafio a ser destacado quando se trata de ambiente digital e eleições é a segurança. É essencial garantir um ambiente digital protegido, livre de desinformações e/ou Fake News, para assegurar uma eleição justa e transparente. Isso reflete a fala do diretor da Escola Judiciária Eleitoral (EJE) do Tribunal Superior Eleitoral (TSE), ministro Floriano de Azevedo Marques Neto, durante o seminário "Democracia – Eleições no Mundo Digital", quando afirmou: "A missão da Justiça Eleitoral é assegurar a lisura das eleições e, principalmente, garantir que, no período eleitoral, o eleitor tenha plenas condições, em um ambiente saudável, de formar a sua convicção".[13]

Conforme demonstrado em pesquisa de opinião rea-

12 PINHO, José A. G. et al. Democracia digital na área de administração: um levantamento da construção do campo no Brasil. Cadernos Gestão Pública e Cidadania, 2019.

13 Seminário debate desafios das eleições no mundo digital. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Abril/seminario-debate-desafios-das-eleicoes-no-mundo-digital. Acesso em: 28 set. 2024.

lizada em 2019, pelo Instituto Data Senado, as redes sociais possuem forte influência nos eleitores, em muitos casos, elas são a única fonte de informação diária. Conforme mencionado na pesquisa: "Quase metade dos entrevistados (45%) afirmaram ter decidido o voto levando em consideração informações vistas em alguma rede social. E a principal fonte de informação do brasileiro hoje é o aplicativo de troca de mensagens WhatsApp, segundo o levantamento. Das 2,4 mil pessoas entrevistadas, 79% disseram sempre utilizar essa rede social para se informar."[14]

Outro ponto de preocupação é o uso da Inteligência Artificial sem a devida responsabilização, ética e transparência. É fundamental que haja um cuidado coletivo em prol da sociedade. Uma possível solução para esses pontos de atenção seria a revisão do processo eleitoral, principalmente no que se refere à aplicação de sanções para os ilícitos eleitorais. O modelo atual de controle e punição tem se mostrado ineficaz frente aos avanços tecnológicos, o que torna necessária a implementação de novos mecanismos de sanções. Essa sugestão foi levantada por Marilda Silveira, representante do Instituto de Ensino, Desenvolvimento e Pesquisa (IDP), durante um debate promovido pelo Conselho de Comunicação Social em audiência pública.[15]

Um ambiente digital vulnerável pode gerar impactos negativos significativos em uma eleição, comprometendo a confiança no processo democrático. Por isso, é essencial criar um ecossistema digital robusto e seguro, capaz de proteger contra ameaças à democracia. Dessa forma, a integridade do

14 BRASIL. Senado Federal. Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/12/12/redes-sociais-influenciam-voto-de-45-da-populacao-indica-pesquisa-do-datasenado. Acesso em: 28 set. 2024.

15 Eleições: Especialistas defendem ambiente digital seguro e transparente. TV Senado. Disponível em: https://www.youtube.com/watch?v=ye0UzLO9Kos. Acessado em 28/09/2024.

ambiente digital é preservada, assegurando que os eleitores possam participar de maneira informada e com segurança.

6. A IMPORTÂNCIA DA INCLUSÃO DIGITAL NA PARTICIPAÇÃO ELEITORAL

Com a crescente migração das relações do universo offline para o online, consequentemente, a forma como o indivíduo busca exercer sua cidadania também se transformou. Surge, assim, um novo modelo: a cidadania digital. Esse novo conceito permite que o cidadão, ao se conectar à internet, exerça sua cidadania em um ambiente virtual, utilizando as redes de sua preferência e se tornando um sujeito político dentro do ciberespaço.[16]

"Um cidadão digital entende como o ambiente digital funciona e os princípios que o orientam. Ele é capaz de analisar o papel das tecnologias na sociedade, avaliar seu impacto no cotidiano e utilizá-las para a construção do conhecimento."[17]

Por não ser um conceito que envolve apenas a acessibilidade, a cidadania digital também esbarra em outras habilidades, como questões educacionais, econômicas e culturais, que influenciam diretamente o pleno exercício da cidadania.

Como era de se esperar, assim como na sociedade digital, a cidadania digital converge em um ponto de partida comum: a inclusão digital e a conectividade significativa. Sem a efetivação desses temas, a prática da cidadania digital torna-se inviável.

---

16 NUNES, Danilo Henrique; LEHFELD, Lucas Souza. Cidadania digital: direitos, deveres, lides cibernéticas e responsabilidade civil no ordenamento jurídico brasileiro. Revista de Estudos Jurídicos UNESP, Franca, ano 22. Disponível em: https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/issue/ archive.

17 NOVAES, Ana Lívia da Silva Souza. Cidadania digital: o acesso democrático à tecnologia no Brasil. Publicado em: 27 fev. 2024. Disponível em: https://www.politize.com.br/cidadania-digital/. Acesso em: 228 set. 2024.

As dificuldades presentes na sociedade criam obstáculos que impedem os cidadãos de participar plenamente dos debates eleitorais. Um estudo recente realizado pelo Reglab, que analisou as propostas de campanha de 13 candidatos a prefeito em São Paulo, Rio de Janeiro, Fortaleza, Salvador e Belo Horizonte em 2024, revelou que "iniciativas que visam reduzir o abismo digital, promovendo o acesso à internet, capacitação em ferramentas digitais e democratização do uso de tecnologias digitais" — ou seja, inclusão digital — estão presentes em 10 propostas.[18]

Com base nas propostas apresentadas, fica evidente a necessidade de maior amadurecimento dos temas inclusão digital e conectividade significativa, com apresentação de proposta mais robustas tanto por parte dos candidatos quanto do poder público em geral.

Diante do contexto apresentado, é evidente que a exclusão digital impacta a vida do cidadão de várias maneiras, dificultando sua participação no processo eleitoral e sua integração em uma sociedade digital. Isso o impede de atuar como um cidadão digital, exercendo plenamente seus direitos em uma sociedade democrática.

7. CONCLUSÃO

A inclusão digital e a conectividade significativa são pilares fundamentais para garantir uma participação cidadã plena no ambiente digital, especialmente no contexto eleitoral. As transformações tecnológicas reconfiguraram não apenas o acesso à informação, mas também as formas de interação e de exercício da cidadania. No entanto, a exclusão digital, seja pela falta de acesso à internet de qualidade ou pela ausência de habilidades digitais, continua sendo um desafio para a democracia, limitando a participação de muitos cidadãos nos processos decisórios.

18 RAMOS, P. H. Cidades do Amanhã: Inovação e Tecnologia nas Eleições Municipais de 2024. Policy Briefs Reglab. n. 1. São Paulo: Reglab, 2024.

Além disso, a informatização da justiça eleitoral, embora essencial para modernizar o sistema e garantir maior eficiência, precisa ser acompanhada por políticas que assegurem a inclusão digital de toda a população. Sem isso, as desigualdades persistirão, deixando muitos eleitores sem acesso à informação ou ao exercício pleno de seus direitos. O debate sobre o uso de tecnologias, como a inteligência artificial, também reforça a necessidade de uma governança responsável, que preze pela ética, transparência e segurança digital.

Portanto, é imperativo que governos, instituições e a sociedade civil atuem em conjunto para promover a inclusão digital e garantir que todos os cidadãos tenham acesso a uma conectividade significativa. Apenas dessa forma será possível fortalecer a democracia digital e assegurar que ela seja verdadeiramente inclusiva, transparente e participativa. A transformação digital pode ser uma ferramenta de empoderamento, reduzindo as desigualdades e promovendo uma participação ativa e consciente nas decisões políticas do país.

REFERÊNCIAS

AMARAL, Vinícius R. A. Os caminhos da cultura digital: a emergência de novas práticas e enunciados políticos. 2012. 108 f. Dissertação (Mestrado) – Mestrado em Ciências Sociais, Pontifícia Universidade Católica de São Paulo, São Paulo.

BRASIL. Tribunal Superior Eleitoral. *Portal da Justiça Eleitoral.* Disponível em: https://www.justicaeleitoral.jus.br/. Acesso em: 25 set. 2024.

BRASIL. Senado Federal. *Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado.* Disponível em: https://www12.senado.leg.br/noticias/materias/2019/12/12/redes-sociais-influenciam-voto-de-45-da-populacao-indica-pesquisa-do-datasenado. Acesso em: 28

set. 2024.

BRASIL. Tribunal Superior Eleitoral. *Seminário debate desafios das eleições no mundo digital.* Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Abril/seminario-debate-desafios-das-eleicoes-no-mundo-digital. Acesso em: 28 set. 2024.

CASTELLS, Manuel. O Poder da Identidade. São Paulo: Paz e Terra, 1999.

Cultura digital. Disponível em: https://pt.wikipedia.org/wiki/Cultura_digital. Acesso em: 24 set. 2024.

ELEUTÉRIO, Kênia I. P. et al. O meme político: Uma análise na perspectiva tecnológica e democrática. Research, Society and Development. Paraná Eleitoral.

Eleições: Especialistas defendem ambiente digital seguro e transparente. TV Senado. Disponível em: https://www.youtube.com/watch?v=ye0UzLO9Kos. Acesso em: 28 set. 2024.

GOMES, Wilson. A democracia no mundo digital: história, problemas e temas. [S.I.]: Edições Sesc, 2018.

NOVAES, Ana Lívia da Silva Souza. Cidadania digital: o acesso democrático à tecnologia no Brasil. Publicado em: 27 fev. 2024. Disponível em: https://www.politize.com.br/cidadania-digital/. Acesso em: 28 set. 2024.

NUNES, Danilo Henrique; LEHFELD, Lucas Souza. Cidadania digital: direitos, deveres, lides cibernéticas e responsabilidade civil no ordenamento jurídico brasileiro. Revista de Estudos Jurídicos UNESP, Franca, ano 22. Disponível em: https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/issue/archive. Acesso em: 28 set. 2024.

Núcleo de Informação e Coordenação do Ponto BR. Co-

nectividade significativa [livro eletrônico]: propostas para medição e o retrato da população no Brasil. Tradução Ana Zuleika Pinheiro Machado. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2024. PDF.

PINHEIRO, Kênia I.; ELEUTÉRIO. Novas tecnologias à disposição do eleitor e a cultura digital nas pequenas jurisdições eleitorais. Paraná Eleitoral.

PINHO, José A. G. et al. Democracia digital na área de administração: um levantamento da construção do campo no Brasil. Cadernos Gestão Pública e Cidadania, 2019.

PINHO, José A. G. et al. Limites e possibilidades da política e da democracia na Internet: um olhar a partir da realidade brasileira. In: PINHO, José A. G. (org.). Estado, sociedade e interações digitais: expectativas democráticas. Salvador: EDUFBA, 2012.

RAMOS, P. H. Cidades do Amanhã: Inovação e Tecnologia nas Eleições Municipais de 2024. Policy Briefs Reglab, n. 1. São Paulo: Reglab, 2024.

Seminário debate desafios das eleições no mundo digital. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Abril/seminario-debate-desafios-das-eleicoes-no-mundo-digital. Acesso em: 28 set. 2024.

FAKE NEWS E IMPACTO NA DEMOCRACIA ELEITORAL: A IMPORTÂNCIA DE POLÍTICAS PÚBLICAS E EDUCAÇÃO DIGITAL

Caroline Vivas Gonçalves[1]
Geysa Camara[2]

1. INTRODUÇÃO

A informação é um dos pilares da sociedade. Ela serve como base para que os cidadãos tomem decisões conscientes sobre questões políticas, sociais e econômicas. Em uma democracia, o acesso a informações corretas e transparentes permite que os eleitores avaliem candidatos e propostas de maneira crítica e racional, promovendo uma participação cidadã efetiva e um controle mais eficaz sobre os governantes. Entretanto, a confiança nas instituições democráticas e nos processos eleitorais está sob ameaça, especialmente devido à proliferação de *fake news*[3]. A desinformação[4], ao distorcer a realidade e minar a credibilidade das fontes de informação,

1 Mestra em Direito pela NOVA School of Law – Lisboa, Portugal. Certificada CIPM e CDPO/BR pela International Association of Privacy Professionals - IAPP. Sócia fundadora da empresa ACG Privacy Solutions. Servidora pública efetiva do Tribunal de Justiça de Sergipe, onde atuou no Comitê Gestor de Segurança da Informação e Comitê Gestor de Proteção de Dados Pessoais. Coautora de obras sobre Direito Digital. Autora de artigos e cursos jurídicos.

2 Advogada desde 2014 Pós-graduada em Direito Digital e Compliance. Mestra em Direito pela Nova School of Law, Lisboa, Portugal. Integra o time de consultores da ACG Privacy Solutions.

3 Apesar de a tradução literal ser "notícia falsa", a expressão mais adequada para a prática seria "desinformação". Fonte: **Não é possível legislar sobre a desinformação, diz diretora do First Draft. Jornal Estado de São Paulo**. Estadão, 28 jun. 2018. Disponível em: https://www.estadao.com.br/estadao-verifica/nao-e-possivel-legislar-sobre-a-desinformacao-diz-claire-wardle-do-first-draft/. Acesso em: 28 set. 2024.

4 Neste artigo, ambas as expressões serão utilizadas de forma intercambiável.

compromete a capacidade dos cidadãos de fazer escolhas conscientes e de participar plenamente do debate público.

A proliferação das *fake news* e a transformação digital configuram desafios significativos para as sociedades em todo o mundo, incluindo o Brasil. Nesse contexto, as políticas públicas emergem como instrumentos para combater as *fake news*, promovendo a educação digital, a inclusão e o acesso à informação de qualidade. A construção de um ambiente digital saudável com base no letramento digital, requer, portanto, a articulação entre Estado e sociedade civil para que juntos possam desenvolver estratégias eficazes para mitigar os riscos da desinformação.

2. O QUE SÃO *FAKE NEWS*

O ditado "a primeira vítima da guerra é a verdade" ilustra bem como a desinformação acompanha a humanidade desde os primórdios da comunicação. No contexto atual, o termo *fake news* refere-se à criação e disseminação intencional de informações falsas ou distorcidas, apresentadas como verídicas.

Fake news possuem um enorme potencial viral, especialmente aquelas que apelam ao emocional[5]. Esse apelo diminui a capacidade crítica de percepção das pessoas, que consomem e compartilham o conteúdo sem verificar sua veracidade. O impacto é amplificado quando a disseminação ocorre através de fontes confiáveis.

Em cenários eleitorais, o objetivo delas é manipular a opinião pública, legitimar pontos de vista ideológicos ou prejudicar adversários políticos. Um exemplo recente ocorreu no Rio de Janeiro, onde a Polícia Federal prendeu quatro pessoas acusadas de divulgar notícias falsas contra candida-

5 Marta Peirano explica que as *fake news* são estrategicamente desenhadas para provocar indignação. PEIRANO, Marta. **O inimigo conhece o sistema**. Santo André - SP: Rua do Sabão, 2022.

tos nas eleições municipais[6].

Um dos casos mais emblemáticos de manipulação de dados e *fake new*s no cenário político foi o escândalo da Cambridge Analytica, que envolveu o uso de dados de 87 milhões de usuários do Facebook[7] para criar campanhas segmentadas. As campanhas pró-Trump nos EUA e a favor do Brexit[8][9] são exemplos claros de como as *fake news* podem influenciar a opinião pública de maneira global. No Brasil, o tema ganhou relevância durante as eleições presidenciais de 2018, tornando-se central no debate político e na polarização crescente no país que se perpetua até os dias atuais.

Em todos esses casos, as redes sociais desempenharam um papel predominante já que seus algoritmos permitem que as *fake news* alcancem milhões de pessoas em poucos minutos, exacerbando a polarização política e corroendo a confiança nas instituições democráticas, criando um desafio cada vez maior para a integridade dos processos eleitorais ao redor do mundo.

Do ponto de vista jurídico, a proliferação de *fake news* traz à tona questões centrais como a liberdade de ex

---

6 **Atores são pagos para sair às ruas e espalhar *fake news* sobre candidatos no Rio de Janeiro**. Fantástico, 15 set. 2024. Disponível em: https://g1.globo.com/google/amp/fantastico/noticia/2024/09/15/atores-sao-pagos-para-sair-as-ruas-e-espalhar-fake-news-sobre-candidatos-no-rio-de-janeiro.ghtml. Acesso: em 20 set. 2024.

7 **Facebook eleva para 87 milhões o nº de usuários que tiveram dados explorados pela Cambridge Analytica.** G1, 04 abr. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/facebook-eleva-para-87-milhoes-o-n-de-usuarios-que-tiveram-dados-explorados-pela-cambridge-analytica.ghtml. Acesso em: 20 set. 2024.

8 DUFFY, B. **The public's Brexit misperceptions**. London: Policy Institute (King's College), 2018. Disponível em: https://www.kcl.ac.uk/sspp/policyinstitute/publications/Brexit-misperceptions.pdf. Acesso em: 20 set. 2024.

9 Referendo que decidiu pela saída do Reino Unido da União Europeia. Durante a campanha de 2016, houve uma proliferação massiva de informações falsas e distorcidas que influenciaram a percepção dos eleitores sobre os benefícios e consequências da permanência ou saída da União Europeia

pressão, o direito à privacidade e a proteção da integridade do processo democrático. A legislação sobre *fake news* ainda está em evolução em muitos países, inclusive no Brasil, e o desafio jurídico reside em equilibrar a proteção da liberdade de expressão com a necessidade de combater a disseminação de informações falsas que podem prejudicar a ordem pública e a democracia.

3. FAKE NEWS E TECNOLOGIAS DIGITAIS

Com a popularização da internet e das redes sociais, a capacidade de difusão de informações falsas aumentou exponencialmente. Hoje, *fake news* circulam em uma escala sem precedentes, impulsionadas por ferramentas automatizadas, como *bots* e algoritmos, que aceleram esse processo.

Plataformas famosas como Instagram, TikTok, Facebook e YouTube utilizam algoritmos que promovem qualquer tipo de engajamento, seja positivo ou negativo, como um indicador de sucesso. O conteúdo emocionalmente carregado tende a gerar mais interação, o que aumenta seu alcance e, em última análise, mantém o modelo de negócios dessas plataformas[10].

Os produtores de *fake news* muitas vezes recorrem a métodos ilegais, como a compra de listas de e-mails e números de telefone, para disparar conteúdos falsos em massa e grupos especializados criam perfis falsos em redes sociais que, aos poucos, se tornam cada vez mais manipuladoras.

A ausência de regulamentação específica torna ainda mais difícil combater a proliferação de *fake news*. Além disso, rastrear a origem dessas informações é um grande desafio, uma vez que os disseminadores frequentemente utilizam perfis falsos para ocultar sua identidade.

10 PEIRANO, Marta – ***op. cit***.

4. INFLUÊNCIA NO COMPORTAMENTO DO ELEITOR

As *fake news* têm o poder de moldar percepções individuais e influenciar diretamente o voto. Muitas vezes, informações falsas sobre candidatos, partidos ou políticas públicas são disseminadas com o objetivo de gerar confusão, manipular o eleitorado e comprometer a integridade da votação. Isso pode levar a uma menor participação eleitoral, enfraquecendo ainda mais a representatividade das decisões políticas.

De acordo com a pesquisa "Panorama Político 2024 - Notícias falsas e Democracia", realizada pelo DataSenado[11], 81% dos brasileiros acreditam que as *fake news* influenciam diretamente os resultados das eleições. Este dado é alarmante, pois revela que a manipulação da informação é amplamente percebida como uma ameaça real à lisura das campanhas eleitorais.

O poder de persuasão das *fake news* é ainda mais acentuado em populações com menor escolaridade[12], que muitas vezes dependem das redes sociais para obter informações. No entanto, independentemente do grau de instrução, quase 90% dos brasileiros admitem já terem acreditado em alguma desinformação[13]. Isso acontece porque as ferramentas

---

11 **Panorama Político 2024 - Notícias falsas e Democracia**. DataSenado, 2024. Disponível em: https://www.senado.leg.br/institucional/datasenado/relatorio_online/fake_news/2024/interativo.html#panorama-pol%C3%ADtico-2024---not%C3%ADcias-falsas-e-democracia. Acesso em: 20 set. 2024.

12 ***Fake news* se combate com educação, dizem especialistas em audiência na CE**. Agência Senado, 27 nov. 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/11/27/fake-news-se-combate-com-educacao-dizem-especialistas-em-audiencia-na-ce. Acesso em: 22 set. 2024.

13 MELO, Daniel**. Quase 90% dos brasileiros admitem ter acreditado em *fake news***. Agência Brasil, 01 abr. 2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-04/quase-90-dos-brasileiros-admitem-ter-acreditado-em-fake-news. Acesso em: 24 set. 2024.

digitais estão cada vez mais sofisticadas, projetando essas notícias para atingir segmentos específicos da população e explorando preconceitos e vulnerabilidades, especialmente em momentos críticos, como debates ou as vésperas de uma eleição.

O apelo emocional é uma das estratégias mais eficazes de desinformação. Notícias que exploram medos, indignação ou esperanças tendem a mobilizar eleitores em torno de causas fictícias ou desmobilizá-los ao semear dúvidas e confusão. Esse processo resulta na polarização do eleitorado, que se fragmenta em bolhas informacionais, tornando-se incapaz de dialogar ou alcançar um consenso sobre a realidade política.

Assim, a desinformação não ameaça apenas o processo eleitoral, mas a coesão social e a capacidade dos cidadãos de tomar decisões informadas e racionais.

O combate às *fake news* requer uma abordagem coordenada que envolva múltiplos setores da sociedade. As plataformas digitais devem ser responsabilizadas por sua participação na propagação de desinformação, e é fundamental a criação de políticas públicas eficazes para monitorar e regular essas práticas. Além disso, é necessário educar a população, capacitando-a a identificar e questionar informações falsas, assegurando que as eleições sejam justas e reflitam a verdadeira vontade popular.

5. POLÍTICAS PÚBLICAS E COMBATE A *FAKE NEWS*

Políticas públicas são amplamente conhecidas como o conjunto de ações e diretrizes estabelecidas pelo Estado para atender às necessidades da sociedade em diversos campos, como saúde, educação, segurança, meio ambiente, economia, dentre outros. No cenário atual de transformação digital, onde o uso de tecnologia é integrado ao cotidiano da administração pública e da população, é impossível deixar

de fora novas necessidades sociais que englobam o mundo digital, como por exemplo: a inclusão e acesso da população à internet; capacitação e combate à desinformação; tecnologia da informação; proteção de dados; e inteligência artificial.

Muito embora seja competência do Estado, a formulação e execução dessas políticas envolve não apenas o Governo, mas também pesquisadores e organizações não governamentais, entidades privadas e a sociedade civil em geral.

O processo de elaboração de políticas públicas é, portanto, multidisciplinar. No Brasil, a participação popular, por meio de conselhos, audiências e consultas públicas, e o destaque e repercussão midiática de temas de extrema importância social tem se tornado um elemento-chave nesse processo. Assim, a reunião de diversos atores sociais na discussão das políticas públicas se torna cada vez mais acessível, especialmente no que tange a tentativa de acompanhar a transformação digital.

Nesse ponto, as *fake news* acabam por ser um desafio significativo para o Estado, enquanto principal ator e provedor de políticas públicas. A proliferação e velocidade de notícias falsas, amplamente disseminadas por meio das redes sociais e aplicativos de mensagens exige cada vez mais uma resposta coordenada do Estado e da sociedade, seja no sentido de possibilitar a educação digital como também a criação de instrumentos legais que responsabilizem os agentes envolvidos na criação e disseminação dessas práticas.

Diante deste cenário existe um panorama regulatório em constante mutação, cujo anseio é tentar acompanhar as transformações digitais e mitigar os riscos da disseminação das *fake news* e seus impactos na sociedade e na própria estruturação do Estado e do regime democrático.

6. PANORAMA REGULATÓRIO E MEDIDAS ADOTADAS

A velocidade de propagação das informações no mundo hiperconectado já é uma realidade que, quando bem empregada, contribui para o desenvolvimento social, mas também tem impactos negativos quando utilizada de forma a causar dano, confusão e desinformação em massa.

Na tentativa de equilibrar este cenário e mitigar os impactos negativos, os esforços do Estado brasileiro e da sociedade começam a ser perceptíveis através das várias iniciativas e medidas adotadas, que evidenciam um panorama regulatório ainda em desenvolvimento.

Uma das principais iniciativas nesse sentido foi o *Projeto de Lei das Fake News* (PL 2630/2020)[14], conhecido formalmente como *Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet* que tem como objetivo regulamentar as plataformas digitais, obrigando-as a adotar medidas mais rígidas contra a disseminação de conteúdos falsos. O PL também visa aumentar a transparência nas operações das redes sociais e mensageiros instantâneos, como o WhatsApp e o Telegram por exemplo, exigindo a rastreabilidade de mensagens reencaminhadas em massa e a identificação de contas automatizadas (*bots*).

Além disso, o PL propôs a remuneração de conteúdos jornalísticos utilizados por essas plataformas, o que gerou ainda mais controvérsias, especialmente entre entidades de imprensa e as próprias plataformas digitais. Entre as críticas estavam preocupações com a liberdade de expressão e a criação de uma agência reguladora específica, que foi vista como uma possível forma de censura por seus críticos.

---

14 BRASIL. Câmara dos Deputados**. Ficha de Tramitação da Proposição nº 2256735**. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735&fichaAmigavel=nao. Acesso em: 29 set. 2024.

Além deste PL, cuja discussão permanece em andamento, o Tribunal Superior Eleitoral (TSE) tem desempenhado um importante papel no combate às *fake news*. A partir de 2020, o TSE intensificou campanhas de conscientização e parcerias com plataformas digitais para combater a disseminação de notícias falsas durante as eleições. A *Coalizão para Checagem de Fatos*[15] foi uma dessas iniciativas. O TSE também criou um canal direto para denúncias de desinformação, possibilitando uma resposta mais rápida e eficaz a tentativas de manipulação do eleitorado por meio de informações falsas.

Assim, o TSE vem adotando várias medidas para combater desinformações nas Eleições de 2024. Dentre as principais temos a atualização da Resolução n.º 23.610/2019[16] que trata de propaganda eleitoral. A atualização da norma vai ao encontro da transformação e avanço dos meios digitais, abarcando com isso a proibição de *deepfakes*[17]*;* a obrigação de aviso sobre o uso de IA na propaganda eleitoral; restrição do emprego de robôs para intermediar contato com o eleitor (a campanha não pode simular diálogo com candidato ou qualquer outra pessoa); e responsabilização das empresas de

15 **TSE lança coalizão de checagem de informações para as eleições 2020**. TSE, 01 out. 2020. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2020/Outubro/tse-lanca-coalizao-de-checagem-de-informacoes-para-as-eleicoes-2020. Acesso em: 25 set. 2024.

16 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024.** Brasília, DF: TSE, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 25 set. 2024.

17 Um exemplo recente ocorreu quando uma vereadora foi vítima de um *deepfake* e teve sua voz digitalmente manipulada em vídeos para parecer que proferia ofensas contra moradores locais . Esse caso ilustra o perigo dessas tecnologias para a integridade do processo eleitoral. Fonte: CARONE, Carlos; PINHEIRO, Mirelle. **Robô simula voz de candidata a prefeita e esculacha eleitores: "Fedem"**. Metrópoles, 16 set. 2024. Disponível em: https://www.metropoles.com/distrito-federal/na-mira/robo-simula-voz-de-candidata-a-prefeita-e-esculacha-eleitores-fedem. Acesso em 28 set. 2024.

tecnologia (*big techs)* que não retirarem do ar, imediatamente, conteúdos com desinformação, discurso de ódio, ideologia nazista e fascista, além dos antidemocráticos, racistas e homofóbicos. As consequências para descumprimento são severas e poderão levar o candidato/partido a ter seu registro ou o mandato cassado, com apuração das responsabilidades conforme disposto no Código Eleitoral.

Outro ponto de destaque da resolução é que provedores e plataformas passam a ser considerados "solidariamente responsáveis, civil e administrativamente, quando não promoverem a indisponibilização imediata de conteúdos e contas durante o período eleitoral". Com isto as *big techs* deverão ainda adotar e divulgar medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral.

Ainda nesse contexto, importa mencionar que o TSE, desde março de 2024, conta com o Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE)[18] que visa conjugar os esforços de diferentes instituições no combate à desinformação e às *deepfakes,* além de atuar no enfrentamento dos discursos de ódio, discriminatórios e antidemocráticos no âmbito eleitoral.

O objetivo do CIEDDE é a promoção, durante o período eleitoral, da cooperação entre Justiça Eleitoral, órgãos públicos, entidades privadas e, em especial, as plataformas de redes sociais e serviços de mensagens instantâneas privadas, para garantir o cumprimento da Resolução n.º 23.610/2019.

Igualmente, temos o SIADE - Sistema de Alerta de

18 **Entenda como funciona o CIEDDE e como denunciar via sistema**. TSE, 21 mai. 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Maio/entenda-como-funciona-o-ciedde-e-como-denunciar-via-sistema. Acesso em: 25 set. 2024.

Desinformação Eleitoral,[19] criado em 2022 como uma ferramenta que dá protagonismo a quem quer ajudar no combate à desinformação durante o período eleitoral. Nela, as denúncias são realizadas por meio do portal do TSE, que coleta as denúncias e repassa para as plataformas digitais, que, por sua vez, avaliam se houve violação à legislação ou aos respectivos termos de uso. Os alertas podem também ser encaminhados ao Ministério Público Eleitoral e demais autoridades para adoção das medidas legais cabíveis. Atualmente, a iniciativa conta com mais de 150 parceiros, como redes sociais e plataformas digitais, instituições públicas e privadas, entidades profissionais, entre outros integrantes, o que por óbvio evidencia o esforço social em prol do combate as *fake news.*

Outra iniciativa relevante é o Programa de Enfrentamento à Desinformação[20], criado em 2019, e que se tornou uma ação permanente do TSE em 2021. Nesta iniciativa os parceiros dividem com a Justiça Eleitoral atribuições que incluem desde o monitoramento e a apuração de notícias falsas até o combate à desinformação, que acompanha esclarecimentos e a informação correta sobre a temática, por meio de notícias publicadas na página Fato ou Boato[21].

Há também a já conhecida página Fato ou Boato, que integra o Programa Permanente de Enfrentamento à Desinformação, que estabelece uma rede nacional de verificação de informações relativas ao processo eleitoral. Com o objeti-

19 **Sistema de Alertas de Desinformação Eleitoral – SIADE**. Tribunal Superior Eleitoral. Disponível em: https://www.tse.jus.br/eleicoes/sistema-de-alertas. Acesso em: 25 set. 2024.

20 **Programa de Enfrentamento à Desinformação com foco nas eleições 2020 mobiliza instituições.** TSE, 22 mai. 2020. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2020/Maio/programa-de-enfrentamento-a-desinformacao-com-foco-nas-eleicoes-2020-mobiliza-instituicoes. Acesso em: 28 set. 2024.

21 **Fato ou Boato. Esclarecimentos sobre informações falsas**. Justiça Eleitoral. Disponível em: https://www.justicaeleitoral.jus.br/fato-ou-boato/#. Acesso em: 28 set. 2024.

vo maior de enfrentamento às *fake news*, nove das principais agências de checagem do Brasil compõem essa força-tarefa em favor da circulação de conteúdos verificados, que efetivamente promovam debates e esclarecimentos fundamentais à tomada de decisão dos eleitores.

Outro ponto relevante é a criação de campanhas educativas e de conscientização sobre o uso responsável das redes sociais e o impacto das *fake news*, conduzidas por órgãos governamentais e também por diversas agências, mídias e canais parceiros da democracia, que tem contribuído para a checagem de fatos e para o combate à desinformação, o que evidencia a importância dos esforços conjuntos e o início de uma maior consolidação social pela disseminação da verdade e combate às *fake news*, cujo intuito supremo é consolidar a conscientização e educação da população sobre o tema e com isso mitigar seus riscos e impactos.

7. EDUCACÃO DIGITAL COMO FERRAMENTA DE PREVENÇÃO E MITIGAÇÃO DE RISCOS

A transformação digital é imparável, sua velocidade e força motriz são desafiantes. Nesta perspectiva, a educação digital se coloca como ferramenta de prevenção e como ferramenta de desenvolvimento necessária às gerações futuras. O sucesso de um novo modelo de sociedade digital se verificará não só através de suas habilidades técnicas de conexão e acesso à internet, mas também com o exercício e desenvolvimento de pensamento crítico e responsabilidade social, estes possibilitados por uma linha do tempo assente na educação digital e bem comum.

É justamente por isso que o uso das tecnologias digitais aliadas ao pensamento crítico para promover o ensino, a aprendizagem e a educação digital devem ser incentivadas. O letramento digital[22] já é uma necessidade.

22 MACARAJÁ, Alek. **Letramento digital: a educação como estratégia de combate à desinformação**. Terra, 14 mar. 2024. Disponível em: https://www.terra.

Não se trata somente de possibilitar o acesso a ferramentas digitais e dispositivos como computadores, *tablets, smartphones* ou plataformas de aprendizado *online* e IA, mas também de disseminar conhecimento e habilidades que possibilitem formar e consolidar competências que serão essenciais num mundo cada vez mais digital, integrado e permeado de notícias falsas.

Num país com dimensões geográficas e diferenças sociais como o Brasil, por óbvio a educação digital enfrenta desafios significativos como desigualdade no acesso à tecnologia e dispositivos e falta de capacitação adequada para professores. Mesmo assim, uma estratégia de educação e letramento digital parece promissora.

Em linhas gerais estratégias de inclusão de conteúdos de alfabetização digital vem cada vez mais sendo incorporados nos currículos para ensinar os estudantes a analisarem e interpretarem informações de diversas fontes. Esse tipo de educação ajuda os alunos a entenderem o funcionamento das mídias sociais e a discernirem entre informações confiáveis e não confiáveis.

Segundo a Unicef[23], as instituições educacionais são fundamentais para construção social de um pensamento crítico que vá além do senso comum, pois nelas é fornecido o ensino capaz de catalisar a alfabetização digital aos jovens. Tal fato se torna ainda mais relevante quando dados são postos em evidência. A exemplo disso, uma pesquisa da TIC Kids Online Brasil, do Comitê Gestor da Internet no Brasil (CGI.br) em 2023, citada pela Unicef, apontou que 95% das crianças e adolescentes entre 9 e 17 anos de todo o país aces-

---

com.br/noticias/brasil/politica/letramento-digital-a-educacao-como-estrategia-de-combate-a-desinformacao,66280cbdb3170bc9d5a2f3452d460001n1csnfqn.html. Acesso em: 29 set. 2024.

23 BRASIL. UNICEF. **Uma jornada educativa**. **O núcleo escolar e o combate à desinformação**. UNICEF, 10 set. 2024. Disponível em: https://www.unicef.org/brazil/blog/uma-jornada-educativa. Acesso em: 29 set. 2024.

sam a Internet, o que corresponde a mais de 25,1 milhões de pessoas nessa faixa etária. Contextualizando, isso pode significar que, se o pensamento crítico da nova geração não for estimulado, a sociedade estará destinada a conviver com uma crise de desinformação devastadora.

Neste panorama, capacitar as pessoas a compreenderem e utilizarem as tecnologias de forma crítica e reflexiva se torna foco central de uma educação digital, de forma que o letramento digital cada vez mais se consolida como ferramenta propulsora.

Tanto é assim que Lei n.º 14.533 de 2023[24] instituiu no Brasil a Política Nacional de Educação Digital (PNED), com foco na educação digital escolar e letramento digital. O inciso III do art. 3º, em particular, relaciona-se diretamente com a desinformação, afirmando que a educação digital inclui a promoção de uma cultura digital e a participação consciente e democrática nas tecnologias digitais, promovendo uma atitude crítica, ética e responsável em relação à diversidade de mídias e conteúdos digitais. O PNED incluiu o letramento digital no currículo das escolas de ensino fundamental e médio, confirmando a importância e atenção ao tema, sendo agora um dever do Estado viabilizar as políticas públicas necessárias à execução do letramento digital.

Embora o problema seja complexo, acredita-se que a Política Nacional de Educação Digital (PNED) pode ajudar a combater a desinformação no Brasil[25] sendo uma das principais ferramentas de políticas públicas para o futuro,

24 BRASIL. **Lei n. 14.533, de 11 de janeiro de 2023. Institui a Política Nacional de Educação Digital.** Diário Oficial da União: Brasília, DF, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14533.htm#promulgacao. Acesso em: 29 set. 2024.

25 CAVALCANTE, Francisco [*et al*]. **A Política Nacional de Educação Digital e o combate à desinformação**. Migalhas, 22 ago. 2023. Disponível em: https://www.migalhas.com.br/depeso/392190/a-politica-nacional-de-educacao-digital-e-o-combate-a-desinformacao. Acesso em: 29 set. 2024.

devendo obviamente ser conjugada com outras iniciativas num esforço conjunto de aprendizagem, prevenção e combate às *fake news*.

8. CONCLUSÃO

A informação é fundamental para a saúde das democracias e a desinformação compromete a capacidade dos indivíduos de tomar decisões conscientes e ameaça a própria integridade do sistema democrático.

O cenário de transformação digital em que vivemos é desafiador e, infelizmente, a velocidade com que novas formas de disseminação de conteúdos falsos se inserem na realidade social todos os dias é alarmante. A educação digital e as políticas públicas emergem nesse cenário como ferramentas cruciais no combate às *fake news* e na promoção do letramento digital.

Para construir um ambiente digital saudável é necessária a colaboração entre Estado, sociedade civil, pesquisadores, organizações não governamentais, plataformas digitais e imprensa, todos num esforço conjunto, visando a educação digital e o acesso à informação de qualidade.

Por fim, a implementação de regulamentações eficazes que responsabilizem plataformas digitais e promovam a transparência é essencial para mitigar os riscos da desinformação; assim como, o fomento de iniciativas educacionais transversais que possibilitem a aprendizagem e amadurecimento do pensamento crítico do cidadão no mundo digital.

CRIMES ELEITORAIS DIGITAIS: CLASSIFICAÇÃO E PENALIDADES NO AMBIENTE *ONLINE*

Eloá de Azevedo Caixeta[1]
Mariana Gomes Lopes[2]

1. INTRODUÇÃO

A crença popular de que a internet é "terra sem lei" infelizmente ainda é difundida, sendo que tal pensamento vem da percepção de que, por muito tempo, o ambiente digital parecia estar fora do alcance das leis tradicionais.

Apesar de existirem certas limitações com relação ao procedimento de investigação de pessoas que praticam crimes *online*, é importante frisar que recai sobre a prática ilícita em ambiente *online* a mesma penalização do crime praticado fora da internet. O crime não deixa de ser crime pelo simples fato de ter sido cometido em ambiente digital.

No Brasil, o ambiente digital é utilizado para as mais diversas finalidades. De acordo com o "Relatório Digital 2024: *5 billion social media users"*, o Brasil ocupa o 2º lugar como o país em que usuários passam mais tempo *online* e,

1 Advogada e consultora em privacidade e proteção de dados pessoais com especialização em Direito Digital e *Compliance*. Atuante em projetos de adequação à LGPD desde 2019, é também coautora em diversos livros cuja temática é proteção de dados pessoais, sendo o mais recente *"LGPD para pequenas empresas: teoria e prática"*, lançado pela Revista dos Tribunais, publicado em setembro de 2024. Colunista do *Jornal de Uberaba* com a coluna Direito Delas.

2 Advogada e servidora pública federal. Mestre em Administração Pública (2019) pelo Programa de Mestrado Profissional em Administração Pública (PROFIAP) da Universidade Federal do Triângulo Mineiro (UFTM). Graduada em Direito (2012) e em Comunicação Social - Habilitação em Jornalismo (2019), ambas pela Universidade de Uberaba (Uniube). Especialista em Direito Constitucional Aplicado (2015) e em Direito e Processo Tributário (2021). Atua há 10 anos na área de assessoria e consultoria jurídica da UFTM.

somado a isso, de acordo com dados fornecidos por pesquisa do IBGE, 87,2% da população brasileira faz uso da internet.

Sendo assim, a internet é muito presente entre os brasileiros e não poderia ser diferente o uso do ambiente digital também em época de eleição para a realização de campanhas eleitorais. Juntamente à campanha eleitoral digital, em que o candidato se utiliza de redes sociais e aplicativos de mensagem para difundir suas propostas e angariar votos, a prática de crimes eleitorais digitais estão muito presentes dentro deste contexto.

Desta forma, o presente artigo tem como finalidade demonstrar que o ambiente *online* faz parte do "mundo real", não sendo mais considerado um mundo à parte, livre de sanções em caso de condutas ilícitas, inclusive dentro do contexto de campanhas eleitorais digitais em que é possível a prática de crimes digitais.

2. CRIMES ELEITORAIS NO AMBIENTE DIGITAL

Considerando que no ano de 2022, de acordo com dados do Tribunal de Superior Eleitoral (TSE), legendas, candidatos e candidatas gastaram R$ 376 milhões com impulsionamento de conteúdos digitais de campanha, surgiu a necessidade de fiscalizar de perto o ambiente digital utilizado para campanhas eleitorais.

Consequentemente, com o objetivo de regular os avanços tecnológicos e a sua utilização no contexto das campanhas eleitorais realizadas em meio digital, o TSE atualizou a Resolução nº 23.610/2019 pela Resolução nº 23.732/2024, para incluir práticas eleitorais permitidas e proibidas no ambiente digital.

No tocante à utilização de dados pessoais, a resolução inclui diversos dispositivos voltados para a proteção dos dados pessoais de eleitores, assegurando o cumprimento da LGPD durante as eleições. Provedores, partidos, candidatos

e candidatas são obrigados a adotar medidas de segurança técnica para prevenir acessos não autorizados a esses dados e utilizá-los exclusivamente para os fins previamente informados e autorizados pelos titulares. Também devem manter registros das operações de tratamento dos dados pessoais.

Além disso, é proibida a cessão, venda ou compartilhamento de dados pessoais de clientes ou usuários para candidatas, candidatos, partidos, federações ou coligações.

Caso haja a venda de cadastros, tanto o responsável pela disponibilização das informações quanto o candidato que se beneficiou – quando comprovado de que já possuía conhecimento sobre o fato – podem ser penalizados com multas que variam de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais).

Com relação à campanha eleitoral paga na internet, é permitida para o impulsionamento de conteúdos nas redes se a contratação se der e for paga por partidos, federações, coligações, candidatos, candidatas e seus representantes.

Todo conteúdo impulsionado deverá conter o número de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) ou no Cadastro de Pessoas Físicas (CPF) do responsável pelo impulsionamento, além da expressão "propaganda eleitoral", sempre de forma transparente para o público. Além disso, o impulsionamento não poderá ser utilizado para propagar dados falsos, notícias fraudulentas ou informações descontextualizadas.

A Resolução do TSE proíbe a contratação de influenciadores com o objetivo de postarem propaganda político-eleitoral de candidatos. No entanto, caso não haja o pagamento, é lícita a veiculação de propaganda político-eleitoral em canais e perfis de influenciadores e de pessoas com grande audiência na internet.

Caso o conteúdo esteja em perfis de pessoas físicas e jurídicas não candidatas, o compartilhamento do conteúdo pode acontecer, desde que não haja remuneração, pagamento

ou monetização pelos materiais divulgados por essas contas.

O anonimato é proibido pela Resolução em questão, sendo que a livre manifestação do pensamento na internet é assegurada durante a campanha eleitoral desde que a pessoa possa seja identificada. Aqueles eleitores e eleitoras que praticarem crimes contra a honra da candidata ou do candidato (difamação, calúnia, injúria), ou divulgarem fatos sabidamente inverídicos, poderão ter a sua liberdade de expressão limitada.

Com relação a propaganda eleitoral realizada por envio de mensagens em massa, há proibição pela Resolução, exceto quando houver a coleta de consentimento das pessoas destinatárias da mensagem. Esta previsão dialoga com o direito do titular dos dados pessoais de revogar o seu consentimento previsto da LGPD quando informa que, mesmo havendo o consentimento, as mensagens precisam conter algum tipo de mecanismo que permita ao destinatário solicitar o descadastramento da lista de envio ou de dados pessoais. Caso o pedido de saída da lista não seja atendido no prazo de 48 (quarenta e oito) horas, o responsável poderá ser condenado a pagar multa no valor R$ 100,00 (cem reais) por mensagem enviada indevidamente.

Com relação às transmissões ao vivo que devem ocorrer apenas por meio de páginas ou canais vinculados aos candidatos e candidatas ou aos seus partidos, elas podem ser realizadas para divulgar candidaturas e tentar angariar votos. Caso o evento ao vivo seja conduzido por um candidato à reeleição, como prefeito, o ambiente da "live" precisa ser neutro, sem símbolos ou objetos associados ao poder público. Além disso, apenas o detentor do cargo pode estar na transmissão, vedada a participação de outros candidatos, sendo que o conteúdo deve tratar apenas da candidatura.

Sobre a utilização de inteligência artificial em campanha eleitoral no meio digital, a Resolução aduz que candidaturas e partidos que fizerem uso da IA durante o período de

campanha precisam garantir total transparência, sendo necessário indicar, explicitamente, que o conteúdo foi fabricado ou manipulado e qual tecnologia foi utilizada (funcionalidade já ofertada pela rede social Instagram). No entanto, o uso de "deep fake" e de inteligência artificial para propagar desinformação é totalmente proibido.

Por fim, no dia da eleição, tanto no primeiro quanto no segundo turno, não poderá haver a publicação de novos materiais ou o impulsionamento de conteúdo. Os materiais publicados e divulgados antes do dia das eleições podem ser mantidos, desde que não sejam submetidos a novo impulsionamento. A pena para quem infringir a regra é de detenção, de 06 (seis) meses a 01 (um) ano, e multa, que pode chegar a até R$ 15.000,00 (quinze mil reais).

Em caso de descumprimento das regras impostas pela Resolução do TSE, o Ministério Público poderá ajuizar ação por propaganda irregular, solicitando que o conteúdo seja retirado do ar, bem como aplicação de multa. Caso seja comprovado que a conduta irregular do candidato ou partido caracterizou abuso de poder econômico, interferindo no resultado da eleição, o Ministério Público Eleitoral poderá solicitar a cassação do candidato ou a declaração de inelegibilidade.

Percebe-se, mediante leitura e análise da Resolução nº 23.732/2024 do TSE, a existência de referência à crimes já tipificados no Código Penal, Código Eleitoral e demais legislações pertinentes que não deixam de existir só porque praticados no ambiente digital.

3. CLASSIFICAÇÃO DOS CRIMES ELEITORAIS DIGITAIS

Antes de adentrarmos ao tema, é importante destacar que quando um crime acontece no âmbito eleitoral, a legislação aplicável depende da natureza do delito. Em geral, crimes eleitorais são regidos pelo Código Eleitoral (Lei nº

4.737/1965), que prevê normas específicas para condutas ilícitas relacionadas às eleições. No entanto, em alguns casos, o Código Penal também pode ser aplicado, especialmente se o crime for de natureza comum, mas relacionado ao processo eleitoral.

São exemplos de crimes eleitorais contidos no Código Eleitoral, estando diretamente relacionados ao processo eleitoral:

- Compra de votos;
- Propaganda eleitoral irregular;
- Abuso de poder político ou econômico;
- Desinformação (*fake news*) durante as eleições;
- Crimes contra a honra (injúria, difamação e calúnia) quando praticados na propaganda eleitoral;
- Inscrição fraudulenta de eleitores.

Se a conduta criminosa for de natureza comum, mas ocorrida no contexto eleitoral, o Código Penal pode ser aplicado. Alguns exemplos incluem:

- Crimes contra a honra (difamação, injúria e calúnia) cometidos em contexto que não envolve propaganda eleitoral;
- Agressões físicas ou ameaças;
- Fraude, falsificação de documentos, ou outros crimes comuns.

No entanto, em certos casos, ambos os códigos podem ser aplicados simultaneamente. Por exemplo, a prática de desinformação (que é crime eleitoral) pode também configurar crime previsto no Código Penal, enquanto a calúnia ou difamação (que são crimes tipificados no CP) podem também configurar crimes previstos na legislação eleitoral.

Feita essa análise inicial, seguem abaixo os crimes digitais mais praticados no âmbito eleitoral:

3.1. Crimes contra a honra (difamação, injúria e calúnia)

No contexto digital, crimes contra a honra, como difamação, injúria e calúnia, são amplamente utilizados como ferramenta para atacar adversários políticos. Nas campanhas eleitorais digitais, essas práticas se intensificam por meio de redes sociais, com a disseminação rápida e massiva de conteúdos ofensivos que buscam manchar a reputação de candidatos. Esse tipo de crime pode resultar em processos tanto no âmbito cível, quanto criminal, além de penalidades eleitorais.

3.2. Desinformação (*"Fake news"* / *"Deepfake"*)

A desinformação é uma das formas mais graves de crime eleitoral digital, sendo usada para manipular eleitores por meio de informações falsas ou distorcidas que podem, inclusive, influenciar o resultado nas urnas. *"Deepfake"*, uma forma mais sofisticada de desinformação, consiste na manipulação de vídeos ou áudios, criando conteúdos falsos que parecem extremamente reais, pois acabam contendo o rosto ou a voz do candidato alvo, aumentando o potencial de engano.

3.3. Fraude de identidade

A fraude de identidade é outra prática comum nas eleições digitais. Candidatos ou grupos de apoio podem utilizar *"bots"* (robôs programados para disseminar mensagens automaticamente) ou perfis falsos para atacar adversários de forma anônima. Esses perfis falsos servem para disseminar desinformação, promover ataques coordenados ou manipular discussões públicas. Além disso, a criação de múltiplos perfis ou contas fictícias pode ser usada para influenciar o engajamento nas redes sociais.

3.4. Uso indevido de dados pessoais

O uso indevido de dados pessoais de eleitores tem sido uma prática cada vez mais comum, infelizmente. Campanhas podem coletar dados pessoais sem que haja o respeito à LGPD, principalmente aos seus princípios, bases legais e direitos dos titulares dos dados. A utilização de dados pessoais sem autorização pode resultar na aplicação de multas de valor elevado e de penalidades severas para os envolvidos, tanto do ponto de vista eleitoral quanto no âmbito da proteção de dados pessoais.

3.5. Disparo em massa de mensagens

O disparo em massa de mensagens, especialmente em aplicativos de comunicação como o *WhatsApp*, é uma prática também comum nas campanhas eleitorais. O TSE, na Resolução já citada anteriormente, prevê medidas cujo objetivo é proibir os envios, tendo em vista que, muitas vezes, é utilizada para disseminar desinformação.

3.6. Caixa dois digital

O caixa dois digital refere-se à prática de arrecadação e utilização de recursos financeiros para campanhas fora das prestações de contas oficiais exigidas pela Justiça Eleitoral. Com a digitalização dos meios de pagamento e a facilidade de transações *online*, essa prática já se tornou frequente.

Utilizar plataformas digitais para angariar recursos sem a devida declaração, ou com o objetivo de ocultar a origem do dinheiro, configura crime.

A prática de crimes eleitorais digitais reflete a necessidade crescente de adaptação da legislação e fiscalização eleitoral ao ambiente digital. A Justiça Eleitoral brasileira tem se empenhado em combater essas práticas, mas os desafios trazidos pela rápida evolução da tecnologia exigem me-

didas cada vez mais sofisticadas para garantir eleições justas e transparentes.

4. LEGISLAÇÃO BRASILEIRA: EVOLUÇÃO HISTÓRICA

A legislação brasileira sobre crimes digitais se encontra em constante e necessária atualização e aprimoramento. Esse movimento contínuo reflete a crescente digitalização da sociedade e a consequente necessidade de garantir segurança jurídica aos usuários do ambiente virtual.

Em 2000, foi promulgada a Lei nº 9.983/2000 que – apesar de não tratar diretamente sobre crimes digitais – foi uma das primeiras a normatizar a questão de crimes em ambiente tecnológico. A normativa alterou o Código Penal e incluiu crimes, tais como a inserção de dados falsos em sistemas informatizados da Administração Pública (artigo 313-A do CP).

A Lei nº 12.737/2012 – conhecida como Lei Carolina Dieckmann – é tida como marco inicial na legislação específica para crimes digitais. Essa Lei surgiu após a divulgação – sem autorização – de fotos pessoais da atriz Carolina Dieckmann. Tipificou crimes como a invasão de dispositivos eletrônicos com o objetivo de obter, adulterar ou destruir dados. A lei trouxe, também, punições para a invasão de privacidade digital.

Em 2014, foi publicada a Lei nº 12.965/2014, referenciada como Marco Civil da Internet ou "Constituição da Internet", por estabelecer princípios, garantias, direitos e deveres no uso da internet no Brasil, sendo considerado a "Constituição da Internet". O foco desse diploma normativo não está diretamente nos crimes digitais. Contudo, a lei trouxe diretrizes relevantes para o tratamento de dados pessoais, responsabilização de provedores e garantia de direitos fundamentais no ambiente virtual.

A Lei Geral de Proteção de Dados (LGPD - Lei nº

13.709/2018) foi um avanço significativo no que diz respeito à proteção de dados pessoais. A Lei, tal qual a "Constituição da Internet", não versa diretamente sobre crimes digitais. Porém, estabelece penalidades àqueles que tratarem inadequadamente os dados pessoais (pilar central na era digital). A LGPD é, hoje, a base jurídica da segurança digital no cenário jurídico brasileiro, vez que regulamenta como as empresas e organizações devem coletar, armazenar e tratar os dados dos usuários.

Em 2021, a Lei nº 14.155/2021 enrijeceu as penas para crimes cometidos nos meios digitais, como a fraude eletrônica. A legislação foi uma resposta ao aumento das fraudes e crimes cibernéticos ocorridos durante a pandemia de COVID-19, que acelerou a digitalização das relações como um todo, mormente as econômicas e sociais. Prevê penas maiores para crimes como o estelionato *online*, com agravantes em casos de prejuízo financeiro significativo.

A LGPD, em especial, tem sido um ponto de destaque no debate sobre segurança digital e crimes envolvendo privacidade de dados. As primeiras sanções de advertência e multa aplicadas pela Agência Nacional de Proteção de Dados (ANPD) por descumprimento à LGPD ocorreram em julho de 2023. Após a conclusão do processo administrativo sancionador, restou evidenciado que a empresa Telekall Infoservice infringiu os arts. 7º e o 41 da LGPD, além do art. 5º do Regulamento de Fiscalização da ANPD. Senão vejamos:

> A fiscalização foi iniciada a partir de denúncia de que a empresa Telekall Infoservice estaria ofertando uma listagem de contatos de WhatsApp de eleitores para fins de disseminação de material de campanha eleitoral. Os fatos denunciados foram relativos à eleição municipal de 2020, em Ubatuba/SP.
>
> A ANPD verificou que o tratamento de dados pessoais denunciado estava ocorrendo sem respaldo legal. Foi apurada ainda a falta de comprovação da indicação de encarregado pelo tratamento de dados pessoais pela empresa. (ANPD, 2023)

Atualmente, as eleições são profunda e diretamente influenciadas pelas redes sociais e outras ferramentas *online*, que se tornaram instrumentos fundamentais (e muito potentes) para campanhas e debates políticos. Neste contexto, a discussão sobre a regulamentação dessas plataformas ganha ainda mais relevância, sendo primordial buscar sempre o equilíbrio entre os direitos fundamentais com o interesse público e, ainda, a necessidade de proteger a integridade do processo eleitoral.

O aumento considerável da criminalidade cibernética que se deu com o avanço das tecnologias e da inteligência artificial demanda a atualização constante da legislação sobre crimes digitais no Brasil. Acompanhar os avanços e regulamentá-los é essencial para enfrentar novas ameaças de modo eficaz e democrático.

5. DESAFIOS PARA A FISCALIZAÇÃO E COMBATE AOS CRIMES ELEITORAIS DIGITAIS

Os desafios para a fiscalização e combate aos crimes eleitorais digitais são imensuráveis, considerando a própria natureza do ambiente no qual ocorrem as atividades ilícitas a serem combatidas. De acordo com Crespo (2011, p. 20), são características do ciberespaço:

> a) Capacidade de processar, guardar e circular, de forma automatizada e em tempo real, grandes quantidades de informações em formato digital dos mais variados (fotos, filmes, sons). Isso é facilitado pela própria estrutura descentralizada e não hierarquizada da internet que inviabiliza a existência de órgãos de controle da informação circulante e, como consectário lógico, torna praticamente impossível supervisionar a qualidade e o volume de informações;
> b) O número enorme de usuários, a frequência com que acessam, a liberdade que têm para enviar, transferir, difundir e acessar informações, de modo que os internautas passam a ser potenciais vítimas, mas também potenciais

sujeitos ativos de delitos;

c) As próprias características físicas, técnicas e lógicas das TIC, que podem ser acessadas de forma ilegítima, tendo seu conteúdo alterado. Consegue-se acesso a arquivos das mais distintas naturezas e aos mais variados programas de computador;

d) A enorme potencialidade de multiplicação das ações ilícitas. Isso decorre da própria estrutura das TIC, como mencionado acima. A criação de fóruns de debates, páginas na internet, comunidades de relacionamento etc., podem facilitar a prática de delitos, podendo, ainda, dar maior repercussão a eles, como nas ofensas contra a honra, por exemplo.

A ciência jurídica tem enfrentado novas realidades quanto às práticas delitivas. Compreender essa recém chegada realidade e, ainda, o *modus operandi* das condutas ilícitas, de modo sistematizado – ou seja, considerando todo o contexto cibernético em que estamos inseridos – é fundamental para se agregue valor aos debates e propostas de novas regulamentações e resoluções de conflitos.

Apesar de existirem tecnologias valiosas que oferecem proteção à privacidade e segurança, elas também podem ser utilizadas de forma maliciosa para dificultar a fiscalização e até mesmo autorizar a prática de atividades ilícitas e danosas.

A resposta a esses desafios envolve o desenvolvimento de ferramentas e protocolos inovadores, capazes de abranger todos as lacunas que são palco de delitos, além de uma maior cooperação internacional e debates (direcionados ao desenvolvimento de ações efetivas) sobre o equilíbrio entre segurança e privacidade.

Igualmente incontáveis são os desafios que surgem quando a regulamentação das novas tecnologias envolve o cenário internacional. Casos que envolvem plataformas digitais globais – que são a grande maioria hoje – apresentam

barreiras jurídicas e, ainda, de jurisdição internacional complexas. As principais dificuldades envolvem a aplicação de leis de nações distintas, o alcance da competência das autoridades locais sobre essas plataformas e, ainda, as inúmeras lacunas nas legislações que não acompanharam o rápido avanço tecnológico.

As plataformas digitais, tais como redes sociais e serviços de *streaming*, costumam possuir sede oficial em um país. Contudo, operam globalmente – ou seja, em todo o território internacional. Isso notoriamente gera uma gama de conflitos sobre qual país / jurisdição tem competência / autoridade para regular, fiscalizar e, principalmente, punir ações que ocorrem nessas plataformas. A situação se agrava quando estamos diante de um conflito de competência no qual a legislação de um país é mais permissiva que a de outro.

Presente, ainda, o problema da falta de cooperação internacional entre as nações. Além das limitações legais (diplomas normativos distintos e mais ou menos rígidos), temos também a ausência de tratados internacionais abrangentes. Assim, surgem as nações conhecidas como "paraísos digitais", que dificultam as investigações internacionais e, por vezes, chegam a se recusar a extraditar cidadãos que praticaram crimes digitais.

Nos casos em que essas barreiras são superadas, ou seja, em que os crimes são investigados e a legislação é aplicada, surge ainda outro problema: garantir a aplicação das penalidades impostas. Mesmo quando um tribunal de um país delibera contra uma plataforma digital global (p. ex. remoção de conteúdo; entrega de dados de usuários), o cumprimento dessa ordem pode ser desafiadora se a plataforma não tiver um aparato jurídico e tático significativo no país que emitiu a decisão.

6. CONCLUSÃO

Do estudo do tema é possível concluir que a regula-

mentação da internet é, hodiernamente, um dos temas mais polêmicos e complexos, envolvendo governos, sociedade civil, comunidades de internet e setores da iniciativa privada na elaboração de princípios, normas, regras e procedimentos decisórios para a regulamentação de ações que podem ou não ser feitas na rede (Segurado et. Al., 2015).

É um campo de grande disputa, reunindo atores com os mais diversos interesses e posicionamentos sobre como a internet deve funcionar e se ela deverá permanecer com a arquitetura livre, colaborativa e com garantia para a liberdade de expressão (Segurado et. Al., 2015).

Portanto, regras claras e bem orientadas ajudam a assegurar uma comunicação transparente e justa, prevenir abusos como a propagação de notícias falsas e a manipulação de eleitores, além de garantir o futuro democrático da sociedade civil.

Não podemos afirmar que na regulação está a solução das práticas delituosas digitais. Mas, podemos afirmar que na ausência dela certamente não está. Apenas o estudo aprofundado, o debate crítico-científico e a compreensão e superação das barreiras internacionais podem nos levar à regulação e concepção de processos eleitorais mais justos, democráticos, éticos e transparentes para o futuro próximo.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ANPD aplica a primeira multa por descumprimento à LGPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 2 out. 2024.

BRASIL. Internet chega a 87,2% dos brasileiros com mais de 10 anos em 2022, revele IBGE. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2023/novembro/internet-chega-a-87-2-dos-brasileiros -com-mais-de-10-anos-em--2022-revela-ibge>. Acesso em: 2 out. 2024.

BRASIL. Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9983.htm. Acesso em: 2 out. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 3 out. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 3 out. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 3 out. 2024.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal e o Código de Processo Penal para agravar a punição de crimes cometidos com o uso de meios eletrônicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 3 out. 2024.

CRESPO, Marcelo Xavier de F. Crimes digitais. Rio de Janeiro: Saraiva Jur, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 2 out. 2024.

DESINFORMANTE. Eleições e a regulação digital. Disponível em: https://desinformante.com.br/eleicoes-regulacao-digital/. Acesso em: 3 out. 2024.

MINISTÉRIO PÚBLICO FEDERAL. Eleições 2024: co-

nheça as regras para propaganda político-eleitoral na internet. Disponível em: <https://www.mpf.mp.br/pgr/noticias-pgr2/2024/eleicoes-2024-conheca-as-regras-para-propaganda-politico-eleitoral-na-internet>. Acesso em: 3 out. 2024.

SEGURADO, R.; LIMA, C. S. M. DE .; AMENI, C. S.. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. História, Ciências, Saúde-Manguinhos, v. 22, p. 1551–1571, dez. 2015.

TRIBUNAL SUPERIOR ELEITORAL. Resolução nº 23.732, de 27 de fevereiro de 2024. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em: 4 out. 2024.

TRIBUNAL SUPERIOR ELEITORAL. Saiba o que é permitido e o que é proibido na propaganda eleitoral nas ruas e na internet. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2024/Agosto/saiba-o-que-e-permitido-e-o-que-e-proibido-na-propaganda-eleitoral-nas-ruas-e-na-internet>. Acesso em: 4 out. 2024.

WE ARE SOCIAL. Digital 2024: 5 billion social media users. Disponível em: <https://wearesocial.com/uk/blog/2024/01/digital-2024-5-billion-social-media-users/>. Acesso em: 6 out. 2024.

CIBERSEGURANÇA NO PROCESSO ELEITORAL: PROTEÇÃO E SEGURANÇA

Flavia Alcassa[1]
Adrianne Lima[2]

1. INTRODUÇÃO

A integridade do processo eleitoral é fundamental para a preservação da democracia e a garantia de que a vontade popular seja devidamente representada. Com o avanço da tecnologia e a crescente digitalização de diversas etapas dos processos eleitorais, desde o registro de eleitores até a

1 Advogada, sócia-fundadora do escritório Alcassa & Pappert Advogados. É especializada em Direito Digital Corporativo e Relações de Trabalho. Atua como professora universitária e é DPO certificada pela Exin. Fundou a empresa Alcassa Innovation Tech. É coordenadora do livro LGPD no Direito do Trabalho (Saraiva Jur) e autora dos livros LGPD para Contratos e LGPD e Cartórios (Saraiva Jur). Possui formação em Proteção de Dados e Segurança Digital (FGV), Direito Contratual e Direito do Trabalho (FGV). É pós-graduada em Advocacia no Direito Digital e Proteção de Dados (Ebradi) e está cursando MBA em Digital Business (USP) e Pós-Graduação em Direito Privado, Tecnologia e Inovação (Ebradi).Contato: https://www.linkedin.com/in/fl%C3%A1via-alcassa

2 Advogada, Segurança da Informação, sócia-proprietária na ACC de Lima Consultoria Jurídica e Treinamentos, Consultora em LGPD, DPO as a service (terceirizado), Mestre em Administração e Desenvolvimento de Negócios pela Mackenzie, Instrutora trilha DPO Exin, Lead Implementer ISO 27701. Professora universitária – Universidade Presbiteriana Mackenzie e PUC Campinas, com as disciplinas de Pilares de Integridade, Proteção de Dados e Privacidade, Coordenadora dos livros LGPD para Contratos e LGPD no Direito do Trabalho (Saraiva Jur), Autora do livro LGPD Cartórios (Saraiva Jur). Coordenadora do livro Lima, A.; Alves, D. (2021). Encarregados - Data Protection Officer - DPOs exigidos pela LGPD - Lei Geral de Proteção de Dados. São Paulo, São Paulo, Brasil: Haikai Editora. ISBN: 978-65-86334-88-3. https://www.linkedin.com/posts/adrianneclima_dpoaas-consultoria-lgpd-activity-6848619432827334656-xoC9

apuração dos votos, as eleições tornaram-se cada vez mais suscetíveis a ataques cibernéticos e a vulnerabilidades digitais. Nesse contexto, a cibersegurança emerge como uma preocupação central para governos, instituições eleitorais e a sociedade como um todo.

No Brasil, o uso de urnas eletrônicas e a implementação de sistemas informatizados trouxeram inovações que aceleram o processo de votação e apuração, mas também geram novos desafios. A segurança das informações, a proteção contra ataques externos, a manipulação de dados e o combate à desinformação são fatores cruciais para garantir a legitimidade e a transparência das eleições.

O artigo reside na crescente importância da confiança pública nos processos democráticos. Em uma era de desinformação e ataques digitais, garantir a integridade eleitoral é essencial para preservar o estado de direito, assegurar a representação política autêntica e evitar crises de legitimidade governamental. A sociedade brasileira, precisa confiar plenamente na segurança e transparência das eleições, e a cibersegurança desempenha um papel crucial nesse sentido.

Embora este estudo tenha como objetivo examinar o papel da cibersegurança no processo eleitoral brasileiro, não se pretende esgotar o tema. A cibersegurança é uma área vasta e em constante evolução, e este artigo se propõe a oferecer uma visão geral, destacando os pontos mais relevantes no contexto atual. Assim, busca-se contribuir para o entendimento e o debate sobre o tema, sem a pretensão de abarcar todas as nuances e complexidades envolvidas. No Brasil, o debate sobre a cibersegurança no processo eleitoral ainda demanda mais aprofundamento e análise crítica.

2. DESENVOLVIMENTO

2.1 Conceito e relevância da cibersegurança no processo eleitoral

Existem várias definições nacionais e internacionais do

termo "cibersegurança". Eles definem cibersegurança como "a coleção de ferramentas, políticas, diretrizes, abordagens de gerenciamento de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser usadas para proteger a disponibilidade, integridade e confidencialidade de ativos nas infraestruturas conectadas pertencentes ao governo, organizações privadas e cidadãos; esses ativos incluem dispositivos computacionais conectados, pessoal, infraestrutura, aplicações, serviços digitais, sistemas de telecomunicações e dados no ambiente digital[3].

Um incidente cibernético que comprometa a segurança de serviços essenciais pode resultar em consequências devastadoras, não apenas para a operação das próprias organizações, mas também para a sociedade como um todo. Por exemplo, a interrupção de sistemas de votação eletrônica ou a manipulação de dados eleitorais pode afetar diretamente a legitimidade dos resultados e, consequentemente, a estabilidade política do país. Outro ponto crítico é a proteção das plataformas de votação e dos sistemas de contagem de votos. A vulnerabilidade desses sistemas pode ser explorada por agentes mal-intencionados, comprometendo a confiança do público nos resultados eleitorais. A necessidade de auditorias independentes e de testes de segurança constantes se torna evidente para mitigar esses riscos[4].

A cibersegurança no processo eleitoral refere-se ao conjunto de práticas, tecnologias e estratégias destinadas a proteger os sistemas eleitorais de ataques cibernéticos, manipulações de dados e fraudes digitais. A crescente digitalização dos processos eleitorais, incluindo o uso de urnas eletrônicas e sistemas informatizados de apuração, tornou-se um dos principais alvos de

3 JEFFERSON, David. **Security vulnerabilities in electronic voting systems**. Verified Voting Foundation, 2014. Disponível em: https://www.verifiedvoting.org/resources/voting-system-security/. Acesso em: 3 out. 2024.

4 FREITAS, Anderson. Cibersegurança e eleições no Brasil: um panorama das vulnerabilidades. **Revista Brasileira de Ciência da Computação**, 2019. Disponível em: https://www.rbccomputacao.org/ciberseguranca-eleicoes. Acesso em: 3 out. 2024.

ameaças cibernéticas, aumentando a necessidade de garantir a integridade, transparência e segurança dessas eleições[5].

A cibersegurança eleitoral envolve a análise e mitigação de vulnerabilidades em sistemas de votação eletrônica, que podem ser exploradas por atacantes para alterar resultados ou comprometer a privacidade dos eleitores. Em seus estudos, Halderman apontou que as urnas eletrônicas, embora eficientes, são suscetíveis a invasões, o que evidencia a importância de auditorias e revisões periódicas desses sistemas. A pesquisa de Halderman sobre vulnerabilidades nas urnas eletrônicas utilizadas no Brasil foi uma das mais impactantes para o debate sobre a segurança desse modelo de votação no país[6].

Rivest, co-inventor do algoritmo RSA[7], enfatiza que a criptografia é um dos pilares para a proteção dos dados eleitorais. Sua proposta de "independência de software" nas eleições sugere que os resultados de uma eleição devem ser verificáveis sem depender exclusivamente do software utilizado. Essa independência fortalece a transparência e dificulta a manipulação dos votos por meio de ataques ao sistema[8].

---

5 JEFFERSON, David. **Security vulnerabilities in electronic voting systems**. Verified Voting Foundation, 2014. Disponível em: https://www.verifiedvoting.org/resources/voting-system-security/. Acesso em: 3 out. 2024.

6 HALDERMAN, J. Alex. **Security analysis of the Diebold AccuVote-TS voting machine**. University of Michigan, 2006. Disponível em: https://jhalderm.com/pub/papers/ts-analysis.pdf. Acesso em: 3 out. 2024.

7 O algoritmo RSA, desenvolvido por Ronald Rivest, Adi Shamir e Leonard Adleman em 1977, é um dos mais amplamente utilizados sistemas de criptografia de chave pública. Baseia-se na dificuldade de fatorar grandes números primos e utiliza um par de chaves: uma pública, para criptografar mensagens, e uma privada, para descriptografá-las. Sua segurança depende da dificuldade em fatorar grandes números, tornando a decodificação impraticável sem a chave correta. O RSA é aplicado em comunicações seguras, como em protocolos HTTPS, assinaturas digitais e estabelecimento de chaves criptográficas em sistemas de segurança online.

8 RIVEST, Ronald. On the notion of 'software independence' in voting systems. **Journal of Cryptology,** 2008. Disponível em: https://people.csail.mit.edu/rivest/pubs.html. Acesso em: 3 out. 2024.

No contexto brasileiro, a cibersegurança no Brasil enfrenta desafios específicos, como a proteção das urnas eletrônicas e a infraestrutura digital associada às eleições. Freitas argumenta que a adoção de novas tecnologias e a digitalização dos processos de apuração tornaram o sistema mais ágil, mas também mais vulnerável a ataques cibernéticos sofisticados. Reforça-se a necessidade de investimentos contínuos em cibersegurança, não apenas em tecnologia, mas também em treinamento e preparação das equipes responsáveis pela gestão do processo eleitoral[9].

Diego Aranha, especialista em criptografia e segurança digital, após participar de testes públicos de segurança, demonstrou diversas vulnerabilidades que, se exploradas, poderiam comprometer a integridade do processo eleitoral. Aranha argumenta que, para assegurar a confiança pública nas eleições, é fundamental que os sistemas sejam auditáveis e que o processo de votação seja transparente e seguro. Ele também propõe melhorias, como o uso de métodos criptográficos mais robustos e a implementação de auditorias independentes[10].

Simons contribui para o debate com a defesa da importância de auditorias manuais e verificações pós-eleitorais para garantir a precisão dos resultados. Ele aponta que a tecnologia, por si só, não pode ser considerada completamente confiável e que os sistemas de votação devem ser testados e monitorados continuamente para detectar e corrigir falhas antes de qualquer tentativa de fraude[11].

---

9 FREITAS, Anderson. Cibersegurança e eleições no Brasil: um panorama das vulnerabilidades. **Revista Brasileira de Ciência da Computação**, 2019. Disponível em: https://www.rbccomputacao.org/ciberseguranca-eleicoes. Acesso em: 3 out. 2024.

10 ARANHA, Diego. **Segurança em urnas eletrônicas: análise crítica e proposta de melhorias.** Universidade Estadual de Campinas, 2020. Disponível em: https://www.ic.unicamp.br/~dir/seguranca-urnas.pdf. Acesso em: 3 out. 2024.

11 SIMONS, Barbara. Verified voting and election integrity. **Verified Voting Foundation**, 2018. Disponível em: https://www.verifiedvoting.org/verified-voting-and-election-integrity/. Acesso em: 3 out. 2024.

Por fim, Specter analisa os ataques realizados contra sistemas de votação remotos, como o ocorrido em Washington, D.C., em 2010. Ele expõe que esses sistemas, embora convenientes, são particularmente vulneráveis a ataques cibernéticos, tanto de atores externos quanto internos. Sua pesquisa reforça a necessidade de manter sistemas altamente seguros, além de implementar mecanismos de detecção de invasões em tempo real[12].

2.1 Importância no Contexto Eleitoral

A cibersegurança desempenha um papel fundamental na proteção de dados pessoais e na integridade dos sistemas eleitorais, garantindo que os processos democráticos ocorram de maneira justa e segura. Em um cenário cada vez mais digital, a defesa contra ataques cibernéticos e a manipulação de informações tornou-se um desafio crucial para a preservação da legitimidade das eleições. A vulnerabilidade dos sistemas eleitorais eletrônicos deve ser tratada como uma prioridade para proteger a integridade dos votos e a confiança pública nos resultados. Jefferson, aponta que, à medida que a tecnologia evolui, também aumentam as oportunidades para interferências externas, seja por hackers ou por atores maliciosos que buscam manipular os resultados[13].

A proteção de dados pessoais é uma das áreas mais críticas, uma vez que os sistemas eleitorais armazenam informações pessoais de eleitores, dados de votação e registros que devem ser mantidos em sigilo. Uma das maiores preocupações em relação às urnas eletrônicas e plataformas

12 SPECTER, Michael A. **Attacking the Washington, D.C. internet voting system**. MIT, 2012. Disponível em: https://people.csail.mit.edu/mspecter/. Acesso em: 3 out. 2024.

13 JEFFERSON, David. **Security vulnerabilities in electronic voting systems**. Verified Voting Foundation, 2014. Disponível em: https://www.verifiedvoting.org/resources/voting-system-security/. Acesso em: 3 out. 2024.

de votação é a possibilidade de invasões que possam comprometer a confidencialidade desses dados ou até mesmo alterar os resultados eleitorais. A adoção de auditorias rigorosas e mecanismos de verificação é essencial para garantir que, mesmo que haja tentativas de ataque, elas possam ser identificadas e mitigadas a tempo[14].

Rivest defende o conceito de "independência de software", que permite que os votos sejam verificados independentemente dos sistemas utilizados, reforçando a transparência e a confiança no processo[15].

No contexto brasileiro, onde as urnas eletrônicas são amplamente utilizadas, a questão da segurança é frequentemente discutida por especialistas. Aranha, em suas análises, no passado, identificou diversas vulnerabilidades nos sistemas eleitorais brasileiros que poderiam ser exploradas para manipular os resultados. Ele destaca a importância de realizar testes públicos de segurança e a necessidade de aprimorar constantemente os sistemas de proteção utilizados nas urnas eletrônicas, de modo a prevenir interferências internas e externas[16].

A cibersegurança não se limita apenas à proteção dos votos, mas também das plataformas de comunicação utilizadas durante o período eleitoral, como redes sociais e sites de campanhas. Estas plataformas podem ser alvos de desinformação e ataques coordenados com o objetivo de influenciar o comportamento dos eleitores. A cibersegurança eleitoral, portanto, deve abranger a defesa contra a disseminação

14 HALDERMAN, J. Alex. **Security analysis of the Diebold AccuVote-TS voting machine**. University of Michigan, 2006. Disponível em: https://jhalderm.com/pub/papers/ts-analysis.pdf. Acesso em: 3 out. 2024.

15 RIVEST, Ronald. On the notion of 'software independence' in voting systems. **Journal of Cryptology,** 2008. Disponível em: https://people.csail.mit.edu/rivest/pubs.html. Acesso em: 3 out. 2024.

16 ARANHA, Diego. **Segurança em urnas eletrônicas: análise crítica e proposta de melhorias.** Universidade Estadual de Campinas, 2020. Disponível em: https://www.ic.unicamp.br/~dir/seguranca-urnas.pdf. Acesso em: 3 out. 2024.

de fake news, ataques de negação de serviço (DDoS) e tentativas de hackeamento que possam comprometer a integridade da comunicação eleitoral[17].

Por fim, além da segurança cibernética. A transparência e a capacidade de rever e auditar os resultados eleitorais são cruciais para preservar a confiança pública e evitar questionamentos sobre a legitimidade das eleições[18].

2.2 Ameaças Cibernéticas no Processo Eleitoral

Os ataques cibernéticos representam uma das maiores ameaças à integridade dos processos eleitorais, uma vez que podem comprometer tanto os sistemas de votação quanto as plataformas de comunicação utilizadas durante as eleições. Esses ataques podem ocorrer de diversas formas, variando em sofisticação e impacto, e têm o potencial de influenciar diretamente os resultados eleitorais, a confiança pública no sistema e a estabilidade democrática.

Os ataques de hacking em sistemas de votação eletrônica podem resultar na alteração ou manipulação dos votos. Esses ataques podem ocorrer de maneira direta, com invasores comprometendo os softwares de votação, ou de forma indireta, com interferências nos sistemas de apuração. Os hackers podem explorar vulnerabilidades desconhecidas, chamadas de "zero-day", para obter acesso aos sistemas antes que as falhas sejam corrigidas[19].

Outro ataque comum em períodos eleitorais é o

17 FREITAS, Anderson. Cibersegurança e eleições no Brasil: um panorama das vulnerabilidades. **Revista Brasileira de Ciência da Computação**, 2019. Disponível em: https://www.rbccomputacao.org/ciberseguranca-eleicoes. Acesso em: 3 out. 2024.

18 SIMONS, Barbara. Verified voting and election integrity. **Verified Voting Foundation**, 2018. Disponível em: https://www.verifiedvoting.org/verified-voting-and-election-integrity/. Acesso em: 3 out. 2024.

19 JEFFERSON, David. **Security vulnerabilities in electronic voting systems**. Verified Voting Foundation, 2014. Disponível em: https://www.verifiedvoting.org/resources/voting-system-security/. Acesso em: 3 out. 2024.

phishing, uma técnica utilizada para enganar usuários e obter acesso a informações confidenciais, como credenciais de login. As campanhas de phishing direcionadas a funcionários eleitorais podem comprometer sistemas inteiros. Ao clicar em links maliciosos ou fornecer informações confidenciais inadvertidamente, esses funcionários podem abrir uma "porta de entrada" para os atacantes, permitindo que eles interfiram diretamente nos sistemas de votação ou obtenham informações sensíveis[20].

Os ataques de negação de serviço (DDoS) também são uma tática amplamente utilizada para desestabilizar os sistemas eleitorais. Embora os ataques DDoS não alterem diretamente os votos, eles podem impedir que os eleitores tenham acesso a plataformas de votação online ou informações importantes sobre o processo eleitoral. Ao sobrecarregar servidores com um volume massivo de solicitações, os atacantes conseguem tirar do ar sites de informação eleitoral, aplicativos de votação ou até mesmo sistemas de apuração de votos, criando caos e desconfiança[21].

Aranha, ao analisar a segurança das urnas eletrônicas brasileiras, no passado, em estudo, identificou a possibilidade de inserção de malware nos dispositivos. O malware, um software malicioso que pode ser instalado secretamente em máquinas de votação, é capaz de manipular os votos sem ser detectado pelos eleitores ou pelos administradores do sistema. Aranha destaca a importância de auditorias e testes de segurança regulares para detectar e remover malwares antes

20 HALDERMAN, J. Alex. **Security analysis of the Diebold AccuVote-TS voting machine**. University of Michigan, 2006. Disponível em: https://jhalderm.com/pub/papers/ts-analysis.pdf. Acesso em: 3 out. 2024.

21 RIVEST, Ronald. On the notion of 'software independence' in voting systems. **Journal of Cryptology,** 2008. Disponível em: https://people.csail.mit.edu/rivest/pubs.html. Acesso em: 3 out. 2024.

que possam comprometer o processo eleitoral[22].

Outro ponto destacado são os ataques direcionados à infraestrutura de rede das eleições, o que pode afetar diretamente a transmissão e o armazenamento dos resultados. Nesse sentido, o uso de técnicas de spoofing e sniffing pode permitir que atacantes interceptem ou modifiquem dados transmitidos entre urnas eletrônicas e servidores centrais de apuração, afetando os resultados de forma imperceptível[23].

Specter explora como ataques direcionados a sistemas de votação remotos, como em eleições online ou por e-mail, são particularmente vulneráveis. Em um estudo de caso sobre o sistema de votação online em Washington, D.C., Specter demonstrou que hackers conseguiram controlar o sistema e modificar votos sem serem detectados, expondo o grande risco de eleições conduzidas por plataformas digitais mal protegidas[24].

Além desses ataques, estudos reforçam a relevância da proteção contra campanhas de desinformação, que são utilizadas para minar a confiança dos eleitores no processo eleitoral. Ataques de desinformação podem ser amplificados por bots automatizados e redes sociais, e frequentemente utilizam técnicas de hacking para acessar dados confidenciais de campanhas eleitorais ou manipular informações, criando

22 ARANHA, Diego. **Segurança em urnas eletrônicas: análise crítica e proposta de melhorias.** Universidade Estadual de Campinas, 2020. Disponível em: https://www.ic.unicamp.br/~dir/seguranca-urnas.pdf. Acesso em: 3 out. 2024.

23 FREITAS, Anderson. Cibersegurança e eleições no Brasil: um panorama das vulnerabilidades. **Revista Brasileira de Ciência da Computação**, 2019. Disponível em: https://www.rbccomputacao.org/ciberseguranca-eleicoes. Acesso em: 3 out. 2024.

24 SPECTER, Michael A. **Attacking the Washington, D.C. internet voting system**. MIT, 2012. Disponível em: https://people.csail.mit.edu/mspecter/. Acesso em: 3 out. 2024.

dúvidas sobre a integridade do processo[25].

Em 2024, um caso emblemático envolvendo a violação de dados eleitorais no Reino Unido destacou a gravidade dos lapsos de segurança digital no contexto eleitoral. Conforme relatado pelo The Guardian (2024), falhas na segurança online resultaram no comprometimento dos dados de 40 milhões de eleitores britânicos, um incidente que chamou a atenção para a fragilidade dos sistemas de proteção utilizados em eleições altamente digitalizadas. Este caso revelou a importância de fortalecer os mecanismos de segurança cibernética e a necessidade de auditorias frequentes para proteger informações sensíveis de eleitores. A lição central aprendida com esse ataque é que, em tempos de crescente digitalização, a cibersegurança deve ser tratada como prioridade máxima por governos e autoridades eleitorais. A vulnerabilidade dos dados expôs a possibilidade de interferências externas que poderiam impactar diretamente o resultado eleitoral ou minar a confiança pública no processo democrático. A falta de proteção adequada não só coloca em risco a privacidade dos eleitores, mas também abre caminho para manipulações internas e externas[26].

Casos como o do Reino Unido ressaltam a necessidade de sistemas robustos de criptografia e a implementação de auditorias frequentes e rigorosas para verificar a integridade sistemas de votação[27], conforme sugerido por Aranha.

---

25 FREITAS, Anderson. Cibersegurança e eleições no Brasil: um panorama das vulnerabilidades. **Revista Brasileira de Ciência da Computação**, 2019. Disponível em: https://www.rbccomputacao.org/ciberseguranca-eleicoes. Acesso em: 3 out. 2024. SIMONS, Barbara. Verified voting and election integrity. **Verified Voting Foundation**, 2018. Disponível em: https://www.verifiedvoting.org/verified-voting-and-election-integrity/. Acesso em: 3 out. 2024.

26 JORNAL THE GUARDIAN. **Lapsos de segurança on-line levaram a dados de 40 milhões de eleitores do Reino Unido sendo hackeados, diz ICO**. Disponível em: https://www.theguardian.com/politics/article/2024/jul/30/online-security-lapses-led-to-data-of-40m-uk-voters-being-hacked-says-ico. Acesso em: 03 out. 2024.

27 ARANHA, Diego. **Segurança em urnas eletrônicas: análise crítica e pro-**

A falha em proteger adequadamente as bases de dados eleitorais não só coloca em risco a integridade dos processos eleitorais, como também pode desestabilizar a confiança dos cidadãos nas instituições democráticas[28].

Durante a campanha presidencial na França em 2017, a equipe de Emmanuel Macron foi alvo de um ataque cibernético que resultou no vazamento de documentos internos, logo antes da votação. O ataque, supostamente realizado por grupos com laços com a Rússia, seguiu um padrão semelhante ao ataque à DNC nos EUA[29].

A resposta rápida da equipe de Macron, que alertou o público sobre o vazamento e as tentativas de manipulação, ajudou a mitigar o impacto. Este caso ressalta a importância da transparência e da comunicação rápida em resposta a ataques cibernéticos, além de evidenciar a necessidade de sistemas de segurança robustos e da preparação para possíveis vazamentos de dados[30].

Nas eleições presidenciais de 2019, a Ucrânia enfrentou uma série de ataques cibernéticos que buscavam desestabilizar o processo eleitoral. O governo ucraniano relatou tentativas de hacking de seus sistemas eleitorais, incluindo um ataque DDoS que visava desativar sites oficiais

---

posta de melhorias. Universidade Estadual de Campinas, 2020. Disponível em: https://www.ic.unicamp.br/~dir/seguranca-urnas.pdf. Acesso em: 3 out. 2024.

28 RIVEST, Ronald. On the notion of 'software independence' in voting systems. **Journal of Cryptology,** 2008. Disponível em: https://people.csail.mit.edu/rivest/pubs.html. Acesso em: 3 out. 2024.

29 AGNÈS, H. Cybersecurity and the 2017 French Presidential Election: Lessons Learned. **Journal of Cyber Policy**, v. 2, n. 2, p. 145-158, 2017. DOI: 10.1080/23738871.2017.1354704.

30 KELLER, T. The Impact of Cyberattacks on the French Presidential Election. **International Affairs**, v. 93, n. 5, p. 1099-1116, 2017. DOI: 10.1093/ia/iix104

relacionados às eleições[31]. As autoridades responderam com uma forte defesa cibernética, incluindo parcerias com empresas de segurança digital para proteger seus sistemas. Este caso destaca a importância de uma estratégia de segurança cibernética proativa e o papel da colaboração internacional na proteção das eleições contra interferências externas[32].

2.3 Legislação e Resolução de Proteção de dados no Brasil

A cibersegurança no processo eleitoral é uma questão crítica que envolve a proteção dos dados pessoais dos cidadãos e a integridade do sistema democrático. No Brasil,

diversas leis e normas regulam a segurança cibernética, com destaque para o Código Eleitoral, a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet e as resoluções do Tribunal Superior Eleitoral (TSE). Essas normativas visam não apenas proteger os dados dos eleitores, mas também assegurar que o processo eleitoral ocorra de maneira transparente e segura.

O Código Eleitoral brasileiro, instituído pela Lei nº 4.737, de 15 de julho de 1965, estabelece as regras fundamentais para a realização das eleições, incluindo diretrizes sobre a coleta e o tratamento de dados dos eleitores. Com a entrada em vigor da LGPD, promulgada em 2018, houve uma importante evolução na proteção de dados pessoais. A LGPD define princípios claros para o tratamento de dados, como a finalidade, a transparência e a segurança. A legisla-

31 NORDLAND, R. Ukraine Accuses Russia of Election Interference as Attacks Target Voting Websites. **The New York Times**, 2019. Disponível em: https://www.nytimes.com/2019/04/18/world/europe/ukraine-election-russia.html. Acesso em: 3 out. 2024.

32 HODGSON, A. Cybersecurity in Ukraine: Lessons from the 2019 Presidential Elections. *Cybersecurity Review*, v. 5, n. 1, p. 22-36, 2020. DOI: 10.1016/j.csr.2020.100010.

ção determina que o tratamento de dados deve respeitar a finalidade original da coleta e que os titulares devem ter acesso a informações sobre como seus dados são utilizados, além de possibilitar a eliminação dos mesmos quando solicitado[33].

Em fevereiro de 2024, a Resolução TSE nº 23.732/2024 foi promulgada, revisando a Resolução TSE nº 23.610/2019, que trata da propaganda eleitoral. Essa nova resolução introduziu diretrizes rigorosas sobre o manejo de dados pessoais durante as campanhas. Ela exige que partidos e candidaturas disponibilizem canais para que os eleitores confirmem o tratamento de seus dados e solicitem a eliminação quando desejarem. Em municípios com menos de 200 mil eleitores, as legendas não precisam indicar um encarregado, mas devem manter um canal de comunicação para questões relacionadas à proteção de dados. Adicionalmente, a resolução estabelece que o tratamento de dados sensíveis requer consentimento explícito dos titulares, reforçando a responsabilidade das agremiações na proteção e segurança dos dados coletados. Os relatórios de impacto são outro aspecto importante da nova normativa. Nas eleições para cargos relevantes, a Justiça Eleitoral pode exigir a elaboração de relatórios que detalhem os tipos de dados coletados, os riscos identificados e as medidas de segurança adotadas. Essa exigência visa aumentar a transparência e a responsabilidade no tratamento de dados, alinhando-se aos princípios da LGPD[34].

2.4 Papel do Tribunal Superior Eleitoral (TSE)

O Tribunal Superior Eleitoral (TSE) tem desempenhado um papel essencial na implementação de medidas de

33 OAB CAMPINAS. **A LGPD no processo eleitoral**. Disponível em: https://oabcampinas.org.br/a-lgpd-no-processo-eleitoral/#_ftnref16. Acesso em: 03 out. 2024.

34 TRIBUNAL SUPERIOR ELEITORAL. **Resolução TSE nº 23.732, de 27 de fevereiro de 2024**. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 03 out. 2024.

cibersegurança para assegurar a integridade e transparência do processo eleitoral no Brasil. Com o avanço da tecnologia e a crescente digitalização das eleições, o TSE adotou diversas estratégias que visam garantir a segurança dos sistemas eleitorais, proteger os dados dos eleitores e promover a confiança pública no processo de votação. Entre as medidas adotadas pelo TSE, destacam-se a criação de comissões de auditoria e a formalização de acordos de cooperação técnica com outras instituições.

Uma das principais iniciativas do TSE foi a assinatura de um acordo de cooperação técnica com a Autoridade Nacional de Proteção de Dados (ANPD). Esse acordo, formalizado em 2024, visa fortalecer a proteção de dados pessoais nas eleições. O objetivo é que as duas instituições atuem em conjunto para garantir que os dados dos eleitores sejam tratados de acordo com a Lei Geral de Proteção de Dados (LGPD), prevenindo violações de privacidade e assegurando a transparência no tratamento das informações pessoais durante o processo eleitoral[35]. Esse acordo reforça a importância de colaboração interinstitucional para enfrentar os desafios da cibersegurança no contexto eleitoral, garantindo a conformidade com as normas legais e regulamentares.

Além disso, o TSE promove amplas oportunidades de auditoria dos sistemas eleitorais, com foco na verificação e transparência do funcionamento das urnas eletrônicas e demais softwares utilizados no processo eleitoral. Segundo a Resolução TSE nº 23.673/2021, as auditorias incluem o Teste Público de Segurança da Urna (TPS), um evento que ocorre antes das eleições e que reúne especialistas em Tecnologia da Informação para testar a segurança das urnas. O TPS permite que eventuais vulnerabilidades sejam identificadas

35 TRIBUNAL SUPERIOR ELEITORAL; AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Acordo de cooperação técnica**. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/TSEANPDacordocooperacaotecnica.pdf. Acesso em: 3 out. 2024.

e corrigidas, garantindo que o sistema esteja devidamente protegido contra possíveis ataques cibernéticos. Em 2024, por exemplo, o TSE realizou o Teste de Confirmação em maio, após as implementações sugeridas no TPS de 2023, reforçando ainda mais a segurança do sistema eleitoral[36] .

No dia da votação, o TSE também realiza outros testes para verificar a integridade dos sistemas e das urnas eletrônicas. Entre esses testes, destacam-se o Teste de Autenticidade dos Sistemas Eleitorais e o Teste de Integridade das Urnas Eletrônicas, que simulam uma votação para garantir que os votos depositados sejam contabilizados corretamente. Além disso, há o Teste de Integridade com Biometria, que utiliza as impressões digitais de eleitores voluntários para assegurar que o sistema biométrico funcione corretamente. Essas medidas, aliadas à emissão do Boletim de Urna (BU), garantem a transparência dos resultados e permitem que a sociedade civil acompanhe de perto o processo eleitoral por meio de ferramentas como o aplicativo "Boletim na Mão"[37].

Essas ações do TSE demonstram um compromisso contínuo com a transparência e a segurança no processo eleitoral, promovendo a confiança pública nas eleições. Ao adotar rigorosas auditorias e estabelecer parcerias com instituições como a ANPD, o TSE fortalece a cibersegurança e assegura que o sistema eleitoral brasileiro continue a ser um exemplo de integridade e eficiência no cenário global.

---

36 TRIBUNAL SUPERIOR ELEITORAL. **Resolução TSE nº 23.673, de 2021**. 2021. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Setembro/faltam-29-dias-auditorias-nos-sistemas-eleitorais-ocorrem-antes-durante-e-depois--das-eleicoes. Acesso em: 3 out. 2024.

37 TRIBUNAL SUPERIOR ELEITORAL. **Resolução TSE nº 23.732, de 27 de fevereiro de 2024.** Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 3 out. 2024.

3. CONSIDERAÇÕES FINAIS

Os processos eleitorais são intrinsecamente complexos, variando conforme os sistemas e contextos democráticos de cada país. Para proteger a integridade desses processos, é fundamental que as instituições eleitorais implementem medidas de segurança robustas, capacitem seus funcionários e assegurem que a sociedade tenha acesso a informações claras sobre as práticas de segurança. Nesse cenário, os acordos de cooperação nacional e internacional permitem a troca de informações e melhores práticas entre países para criar frameworks globais de cibersegurança. Dado que as ameaças podem surgir de qualquer parte do mundo, a cooperação internacional fortalece a defesa cibernética, facilitando o compartilhamento de informações sobre ameaças e estratégias de mitigação.

Investir na educação do eleitorado sobre segurança digital também se mostra crucial, capacitando os cidadãos a reconhecerem tentativas de fraude e desinformação. A construção de um ambiente eleitoral seguro é um esforço coletivo que demanda a colaboração de governos, instituições eleitorais e a sociedade civil. A cibersegurança, portanto, desempenha um papel central na preservação da integridade e confiança no processo eleitoral. Analisando casos práticos de ataques cibernéticos em eleições internacionais, reforça-se a vulnerabilidade dos sistemas eleitorais, destacando a necessidade de uma vigilância contínua e de medidas protetivas robustas. À medida que a tecnologia avança, o processo eleitoral digitalizado traz tanto oportunidades quanto novos desafios, como o aumento dos ataques direcionados. A resposta a essas ameaças deve evoluir com as táticas maliciosas, exigindo uma constante atualização das práticas de segurança para garantir a confiança no sistema democrático.

REFERÊNCIAS

AGNÈS, H. Cybersecurity and the 2017 French Presidential Election: Lessons Learned. Journal of Cyber Policy, v. 2, n. 2, p. 145-158, 2017. DOI: 10.1080/23738871.2017.1354704.

ARANHA, Diego. Segurança em urnas eletrônicas: análise crítica e proposta de melhorias. Universidade Estadual de Campinas, 2020. Disponível em: https://www.ic.unicamp.br/~dir/seguranca-urnas.pdf. Acesso em: 3 out. 2024.

DIVVA, A. Cybersecurity and Election Integrity: The Role of Audits and Collaboration. Linnæus University, 2024. Disponível em: https://lnu.diva-portal.org/smash/get/diva2:1867013/FULLTEXT01.pdf. Acesso em: 3 out. 2024.

FREITAS, Anderson. Cibersegurança e eleições no Brasil: um panorama das vulnerabilidades. Revista Brasileira de Ciência da Computação, 2019. Disponível em: https://www.rbccomputacao.org/ciberseguranca-eleicoes. Acesso em: 3 out. 2024.

HALDERMAN, J. Alex. Security analysis of the Diebold AccuVote-TS voting machine. University of Michigan, 2006. Disponível em: https://jhalderm.com/pub/papers/ts-analysis.pdf. Acesso em: 3 out. 2024.

HODGSON, A. Cybersecurity in Ukraine: Lessons from the 2019 Presidential Elections. *Cybersecurity Review*, v. 5, n. 1, p. 22-36, 2020. DOI: 10.1016/j.csr.2020.100010.

JEFFERSON, David. Security vulnerabilities in electronic voting systems. Verified Voting Foundation, 2014. Disponível em: https://www.verifiedvoting.org/resources/voting-system-security/. Acesso em: 3 out. 2024.

JORNAL THE GUARDIAN. Lapsos de segurança on-line levaram a dados de 40 milhões de eleitores do Reino Unido sendo hackeados, diz ICO. Disponível em: https://www.theguardian.com/politics/article/2024/jul/30/online-securi-

ty-lapses-led-to-data-of-40m-uk-voters-being-hacked-says-ico. Acesso em: 03 out. 2024.

KELLER, T. The Impact of Cyberattacks on the French Presidential Election. International Affairs, v. 93, n. 5, p. 1099-1116, 2017. DOI: 10.1093/ia/iix104.

NORDLAND, R. Ukraine Accuses Russia of Election Interference as Attacks Target Voting Websites. The New York Times, 2019. Disponível em: https://www.nytimes.com/2019/04/18/world/europe/ukraine-election-russia.html. Acesso em: 3 out. 2024.

OAB CAMPINAS. A LGPD no processo eleitoral. Disponível em: https://oabcampinas.org.br/a-lgpd-no-processo-eleitoral/#_ftnref16. Acesso em: 03 out. 2024.

OTEMPO. Ano eleitoral é desafio para cibersegurança e dados, diz especialista. O Tempo, 2024. Disponível em: https://www.otempo.com.br/brasil/ano-eleitoral-e-desafio-para-ciberseguranca-e-dados-diz-especialista-confira-1.3322007. Acesso em: 3 out. 2024.

RIVEST, Ronald. On the notion of 'software independence' in voting systems. Journal of Cryptology**,** 2008. Disponível em: https://people.csail.mit.edu/rivest/pubs.html. Acesso em: 3 out. 2024.

SIMONS, Barbara. Verified voting and election integrity. Verified Voting Foundation, 2018. Disponível em: https://www.verifiedvoting.org/verified-voting-and-election-integrity/. Acesso em: 3 out. 2024.

SPECTER, Michael A. Attacking the Washington, D.C. internet voting system. MIT, 2012. Disponível em: https://people.csail.mit.edu/mspecter/. Acesso em: 3 out. 2024.

TRIBUNAL SUPERIOR ELEITORAL; AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Acordo de cooperação técnica. 2024. Disponível em: https://www.gov.br/

anpd/pt-br/assuntos/noticias/TSEANPDacordocooperacao-tecnica.pdf. Acesso em: 3 out. 2024.

TRIBUNAL SUPERIOR ELEITORAL. Resolução TSE nº 23.673, de 2021. 2021. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Setembro/faltam-29-dias-auditorias-nos-sistemas-eleitorais-ocorrem-antes-durante-e-depois-das-eleicoes. Acesso em: 3 out. 2024.

TRIBUNAL SUPERIOR ELEITORAL. Resolução TSE nº 23.732, de 27 de fevereiro de 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 3 out. 2024.

UN. General Assembly Resolution on Privacy and Protection of Data. 2018. Disponível em: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/179. Acesso em: 3 out. 2024.

DEEPFAKES E MANIPULAÇÃO ELEITORAL: RISCOS DE CONTEÚDOS AUDIOVISUAIS MANIPULADOS

Gisele Truzzi[1]
Beatriz de Andrade Junque[2]
Iasmin Palotta[3]

1 Advogada especialista em Direito Digital e Segurança da Informação; Fundadora de *Gisele Truzzi Tech Legal Advisory*. Atuante na área do Direito Digital há mais de 19 anos, dos quais 14 são à frente de seu próprio escritório. Graduada em Direito pela Universidade Presbiteriana Mackenzie, com pós-graduação em Segurança da Informação e Direito Eletrônico pela FGV-RJ. Certificada em Direitos Autorais para a Internet pela Harvard Law School, em parceria com o ITS-RJ. Atualmente cursa pós-graduação em Neurociências, Comunicação e Desenvolvimento Humano pelo Centro de Mediadores. É professora convidada de diversas instituições de ensino jurídico, lecionando matérias relacionadas ao Direito Digital, Proteção de Dados e Privacidade, Compliance, Inovação e Segurança da Informação (EPD/SP, PUC – Campinas, ESA/OAB, entre outras). Autora de diversas obras jurídicas e artigos, publicados em diversos portais e revistas, tais como ISTOÉ Dinheiro, Conjur, Galileu, IBDI/IOB, entre outros. Coautora das obras "Direito Digital: Debates Contemporâneos" (ed. RT, 2019) e "Manual de Educação Digital, Cibercidadania e Prevenção de Crimes Cibernéticos" (ed. Juspodivm, 2021). Atualmente assessora diversas empresas que necessitam de suporte jurídico especializado em demandas relacionadas à Tecnologia. Ministra palestras e treinamentos em todo o Brasil.

2 Advogada e Gestora de Projetos em *Gisele Truzzi Tech Legal Advisory.* Atuante nas áreas de Direito Digital, Privacidade e Proteção de Dados, Propriedade Intelectual e Direito do Entretenimento. Graduada pela PUC-Campinas e Especialista em Direito Digital e Compliance pelo Damásio/IBMEC. Presidente da Comissão de Direito Digital da OAB subseção de Indaiatuba/SP. Membro da Comissão de Proteção de Dados e da Comissão de Startup e Inovação, ambas da OAB subseção de Campinas/SP. Cofundadora do Grupo de Estudos de Direito Digital da PUC-Campinas. Autora das obras coletiva "Direito Digital: Reflexões do grupo de estudos sobre os impactos no direito público e privado", Grupo Editorial Livramento e "Lei Geral de Proteção de Dados: aspectos de direito penal e combate à discriminação", Editora Almedina, 2024.

3 Advogada, sócia em *Gisele Truzzi Tech Legal Advisory.* Atuante nas áreas de Direito Digital, Privacidade e Proteção de Dados e Propriedade Intelectual.

Com a evolução das tecnologias estamos cada vez mais imersos em um mundo altamente conectado, no qual utilizamos inovações de diversas formas em nosso cotidiano.

Nos últimos anos, a Inteligência Artificial (IA), ganhou destaque tornando-se acessível ao público em geral. Isso facilita tarefas cotidianas e integra a IA em nossa realidade de várias maneiras.

Atualmente, temos ferramentas de IA que nos ajudam a criar imagens e textos, facilitam o cotidiano em atividades domésticas, mapeiam dados, otimizam nossa rotina e muito mais, tudo ao alcance de nossos celulares, tablets e dispositivos domésticos.

Assim, a tradução literal de *deepfake* é "profundamente falso". Essa tecnologia envolve o uso de inteligência artificial para criar vídeos, imagens e vozes quase idênticos aos do ser humano retratado, gerados inteiramente por algoritmos. Isso permite que a pessoa retratada apareça em um vídeo falando algo que nunca disse ou que sua aparência seja alterada, possibilitando que sua imagem seja manipulada conforme a vontade de quem está manipulando o *deepfake*.

Deste modo, em entrevista para o Jornal da USP, a professora Giselle Beiguelman descreve deepfakes como:

> "Os *deepfakes* são imagens produzidas por processos de aprendizado maquínico (*machine learning*), ou seja, de Inteligência Artificial, através de uma metodologia chamada redes neurais, e que têm como principal característica serem criadas integralmente por algoritmos. Como o próprio nome diz, procura reproduzir comportamentos e mecanismos de sistemas neurais humanos."[4]

Dessa forma, estes programas, possibilitam reunir milhões de imagens presentes em banco de dados, criando vídeos e imagens extremamente realistas.

4 Fonte: https://jornal.usp.br/cultura/cada-vez-mais-sofisticados-deepfakes--vieram-para-ficar/. Acessado em 10/10/2024.

Sendo assim, o que mais chama a atenção nos casos de uso do *deepfake* é a dificuldade em identificar que o conteúdo foi gerado exclusivamente por inteligência artificial, o que facilita a disseminação de notícias falsas à população.

Por ser uma ferramenta eficaz na disseminação de notícias falsas, o *deepfake* representa grande perigo, especialmente no cenário eleitoral, pois pode espalhar informações errôneas entre os eleitores, prejudicando a reputação e a campanha dos candidatos, além de gerar manipulação em massa, levando à conclusões equivocadas.

Por mais que posteriormente, a pessoa que se viu vítima de um *deepfake* consiga esclarecer que o conteúdo foi gerado falsamente, até que isso seja provado, o dano à sua imagem e reputação já foi causado; com inúmeras pessoas acessando o conteúdo falso e acreditando primariamente no *deepfake* divulgado. Esse impacto pode trazer inúmeras consequências irreversíveis à vida pessoal, profissional e emocional do indivíduo, ocasionando reputação equivocada, ruptura em relacionamentos, demissões, rescisão de contratos, entre outros problemas; sem contar as questões de hiperexposição e difamação.

Deste modo, com o presente artigo, buscamos entender o cenário atual eleitoral, com a utilização de *deepfakes*, e possíveis soluções.

1. HISTÓRICO DO USO DE *DEEPFAKES*

Notícias falsas sempre estiveram presentes nas redes sociais, conhecidas popularmente como *fake news*, e com a evolução passamos a ter o *deepfake,* revolucionando a forma de disseminação de *fake news*.

O *deepfake* pode ser utilizado na indústria audiovisual, como por exemplo, envelhecendo atores, ou os tornando mais jovens. No entanto, surgem problemas quando essa tecnologia ultrapassa o âmbito ficcional e começa a interferir em nosso cotidiano, gerando falsas conclusões e produzindo

manipulação do público.

Entre os casos de grande relevância que se tornaram notícias mundiais, destaca-se o *deepfake* do Papa Francisco, vestido com uma enorme jaqueta branca e tênis com detalhes em dourado, que gerou o título de "Papa Fashion"[5]. Outro exemplo é a conta criada no TikTok com a aparência do ator Tom Cruise, também feita por meio de *deepfake*, além de vídeos e imagens de diversos outros artistas que circulam nas redes sociais[6].

No cenário político, o uso de *deepfakes* não é novidade. Um exemplo notável é um vídeo divulgado em 2018 no site BuzzFeed, que apresenta o ex-presidente dos Estados Unidos, Barack Obama, fazendo ataques aos Panteras Negras, uma organização antirracista, além de proferir ofensas ao ex-presidente Donald Trump[7].

Nas eleições de 2018, a preocupação com a disseminação de *fake news* tornaram-se essenciais.

Assim, em 2020 o TSE (Tribunal Superior Eleitoral) iniciou a conscientização acerca de *deepfakes*, informando que é necessário desconfiar até daquilo que se vê com os próprios olhos.

Neste contexto, são apresentadas dicas para reconhecer um *deepfake*. É importante prestar atenção aos movimentos da boca, garantindo que estejam sincronizados com o que está sendo falado. Além disso, deve-se avaliar se a entonação e o som da voz são naturais e observar se os olhos da pessoa piscam normalmente[8].

---

5 Fonte: https://www.palavraaberta.org.br/artigo/o-estranho-caso-do-papa-fashion. Acessado em 10/10/2024.

6 Fonte: https://tecnoblog.net/noticias/criador-de-deepfakes-de-tom-cruise-no-tiktok-conta-como-criou-videos/. Acessado em 10/10/2024.

7 Fonte: https://variety.com/2018/digital/news/jordan-peele-obama-fake-news-video-buzzfeed-1202755517/. Acessado em 10/10/2024.

8 Fonte: https://www.tre-pr.jus.br/comunicacao/noticias/2020/Janeiro/justica-eleitoral-alerta-para-deepfakes. Acessado em 10/10/2024.

Frequentemente, a pessoa pode se mover de maneira não natural. Por isso, é recomendável assistir a vídeos da mesma pessoa para facilitar a comparação.

Um dos primeiros casos no Brasil do uso de *deepfake* no contexto político ocorreu em 2018, envolvendo o ex-prefeito e ex-governador de São Paulo, João Dória Júnior: na cena divulgada em vídeo, ele aparecia nu com diversas mulheres nuas em um quarto[9].

Além de notícias, também foi realizado o Programa Minuto da Checagem, que é uma ação do TSE com o objetivo de combater a desinformação, explicando o que é o *deepfake*[10].

No entanto, entre 2018 e 2024, a inteligência artificial evoluiu de forma significativa e se tornou amplamente acessível ao público. Isso ressalta a necessidade urgente de desenvolver orientações e regulamentações para o uso de *deepfakes* no contexto atual.

2. O IMPACTO DE *DEEPFAKES* NO CENÁRIO ELEITORAL ATUAL

Em 27/02/2024 o TSE regulamentou o uso da inteligência artificial na propaganda política para as eleições deste ano.

Ao alterar a Resolução nº 23.610/2019, que trata de propaganda eleitoral, o Tribunal incluiu diversas novidades que envolvem a inteligência artificial. São elas: proibição das *deepfakes;* obrigação de aviso sobre o uso de IA na propaganda eleitoral; restrição do emprego de robôs para intermediar contato com o eleitor (a campanha não pode simular diálogo com candidato ou qualquer outra pessoa); e respon-

9 Fonte: https://gizmodo.uol.com.br/video-joao-doria-provavelmente-fake/. Acessado em 10/10/2024.

10 Fonte: https://www.tse.jus.br/comunicacao/noticias/2020/Fevereiro/programa-minuto-da-checagem-explica-o-que-e-201cdeepfake201d. Acessado em 10/10/2024.

sabilização das *big techs* que não retirarem do ar, imediatamente, conteúdos com desinformação, discurso de ódio, ideologia nazista e fascista, além dos antidemocráticos, racistas e homofóbicos[11].

Por mais que tenhamos já algumas limitações implantadas pelo TSE em 2019, isso não livrou alguns candidatos, mais especialmente mulheres, de serem vítimas da pior espécie de *deepfake*, o *deepnude*: conteúdo falso de conotação erótica, criado a partir de imagens de rosto da pessoa, vinculadas a imagens em corpo nu de terceiro(a).

Tivemos várias candidatas no pleito eleitoral de 2024, concorrendo aos cargos de Prefeita ou Vereadora de seus municípios, que foram alvo de *deepnudes*, onde foram falsamente retratadas em vídeos pornográficos divulgados em redes sociais e grupos de WhatsApp, com o intuito de desmoralizá-las perante o eleitorado. A situação foi tão grave que este fato foi objeto de matéria jornalística divulgada pelo programa Fantástico, da Rede Globo[12], em 06/10/2024.

Tais vídeos procuravam simular relações sexuais protagonizadas por tais candidatas, em filmagens teoricamente "sigilosas" que teriam sido objeto de vazamento de informações. Obviamente que tais vídeos nunca existiram, foram criados a partir de gerações de imagens das candidatas, extraindo-se seus rostos de outros vídeos e aplicando-os em vídeos eróticos de terceiros já divulgados. É nítido que nesse contexto houve, contra tais candidatas, a violência política de gênero, onde por serem mulheres, foram objetificadas, em um contexto falso, com o objetivo maior de convencer o eleitorado a não votarem nelas, e impactando assim a sua

11 Fonte: https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes. Acessado em 10/10/2024.

12 Fonte: https://g1.globo.com/fantastico/noticia/2024/10/06/deep-nudes-fotos-e-videos-sao-manipulados-por-ia-para-produzir-conteudo-erotico.ghtml Acessado em: 14/10/2024.

honra, imagem e reputação; em um ato totalmente difamatório. Esse é um dos piores contextos do *deepfake*.

A inclusão de novas regras pelo TSE sobre o uso de inteligência artificial (IA) e tecnologias digitais na propaganda eleitoral, reflete o reconhecimento da importância dessas ferramentas no cenário político contemporâneo, mas também os riscos que elas podem representar.

A implementação dessas medidas reflete uma preocupação com a integridade do processo eleitoral em um mundo onde a tecnologia digital, especialmente a IA, pode ser usada tanto para aprimorar as campanhas quanto para distorcer a verdade. O principal objetivo é assegurar que o eleitor continue sendo o protagonista do processo eleitoral, tomando decisões informadas, sem ser manipulado por tecnologias que possam distorcer o processo democrático.

3. REGULAMENTAÇÃO DE *DEEPFAKES* NO CENÁRIO ELEITORAL

Embora o TSE tenha regulamentado o uso de *deepfakes* nas eleições, ainda não há uma Lei Federal específica que trate acerca dos *deepfakes* no Brasil de forma abrangente. No entanto, alguns projetos de lei têm sido propostos para regular essa questão em outras esferas.

3.1. PL 2630/2020 - Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet ("PL das Fake News")

Um dos principais projetos em tramitação é o PL 2630/2020[13], conhecido como "PL das Fake News", que busca criar uma regulamentação mais ampla para combater a desinformação online. Embora não seja focado exclusivamente em *deepfakes*, o projeto:

13 Fonte: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983&filename=PL%202630/2020.

- Inclui disposições que podem abranger o uso de *deepfakes* como uma forma de desinformação;
- Estabelece normas para plataformas digitais e redes sociais em relação à remoção de conteúdos falsos ou enganosos;
- Propõe a criação de mecanismos de transparência e responsabilização para as plataformas que falharem em combater a disseminação de conteúdos manipulados.

Esse projeto de lei ainda está em debate, e sua aprovação ou modificações ainda dependem do trâmite no Congresso Nacional.

3.2. Outros Projetos de Lei

Além do projeto descrito acima, há também outros projetos de lei com o objetivo de regulamentar o uso de tecnologias avançadas de manipulação de conteúdo, como os *deepfakes*[14]. Algumas propostas visam:

- Tipificar o uso malicioso de *deepfakes* como crime.
- Estabelecer sanções específicas para quem cria ou dissemina deepfakes que causem danos a indivíduos ou ao público.

4. CONCLUSÃO

No cenário atual, é imprescindível discutir novas tecnologias, especialmente a inteligência artificial e o *deepfake*, visto que essas inovações impactam nosso cotidiano e podem trazer uma série de riscos e danos.

No Brasil, apesar da alteração na Resolução nº 23.610/2019, há ainda uma lacuna legal em relação a outros contextos de uso dessa tecnologia, que pode ser preenchida com a aprovação de projetos de lei, como o PL 2630/2020. A regulamentação de *deepfakes* é essencial não só para proteger o processo eleitoral, mas também para garantir a proteção da privacidade e da imagem dos cidadãos e combater a

14 Fonte: https://www12.senado.leg.br/noticias/materias/2024/02/07/projetos-buscam-restringir-manipulacao-de-imagens-com-inteligencia-artificial.

desinformação em diversos níveis.

Embora a regulamentação atual esteja avançando, é fundamental destacar que existem outras legislações que podem ser utilizadas para proteger a pessoa retratada, tais como o Código Penal, o Código Civil e a Constituição Federal, além da LGPD – Lei Geral de Proteção de Dados Pessoais.

Entretanto, é importante reconhecer que a regulamentação completa de novas tecnologias não é viável, devido ao seu rápido avanço e à capacidade de indivíduos mal-intencionados de descobrir e explorar novas funcionalidades.

O desafio, no entanto, reside em equilibrar a proteção contra os abusos dessa tecnologia com a preservação da liberdade de expressão e a inovação tecnológica, além da criação de diretrizes e princípios, que possam ser aplicados para diversos casos.

A regulamentação do uso desse tipo de tecnologia caminha em conjunto com a regulação da própria IA no nosso país.

Esperamos que o debate para regulação da IA avance urgentemente, para que tenhamos diretrizes para limitarmos alguns pontos sensíveis e avançarmos tecnologicamente com segurança.

REDES SOCIAIS: SANÇÕES EM PERÍODO ELEITORAL

João Victor Barcellos Machado Correia[1]

1. INTRODUÇÃO

Com as recentes disrupções tecnológicas, as redes sociais instalaram um novo cenário na dinâmica da comunicação das informações[2]. Nesse tear, os indivíduos deixaram de ser meros receptores das informações e passaram a ser transmissores, criando novas correntes de pensamentos em um verdadeiro empoderamento social.

Ao analisar as redes sociais mais conhecidas no Brasil[3], como o WhatsApp, Facebook, YouTube, Instagram, TikTok e LinkedIn, vemos o papel crescente dos influenciadores digitais, seja em conteúdos curtos e simples como releituras ou *reacts*, seja em complexos como análises geopolíticas e afins em diferentes formatos.

Em realidade, as camadas de serviços e aplicações construídas sobre a internet empoderaram os indivíduos a ponto de eles terem o poder de "fazer a notícia". E vai além,

---

1 Advogado. Pesquisador de direito digital e municipal; autor do capítulo "Dadosfera (*datasphere*) e o problema do dado: novos espaços e problemas teóricos para o direito" no e-book do Legal Hackers Belo Horizonte, "Direito e tecnologia: discussões para o século XXI"; Bacharel em Direito pelo Centro Universitário Vale do Cricaré (UNIVC); e-mail: jvbmc11@gmail.com.

2 A informação aqui não está no sentido técnico da Ciência da Informação e de Dados. A informação aqui é expressão genérica para remeter a notícias, pensamentos, ideias, projetos e similares.

3 RD STATION. **Ranking: as redes sociais mais usadas no Brasil e no mundo em 2023, com insights, ferramentas e materiais.** Disponível em: https://www.rdstation.com/blog/marketing/redes-sociais-mais-usadas-no-brasil/. Acesso em 07 de out. de 2024.

é "poder de introduzir ou direcionar pensamentos" [4], podendo recair em desinformação ao "manipular a realidade e retirar a capacidade de discernir o real do irreal"[5].

E por ser algo tão relevante, a questão que surge é que as redes sociais são um palco eleitoral a ser disputado, com influência de perfis profissionais/comerciais dos candidatos e pessoais dos eleitores.

O ponto crítico é: é dever da plataforma fiscalizar seu próprio ambiente virtual, mantendo-o saudável aos seus consumidores, no entanto a plataforma não o pode fazer sem um verdadeiro procedimento administrativo para garantir o contraditório e ampla defesa em ações mais incisivas, ainda mais em período eleitoral.

O objetivo do presente artigo é apresentar um *draft* do tema sem esgotá-lo, visando apresentar uma nova perspectiva doutrinária com efeitos práticos, sem estar atrelado necessariamente a forma de aplicação atual pelo Tribunal Superior Eleitoral.

2. DEVIDO PROCEDIMENTO TECNORREGULACIONAL EM REDES SOCIAIS

Aquando se fala em aplicação de sanções[6] em redes sociais, não se discute sua impossibilidade, porém como fazê-lo sem ofender os direitos constitucionais, do consumidor, eleitorais, do titular de dados e outros.

---

4 MATTIOTI, Luise S.; BATISTA, Mayza Magalhães V. Novos canais de comunicação: democratização ou manipulação das informações. *In*: PINHEIRO, Patricia Peck. (Coord.). **Revista de Direito Digital**. Vol. 1, n. 1, 2019, pp.113-115.

5 TOFFOLI, José Antonio Dias. Fake News, desinformação e liberdade de expressão. *In*: ABBOUD, Georges; JÚNIOR, Nelson Nery; CAMPOS, Ricardo (Org.). **Fake News e Regulação**. 2. ed, 2020, p.20.

6 As sanções nada mais são que penalidades ao perfil, como redução de alcance de publicações, proibição de publicações, remoção de conteúdo, exclusão ou suspensão de conta e outras medidas.

Sobre o dever de fiscalização, conquanto aguarde manifestação do Supremo Tribunal Federal no Tema 987, o Ministro Dias Toffoli já se manifestou em artigo asseverando os termos da repercussão geral:

> […] à luz dos princípios constitucionais e da Lei nº 12.965/2014, a empresa provedora de aplicações de internet possui os deveres (i) de fiscalizar o conteúdo publicado nos seus domínios eletrônicos, (ii) de retirar do ar informações reputadas como ofensivas mediante simples notificação extrajudicial e (iii) de se responsabilizar legalmente pela veiculação do aludido conteúdo antes da análise pelo Poder Judiciário[7].

Nesse tear, cunhei a terminologia "devido procedimento tecnorregulacional" como *framework* teórico que engloba todos os problemas das plataformas digitais, incluindo aqueles "advindos diretamente da imposição de regras via código das novas tecnologias, permitindo um debate muito mais amplo para concretização de uma nova era de direitos humanos digitais por desenho e padrão"[8].

Em detalhamento, o conceito visa os mecanismos de decisão das plataformas em geral, sejam aqueles implícitos no código, como impossibilidade de fazer determinadas ações, como aqueles em que a plataforma se utiliza de funcionários verificadores de conteúdo.

Seja de um jeito ou doutro, há uma decisão na plataforma sem contraditório e ampla defesa por desenho e padrão, em alguns casos implícita e automática como o *shadowban*[9] do Instagram, que restringe o alcance das publi-

7 TOFFOLI, José Antonio Dias. Fake News, desinformação e liberdade de expressão. *In*: ABBOUD, Georges; JÚNIOR, Nelson Nery; CAMPOS, Ricardo (Org.). **Fake News e Regulação**. 2. ed, 2020, p.27.

8 CORREIA, João Victor Barcellos Machado Correia. **Do devido procedimento tecnorregulacional e transcedência dos bens em jogos on-line**. No prelo.

9 RD STATION. **Shadowban no Instagram: o que é, como evitar e como reverter a punição.** Disponível em: https://www.rdstation.com/blog/marketing/shadowban-no-instagram/. Acesso em 07 de out. de 2024.

cações do usuário sem qualquer aviso.

A exemplo, o *shadowban* pode ocorrer quando o usuário se utiliza de *hashtags* e expressões que em outras línguas podem ter cunho sexual, como o famoso "sextou", que o algoritmo pode "confundir" com "*sex to you"*.

Nota-se que é um procedimento que viola os direitos do consumidor e no período eleitoral pode configurar até crime.

Em se tratando do devido procedimento tecnorregulacional em redes sociais, indicam-se as seguintes melhorias de boas-práticas para aplicação de sanções aos usuários:

> **Direitos e Garantias Básicas:** presunção de inocência (constitucional e tecnológica – existe a possibilidade de um terceiro ter praticado o ato); oportunização do contraditório e ampla-defesa; fundamentação específica das decisões (sem justificativa genérica); transparência dos procedimentos e provas acusatórias (deve-se comprovar a suposta conduta desleal do usuário); direito à explicação e dever de transparência dos softwares automatizados; irretroatividade das punições; proporcionalidade das sanções; suspensão da conta do usuário como último recurso;
>
> **Melhorias no processo de julgamento:** estruturação de procedimento eletrônico para decisão; acessibilidade via PROCONs; preferência por julgamento não automatizado;
>
> **Melhorias na avaliação:** critério da gravidade e potencial resultado dos atos do usuário para fins de aplicação de sanções; mitigação das sanções de acordo com o índice de pessoalidade da conta do usuário; mitigação de sanções em contas de candidatos em período eleitoral.

Conquanto alguns critérios sejam autoexplicativos, imperioso não olvidar que a irretroatividade e proporcionalidade de sanções estão associadas a delimitação da plataforma de quais são as condutas desleais dos usuários, ocasião em que se deve avaliar as sanções proporcionais e até alterar a plataforma para que elas sejam aplicáveis.

Após isso, como é difícil garantir a vascularidade da

aplicação de todos esses critérios a todos os milhões ou bilhões de usuários, deve-se dar prioridade a sancionar as condutas desleais não somente mais graves, mas que possuem um risco de prejuízo maior pelo alcance do usuário e outros fatores. Essas são informações que somente a própria plataforma, controladora dos dados, pode avaliar com maior clareza e facilidade.

Cumpre referir que para aplicação das sanções faz diferença se o perfil é majoritariamente profissional ou pessoal. Um perfil pessoal pode ser considerado como pertencente a vida privada de seu usuário e, assim, é mais factível que uma sanção possa afetar sua honra; noutro lado, uma conta profissional ou comercial sancionada pode sofrer com lucros cessantes e, em período eleitoral, é crime impedir a propaganda pelo perfil do candidato.

É preciso entender que a necessidade de maturação da aplicação de boas-práticas pelas próprias plataformas é decorrente de que o conhecimento para julgar e avaliar o que é importante para decidir e agir "em sua maioria não se encontra no Estado", e sim nas próprias plataformas[10].

Nos termos expostos, a própria proporcionalidade e criação de sanções depende de estudo prévio a ser realizado pela plataforma. Todavia, como não se pode esperar esse tipo de *compliance*, é mais indicado o modelo da autorregulação regulada por meio da qual o Estado pode "gerar o conhecimento para decisão dentro de um procedimento preestabelecido"[11].

---

10 ABBOUD, George; CAMPOS, Ricardo. A autorregulação regulada como modelo do Direito proceduralizado: regulação de redes sociais e proceduralização. *In*: ABBOUD, Georges; JÚNIOR, Nelson Nery; CAMPOS, Ricardo (Org.). **Fake News e Regulação**. 2. ed, 2020, p.128.

11 ABBOUD, George; CAMPOS, Ricardo. A autorregulação regulada como modelo do Direito proceduralizado: regulação de redes sociais e proceduralização. *In*: ABBOUD, Georges; JÚNIOR, Nelson Nery; CAMPOS, Ricardo (Org.). **Fake News e Regulação**. 2. ed, 2020, p. 129.

Em outras palavras, o Estado deve criar um procedimento para que a plataforma acumule os conhecimentos para melhorar a eficácia da forma de sancionamento dos usuários das redes sociais, permitindo uma legislação definitiva posteriormente.

Na seara eleitoral, com as alterações do art. 9-D e ss. da Resolução n. 23.610/2019 do Tribunal Superior Eleitoral (TSE), houve aplicação de um modelo de autorregulação regulada em que as redes sociais deveriam garantir medidas de combate a fatos inverídicos, tendo que elaborar políticas, instrumentos de denúncia e ações corretivas[12].

3. DO PERFIL EM REDE SOCIAL

Como cediço, a conta do usuário em uma rede social tem o condão de não somente permitir novas interações com outros usuários, mas de digitalizar a própria imagem do usuário, isto é, da sua personalidade e permitir que ele interaja na comunidade virtual.

Noutros termos, a conta do usuário em rede social representa não somente ele na plataforma, mas é a exteriorização digital do seu "eu", isto é, da sua "ipseidade que difere o ser humano dos outros entes e entre seus próprios pares"[13].

Um maior grau de personalidade será exteriorizado na rede social de acordo com o que permite a plataforma e do desejo do próprio usuário em se expor a terceiros.

Dalém de dados pessoais até mesmo sensíveis, tais quais condições de saúde, opinião política, filiação sindical, dados biométricos, a plataforma pode permitir níveis de detalhamento e conexões que podem substituir grande parte da

12 BRASIL. **Resolução n. 23.610, de 18 de dezembro de 2019.** Dispõe sobre a propaganda eleitoral. Disponível em:< https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 07 out. 2024.

13 BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2019. p.99.

vivência social de alguns usuários.

Nesse sentido, quanto a natureza jurídica da relação entre usuários e plataforma, os usuários são consumidores e titulares de dados pessoais, sendo a plataforma fornecedora e controladora de dados.

Quanto a natureza jurídica consumerista da plataforma em relação aos usuários, a plataforma oferece a prestação de um serviço (art. 3, §2º, do CDC[14]), recebendo remuneração com comercialização dos dados dos usuários e doutras formas indiretas.

Assim, a conta do usuário é meio para acesso a esse serviço. Sobre a comercialização da conta, ao seu modo é possível considerá-la como produto, na medida em que é bem jurídico, com movimento próprio entre titulares, sem alteração da sua finalidade e substância.

Estabelecido isso, quanto as sanções, a legislação pátria é clara e imperativa quanto aos direitos assegurados aos usuários. Agora, no constante a atuação da plataforma de rede social para aplicar sanções, ela deve avaliar e priorizar a avaliação do ecossistema digital como um todo em seu espaço que cada vez mais é público, uma vitrine do eu digital para o mundo.

4. DAS SANÇÕES A PERFIS PESSOAIS

De seu turno, se um perfil tiver uso majoritariamente pessoal, utilizando o usuário os serviços da plataforma para interação com amigos e demais conexões, uma sanção deve levar em conta que a suspensão acarretaria retirar o indivíduo do convívio na sociedade digital.

Tais sanções potencialmente poderiam atingir os direitos constitucionais à vida privada, manifestação de

14 GRINOVER, Ada Pellegrini *et al*. **Código brasileiro de defesa do consumidor: comentado pelos autores do anteprojeto**.7.ed. Rio de Janeiro: Forense Universitária, 2001. p.21.

pensamento, liberdade de expressão e acesso à informação nos termos do art. 5, incisos IV, IX, X e XIV da Constituição Federal, *in verbis*:

> Art. 5: IV - é livre a manifestação do pensamento, sendo vedado o anonimato; IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;[15]

Cogente pontuar que um perfil pessoal pode ser considerado como pertencente a vida privada de seu usuário e, assim, é mais factível que uma sanção possa afetar sua honra.

Em época de eleição, uma sanção que proíba publicações, comentários ou acesso ao conteúdo da plataforma afeta diretamente a participação democrática do usuário, no que qualquer medida deve passar por um devido procedimento para evitar ou, ao menos, mitigar eventuais riscos de ofensa a honra e direitos constitucionais dos usuários, evitando condenações em indenização em danos extrapatrimoniais.

Para efeito de aplicação das Resoluções do TSE sobre desinformação, é vital reiterar os princípios do procedimento sancionatório, como a prova da acusação com garantia da integridade, autenticidade e veracidade.

5. DAS SANÇÕES A PERFIS PROFISSIONAIS

Noutro giro, mais gravoso seria uma sanção em face de uma conta profissional ou comercial sancionada pode sofrer com lucros cessantes pela queda em seu faturamento e,

15 NERY, Nelson Júnior; NERY, Maria de Andrade. **Constituição federal comentada e legislação comentada**. 3. ed. São Paulo: Revista dos Tribunais, 2012. pp. 213-214.

em período eleitoral, se a conta do usuário tiver por finalidade publicar propaganda de candidato, pode configurar o crime dos arts. 331 e 332 do Código Eleitoral, a saber:

> Art. 331. Inutilizar, alterar ou perturbar meio de propaganda devidamente empregado: Pena - detenção até seis meses ou pagamento de 90 a 120 dias-multa.
>
> Art. 332. Impedir o exercício de propaganda: Pena - detenção até seis meses e pagamento de 30 a 60 dias-multa.[16]

Em realidade, no quesito da sanção ao perfil de rede social de candidato eleitoral, é preciso elucidar que o próprio perfil é ferramenta da propaganda, seja em interações diretas com terceiros e potenciais eleitores em seus perfis, com curtidas, comentários e outras interações, seja através de publicações na própria conta do candidato.

Nessa linha de intelecção, qualquer sanção que afete o funcionamento costumeiro do perfil pode ser considerada nos referidos artigos, mesmo que de modo mais sutil.

Essa afetação da propaganda por meio do perfil em rede social dependerá que a falha na prestação do serviço pela plataforma gere a quebra da expectativa do que se poderia esperar do perfil em condições normais, como disciplina o art. 14 do Código de Defesa do Consumidor:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam;

16 BRASIL. **Lei 4.737, de 15 de julho de 1965**. Institui o Código Eleitoral. Disponível em:<https://www.planalto.gov.br/ccivil_03/leis/l4737compilado.htm>. Acesso em 07 de out. de 2024.

> III - a época em que foi fornecido.[17]

Em razão disso, não é indicado que a plataforma altere suas políticas e mecanismos de funcionamento durante o período eleitoral para não prejudicar as eleições por meio de sua plataforma.

De mais a mais, se a rede social tiver um viés discriminatório em relação ao candidato, com sanções imotivadas aos perfis, também é possível o enquadramento como prática abusiva nos termos do art. 39, incisos II e IX, do Código de Defesa do Consumidor:

> Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: II - recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque, e, ainda, de conformidade com os usos e costumes; IX - recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais;[18]

Noutra banda, se a rede social estiver em conluio com algum candidato para prejudicar adversário político, é possível mover ação contra o referido candidato por abuso de poder.

De toda sorte, havendo uma sanção imotivada da plataforma a um perfil de um candidato, dalém dos danos materiais e morais pelos prejuízos causados, caberá o crime eleitoral.

---

17 BRASIL. **Lei n. 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em:<https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em 07 de out. de 2024.

18 BRASIL. **Lei n. 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em:<https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em 07 de out. de 2024.

6. CONSIDERAÇÕES FINAIS

No constante as sanções de qualquer tipo a perfis em rede social, a plataforma digital deve garantir a aplicação de um devido procedimento interno, o "devido procedimento tecnorregulacional", com princípios próprios, buscando sempre a melhor aplicação do direito pátrio.

Nessa seara, se fora da eleição já se deve ter cautela, em período eleitoral mais ainda. Por um lado, porque muitos eleitores se informam e participam das eleições pelas redes sociais. Em outra seara, os candidatos dependem do funcionamento costumeiro da rede social para propagar suas campanhas.

Curioso que na prestação do serviço das redes sociais, apesar da plataforma ser privada, submete-se a legislação pátria e cria um espaço de debate público, de todos, em que deve prevalecer a vontade da lei, sem discriminações.

Com efeito, as sanções sem provação judicial não são indicadas em período eleitoral pelo risco de os prejuízos superarem eventuais benefícios das medidas. Deve-se levar em consideração que, nas eleições, os atores políticos estão atentos e as decisões judiciais são céleres, o que reduz a potencialidade nociva de alguns atos.

Nessa toada, surge a indagação como a rede social deve se comportar quando decisões judiciais de diferentes países forem conflitantes. A exemplo, se um certo país requisitar a remoção de um perfil a nível global e outro sua manutenção. Dalém de questões econômicas, vê-se por adequado que o atendimento da solicitação governamental deve ser a nível local, sem atingir o funcionamento do perfil em outras localidades.

De seu plano, o combate a desinformação, cancelamentos e outros fenômenos nocivos são um desafio a ser enfrentado. Para isso, recomenda-se o uso da autorregulação regulada. Nesse modelo, o Estado cria um procedimento para que a rede social possa gerar o conhecimento necessá-

rio para solucionar ou minimizar o problema.

De um jeito ou outro, um fator concreto é que essa adequação das redes sociais depende de investimento, penalidades estatais e criação de modelos regulatórios para incentivar a coesão e harmonia desse importante espaço público virtual.

REFERÊNCIAS

ABBOUD, George; CAMPOS, Ricardo. A autorregulação regulada como modelo do Direito proceduralizado: regulação de redes sociais e proceduralização. *In*: ABBOUD, Georges; JÚNIOR, Nelson Nery; CAMPOS, Ricardo (Org.). Fake News e Regulação. 2. ed, 2020, pp. 121-141.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2019.

BRASIL. Lei 4.737, de 15 de julho de 1965. Institui o Código Eleitoral. Disponível em:< https://www.planalto.gov.br/ccivil_03/leis/l4737compilado.htm>. Acesso em 07 de out. de 2024.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em 07 de out. de 2024.

BRASIL. Resolução n. 23.610, de 18 de dezembro de 2019. Dispõe sobre a propaganda eleitoral. Disponível em:<https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 07 out. 2024.

CORREIA, João Victor Barcellos Machado Correia. Do devido procedimento tecnorregulacional e transcendência dos bens em jogos on-line. No prelo.

GRINOVER, Ada Pellegrini *et al*. Código brasileiro de defesa do consumidor: comentado pelos autores do anteprojeto.7.ed. Rio de Janeiro: Forense Universitária, 2001.

MATTIOTI, Luise S.; BATISTA, Mayza Magalhães V. Novos canais de comunicação: democratização ou manipulação das informações. *In*: PINHEIRO, Patricia Peck. (Coord.). Revista de Direito Digital. Vol. 1, n. 1, 2019, pp. 109-119.

NERY, Nelson Júnior; NERY, Maria de Andrade. Constituição federal comentada e legislação comentada. 3. ed. São Paulo: Revista dos Tribunais, 2012.

RD STATION. Ranking: as redes sociais mais usadas no Brasil e no mundo em 2023, com insights, ferramentas e materiais. Disponível em: https://www.rdstation.com/blog/marketing/redes-sociais-mais-usadas-no-brasil/. Acesso em 07 de out. de 2024.

RD STATION. Shadowban no Instagram: o que é, como evitar e como reverter a punição. Disponível em: https://www.rdstation.com/blog/marketing/shadowban-no-instagram/. Acesso em 07 de out. de 2024.

TOFFOLI, José Antonio Dias. Fake News, desinformação e liberdade de expressão. *In*: ABBOUD, Georges; JÚNIOR, Nelson Nery; CAMPOS, Ricardo (Org.). Fake News e Regulação. 2. ed, 2020, pp. 17-28.

DEEPFAKES E MANIPULAÇÃO ELEITORAL: RISCOS DE CONTEÚDOS AUDIOVISUAIS MANIPULDOS NO CONTEXTO ELEITORAL

Letícia Zampieri[1]

1. INTRODUÇÃO

A Era Digital, ou conhecida por alguns como a Revolução Industrial 4.0, marcada pela crescente sofisticação da Inteligência Artificial (IA), trouxe consigo um novo desafio para a democracia: os *deepfakes*.

As manipulações digitais altamente realistas, capazes de criar vídeos e áudios falsos de qualquer pessoa, pública ou não, representam uma ameaça significativa à integridade dos cidadãos, não sendo diferente em campanhas eleitorais.

Ao simular declarações e ações falsas de candidatos, a tecnologia tem alto poder de conseguir influenciar com facilidade a opinião pública.

O uso indevido e manipulado dessa ferramenta proporciona desinformação e *fakes news*, trazendo efeitos nefastos para o funcionamento do sistema eleitoral

1 Advogada formada em 2015 pela FMU/SP. Especialista em Ética dos Dados, Inteligência Artificial e Direito Digital e *Compliance*. DPO (Data Protection Officer) certificada pela ADAPTNOW (ISO 27001 - PDPP - PDPF). Pós-graduada em Direito Digital e *Compliance* pela IBMEC/Damásio Educacional; Pós-graduada em Direito Digital pela Escola Superior da Advocacia. Especialista em *Risk and Cyber Insurance* pela Escola Nacional de Seguros. Especialista em IA e Direito pela PUC/RJ. Membro do Comitê Público da Associação Nacional dos profissionais de Privacidade de Dados - ANPPD. Membro efetivo das Comissões de Direito Digital Tecnologia e Inteligência Artificial e Direito Securitário da OAB/SP- 116ª Subseção Jabaquara/Saúde. Membro Efetivo da Comissão Especial de Privacidade e Proteção de Dados da OAB/SP. Membro da Associação Nacional de Advogados do Direito Digital – ANADD. Contato: <leticia.zampieri@lzadvocacia.adv.br>

democrático de direito e proporciona a extensão da polarização política.

O termo *deepfake* começou a ganhar notoriedade em meados de 2017. Mas afinal, do que se trata? Quais são os impactos para a sociedade e qual a relação com o contexto eleitoral?

O presente artigo busca analisar quais são os impactos das *deepfakes* no cenário político contemporâneo, discutindo as implicações para a democracia e propondo medidas para mitigar seus efeitos. Além disso, traz os possíveis impactos no contexto eleitoral, demonstrando aspectos práticos e jurídicos pertinentes ao tema, ante os avanços tecnológicos diante do cenário da polarização política na era das *fakes news*.

2. O QUE SÃO E QUAL A FINALIDADE DA DEEPFAKE?

O primeiro passo para entendermos "o que é *deepfake"*. A palavra é uma combinação dos termos "*deep learning*" (aprendizado profundo) e "*fake news*" (falsas notícias).

Segundo Lan Goodfellow, Bengio e Courville (2016, p.483), é uma evolução das metodologias de aperfeiçoamento de Inteligência Artificial ("IA"), que deriva do *machine learning* ("ML"), também conhecido como aprendizado da máquina.

Analisando superficialmente, *machine learning* é subcampos da IA que desenvolve máquinas capazes de aprender sem que sejam explicitamente programadas. De outro lado, *deep learning* é o subcampo de *machine learning* que simula o jeito como os seres humanos adquirem certas formas de conhecimento, atuando principalmente com dados no estruturados, ou seja, dados que não possuem nenhum modelo definido e nem uma ordem, como por exemplo: arquivos de texto e vídeo, e-mails e imagens.

Os modelos de *deep learning* são treinados para

classificar e reconhecer padrões, além de serem capazes de descrever imagens e transcrever arquivos de áudio, funcionando a partir de redes neurais, simulando, portanto, o cérebro humano.

Para a realidade da sociedade, esse assunto pode parecer muito atual, porém o conceito surgiu em 2017, ou seja, 07 (sete) anos atrás, sendo a origem por meio de um usuário da plataforma Reddit (rede social), de codinome *deepfakes*, que utilizou ferramentas de IA e aprendizado de máquina para criar um algoritmo, com intuito de treinar uma rede neural com o objetivo de mapear o rosto de uma pessoa no corpo de outra.

Além disso, a Lei de IA da União Europeia, recentemente publicada, dispõe uma definição sobre *deepfakes* sendo:

> uma imagem ou conteúdo de áudio ou vídeo gerado ou manipulado com Inteligência Artificial que se assemelha a pessoas, objetos, locais ou outras entidades ou eventos reais existentes que se aparentam falsamente autêntico ou verídico a uma pessoa (art. 3º, "60").

No entanto, com o avanço tecnológico os processos estão cada vez mais aperfeiçoados, gerando um alerta vermelho de preocupação vez que são ferramentas que podem causar grandes prejuízos, principalmente para a vítima que teve sua imagem vinculada com conteúdo não realista; inclusive com a facilidade de propagação e viralização de conteúdos por meio das redes sociais.

A decisão de compartilhar *deepfakes* é intencionalmente projetada para manipular a opinião pública, alimentando narrativas que reforça preconceitos e desconfiança em relação a sociedade, no contexto eleitoral, com objetivo de desestabilizar o debate público e minar a confiança nas instituições democráticas.

3. DESINFORMAÇÃO E PROPAGAÇÃO DE NOTÍCIAS FALSAS

Afinal, como os *deepfakes* podem ser utilizados para disseminar informações falsas e manipular a opinião pública?

Com a explosão das redes sociais, a desinformação tomou conta do cenário na mesma intensidade. Reflita: quantos conteúdos você leitor recebe de candidatos políticos e não possui uma certeza imediata se as informações são verdadeiras ou falsas/inventadas?

O Tribunal Superior Eleitoral (TSE), no Plano Estratégico das Eleições 2022, criou dentro do Programa de Enfrentamento à Desinformação[2], o "conceito guarda-chuva, que sintetiza os diferentes conteúdos relacionados aos contextos de desordem informacional e manipulação informacional".

No âmbito do presente programa, é considerado "potencial desinformação" qualquer conteúdo "falso, equivocado, enganoso, impreciso, manipulado, fabricado, fraudulento, ilícito ou odioso", além das informações fora de contexto, independentemente do formato, do canal de veiculação ou da intenção do agente.

Segundo estudo do *Massachussetts Institute of Technology* (MIT) em 2018, os conteúdos mentirosos possuem 70% (setenta por cento) mais chance de serem compartilhados como se fossem verdadeiros, ou seja, esse tipo de conteúdo viraliza mais fácil que um conteúdo verídico, em decorrência de serem normalmente conteúdos que trazem algum choque à sociedade e acabam sendo compartilhados em massa com o auxílio das diversas redes sociais disponíveis.

O poder das notícias falsas é imensurável e preocupante. Inclusive, dentro do cenário político, não tem como

2 Programa de Enfrentamento à Desinformação. Disponível em <https://www.justicaeleitoral.jus.br/desinformacao/>

não citarmos o ocorrido nas eleições presidenciais dos Estados Unidos, em 2016. Nesse fato histórico, com o auxílio de uma assessoria política – que se declarou culpada publicamente– realizou a utilização indevida de mais de 87 milhões de usuários sem o consentimento dos mesmos para coletar informações e propagar desinformações.

Nessa época ainda, o *BuzzFeed* observou que no período anterior aos três últimos meses da campanha do candidato, na época as eleições presidenciais norte americana, a performance do conteúdo dos principais veículos superou as falsas notícias. No entanto, à medida que a eleição se aproximava, o envolvimento com conteúdos falsos na rede social *Facebook* disparou e ultrapassou o conteúdo das principais fontes de notícias.

As *deepfakes*, conforme tratamos, desde as eleições presidenciais dos Estados Unidos em 2016 evoluíram e, recentemente, outra notícia se espalhou de um candidato que usou a *deepfake* de uma cantora globalmente conhecida para conquistar os seus eleitores, com intuito de fomentar a desinformação nas redes sociais durante a campanha eleitoral. As informações são do The Guardian[3].

Na América do Sul, tivemos nas eleições da Argentina, em 2023, uma produção em grande escala de propagandas com a adoção de computação gráfica e outras ferramentas realísticas ou fantasiosamente destinadas a gerar emoções diversas ao que seria se fosse real.

Na Europa, o processo eleitoral na Polônia, no mesmo período em 2023, também foi marcado pela adulteração de um vídeo para disparar intencionalmente medo em torno das supostas ameaças de bomba às estações que iriam ocorrer os votos, e assim gerar medo e desistências da população para votar.

3 "Trump posts deepfakes of Swift, Harris and Musk in effor to shore up support". Disponível em: <https://www.theguardian.com/us-news/article/2024/aug/19/trump-ai-swift-harris-musk-deepfake-images>

4. CONTEXTO ELEITORAL NO BRASIL

As eleições gerais no Brasil em 2022 foram marcadas pelo combate às notícias falsas, conhecidas como *Fake News*. Para o pleito municipal de 2024, o grande desafio será o enfretamento contra o uso indevido de ferramentas de IA e *deepfakes* nas campanhas eleitorais.

No cenário eleitoral brasileiro, com os aprimoramentos na resolução da propaganda, as ***deepfakes*** estão proibidas, seja para promover candidatos ou atacar adversários por meio de informações negativas.

No entanto, o TSE não proibiu o uso de Inteligência Artificial para criações, com a condicionante de que esta não seja para proporcionar desinformação e induzir o eleitor ao engano. Além disso, todo conteúdo criado pela IA, foi determinado a identificação por meio de marca d'água, rótulo, não isentando a responsabilidade de cada criador.

Recentemente, no dia 30.09.2024[4], a própria Justiça Eleitoral removeu publicações irregulares criadas com auxílio de IA, e *deepfakes*, e ainda propagadas com o teor de cunho sexual. Inclusive, já houve ao menos cinco decisões considerando o uso irregular da tecnologia que acarretou na remoção do conteúdo ou mesmo de perfis, seguindo a resolução do TSE, aprovada em fevereiro que proibiu o uso de *deepfakes*.

O tema de IA generativa [5]vem ganhando cada vez mais espaço em campanhas político-eleitorais. Analisando os impactos não benignos, possuem claramente o potencial de forte aliada para o engajamento dos eleitores, porém, com

4 "Justiça Eleitoral remove publicações irregulares com IA, e 'deepfakes' de teor sexual não investigado. Disponível em < https://oglobo.globo.com/politica/noticia/2024/09/30/justica-eleitoral-remove-publicacoes-irregulares-com-ia-e-deepfakes--de-teor-sexual-sao-investigados.ghtml>

5 A inteligência artificial generativa (IA generativa) é um tipo de IA que pode criar novos conteúdos e ideias, incluindo conversas, histórias, imagens, vídeos e músicas.

a perspectiva negativa, ou seja, o lado obscuro poderá amplificar a polarização política existente, por exemplo, ao introduzir ameaças (como ocorreu na Polônia em 2023), gerar desinformação de forma incontrolável, podendo inclusive facilitar as fraudes, dentre outras consequências possíveis.

No Brasil não foi diferente nas eleições dos anos de 2018 e em 2022, considerando que houve diversos casos envolvendo polêmica com o uso de tecnologia com viés de desinformação, prejudicando a sociedade. Não restam dúvidas que a desinformação no processo eleitoral brasileiro é a realidade presente que somente se intensifica e se potencializa com a rápida evolução das IAs generativas, ainda que haja uma privação do uso da tecnologia.

Apesar de não ter uma legislação específica sobre Inteligência Artificial no Brasil, o TSE estabeleceu, conforme já citamos, regras específicas para o uso da IA na criação e propagação de conteúdo durante o período eleitoral, por meio da Resolução 23.610/2019, e sua subsequente alteração pela Resolução 23.732/2024.

Dessa forma, não há outra saída que não seja os órgãos responsáveis realizarem a vigilância devida. O TSE adotando tais diretrizes demonstra um compromisso significativo com a luta contra a desinformação e a proteção do processo democrático dessas ameaças digitais.

Por fim, não podemos isolar a importância do papel que a sociedade possui, vez que é primordial que os cidadãos brasileiros deixem de lado a polarização política, devendo estes realizarem somente o compartilhamento após confirmação de que o conteúdo é verdadeiro, afinal a tecnologia, para algumas pessoas, pode parecer até traiçoeira, porém sendo bem manipulada proporciona resultados e experiências diferenciadas sendo acessório à capacidade humana.

5. A ESPADA DE DOIS LAMES DA CRIMINALIZAÇÃO DAS FAKES NEWS

A internet, no contexto da Era Digital, é conhecida erroneamente como "terra sei lei", já que diversos indivíduos promovem conteúdo e compartilham postagens que violam diversos direitos, realizando prática de crime, sem ter conhecimento.

A Constituição Federal Brasileira dispõe de diversos direitos fundamentais, dentre eles a livre expressão, liberdade de imprensa e o direito à informação.

O artigo 5º, IX da Constituição Federal, assegura nos seguintes termos: *"é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença".*

O conceito de liberdade de expressão, portanto, pode ser definido como possibilidade de cada indivíduo expressar e manifestar sua opinião própria sem imposição de restrição perante as autoridades, ou seja, como temos conhecimento, sendo uma segurança para restringir a censura, dado que o Brasil é um Estado Democrático de Direito.

Nessa vertente, muitos cidadãos eleitores acreditam que compartilhando notícias inverídicas não estão ferindo nenhum direito, pois se "protegem" sob a justificativa de que estão exercendo direito à liberdade de expressão. No entanto, esse ponto merece extrema atenção considerando que há, inegavelmente, violações de diversos outros direitos, inclusive podendo ser considerado CRIME.

O Código Eleitoral brasileiro proíbe expressamente qualquer pessoa divulgar, na propaganda eleitoral ou durante o período da campanha, fatos inverídicos em relação a partidos políticos ou candidatos.

Tal disposição encontra-se no art. 323[6] do Código

6 **Art. 323.** Divulgar, na propaganda eleitoral ou durante período de campanha

Eleitoral, incluído pela Lei nº 14.192, de 2021.

Conforme o artigo supracitado, a pena para o responsável pela prática dessa conduta ilegal é de detenção de dois meses a um ano, ou o pagamento de 120 a 150 dias-multa.

Segundo uma pesquisa realizada pelo Instituto Locomotiva, cerca de 90% (noventa por cento) da população brasileira admitiu ter acreditado em conteúdos falsos. Conforme o levantamento, oito em dez brasileiros já deu credibilidade a fake News.

Ainda nesse mesmo estudo, 63% (sessenta e três por cento) são relacionados a propostas em campanhas eleitorais.

Analisando os números, percebe-se a extensão e causa evidentemente preocupação das consequências, algumas inclusive podendo ser irreversíveis, vez que se atrelado a imagem, ao ter o direito da personalidade ferido, poderá demorar um grande tempo para se recuperar.

A *Fake News,* conforme dispõe o Código Penal Brasileiro, pode ser enquadrada como crime contra à honra, como por exemplo, Injúria e Calúnia.

Nesse sentido, ainda que não haja uma legislação específica para *Fake News*, a Justiça brasileira, acompanhando os assuntos relacionados e entendendo das consequências graves geradas, não teve outra escolha que não fosse indicar dentro da legislação específica e também por meio de Reso-

---

eleitoral, fatos que sabe inverídicos em relação a partidos ou a candidatos e capazes de exercer influência perante o eleitorado: (Redação dada pela Lei nº 14.192, de 2021)
Pena - detenção de dois meses a um ano, ou pagamento de 120 a 150 dias-multa.
Parágrafo único. Revogado. (Redação dada pela Lei nº 14.192, de 2021)

§ 1º Nas mesmas penas incorre quem produz, oferece ou vende vídeo com conteúdo inverídico acerca de partidos ou candidatos. (Incluído pela Lei nº 14.192, de 2021)
§ 2º Aumenta-se a pena de 1/3 (um terço) até metade se o crime: (Incluído pela Lei nº 14.192, de 2021)
I - é cometido por meio da imprensa, rádio ou televisão, ou por meio da internet ou de rede social, ou é transmitido em tempo real; (Incluído pela Lei nº 14.192, de 2021)
II - envolve menosprezo ou discriminação à condição de mulher ou à sua cor, raça ou etnia. (Incluído pela Lei nº 14.192, de 2021).

luções (TSE), além da criação de programas de combate à desinformação como já vimos.

Esse capítulo é um tema extenso e proporciona um debate crucial sobre o futuro da democracia e da sociedade informacional, vez que conforme já exposto, temos que considerar a revolução inclusive da liberdade de expressão na Era Digital, demonstrando os riscos que devem ser mitigados a fim de evitar a associação do direito fundamental com a desinformação, já que são absolutamente opostos.

6. CONSIDERAÇÕES FINAIS

Após breve análise sobre o tema, muitos questionam sobre permitir ou proibir o desenvolvimento e o consequente uso das IAs generativas, considerando todos os impactos possíveis, principalmente os negativos que obviamente são os mais preocupantes.

A crescente sofisticação das IAs generativas desafia nossa capacidade de distinguir o real do falso. A disseminação de notícias falsas e a manipulação da opinião pública representam sérios riscos para a democracia e a sociedade como um todo. É fundamental que tanto indivíduos quanto instituições estejam preparados para enfrentar esses desafios.

A obrigatoriedade de identificar o conteúdo gerado por IA, por meio de selos ou outros mecanismos, é um passo importante para aumentar a transparência e permitir que os usuários avaliem a credibilidade das informações. No entanto, a implementação dessa medida exige um debate cuidadoso sobre sua eficácia e os possíveis impactos na liberdade de expressão.

No que concerne as responsabilidades de combate à desinformação e o uso consciente de IA no contexto eleitoral, não se limita somente aos partidos, federações e candidatos(as), sendo aplicada também aos provedores de internet, uma vez que as plataformas são obrigadas a remover postagens falsas ou com informações gravemente descon-

textualizadas de forma imediata e direta.

Aos provedores da internet, conforme decisão do TSE, foi dado, ainda que indiretamente, uma autonomia para poderem tomar as respectivas decisões sendo desnecessário uma prévia decisão judicial autorizando, porém promove uma responsabilidade significante.

É preciso investir em educação digital, promover o pensamento crítico e desenvolver ferramentas tecnológicas para detectar e neutralizar a desinformação.

A regulamentação das IAs generativas é um tema urgente que exige uma abordagem equilibrada, capaz de promover a inovação sem comprometer os direitos fundamentais. É necessário um diálogo constante entre governos, empresas de tecnologia, pesquisadores e a sociedade civil para construir um futuro no qual a inteligência artificial seja utilizada para o bem comum, e tendo claro, uma segurança jurídica para o uso.

REFERÊNCIAS

BERINATO, Scott. Business in the Age of Computational Propaganda and Deep Fakes. 28 jul.2018. Disponível em: <https://hbr.org/2018/07/business-in-the-age-of-computational-propaganda-and-deep-fakes> Acesso em 01 de outubro de 2024.

BITTAR, Carlos Alberto. Os direitos da personalidade. 7. ed. Rio de Janeiro: Forense Universitária, 2008.

BLEISCH, N. David. Deepfakes and American Elections. 06 mai.2024, Disponível em: <https://www.americanbar.org/groups/public_interest/election_law/american-democracy/resources/deepfakes-american-elections/>

BRAGA, Renê Morais da Costa. A indústria da fake news e o discurso de ódio. In: PEREIRA, Rodolfo Viana (Org.). Direitos políticos, liberdade de expressão e discurso de ódio:

volume I. 2018.

DEEPMIND. SynthID: identifying AI-generated content with SynthID. 2023. Disponível em: https://deepmind.google/discover/blog/identifying-ai-generated-images-with-synthid/>. Acesso em 28 de setembro de 2024.

DURÃES, Uesley. Novo estágio das fake news: deepfake vira arma de campanha na Argentina. Uol, 18 nov. 2023. Disponível em: <https://noticias.uol.com.br/internacional/ultimas-noticias/2023/11/18/novo-estagio-das-fake-news-deepfake-vira-arma de-campanha-na-argentina.htm> Acesso em 28 de setembro de 2024.

FIGUEIREDO, Janaína. Campanha presidencial na Argentina usa inteligência artificial em grande escala. O Globo, 14 nov. 2023. Disponível em: <https://oglobo.globo.com/mundo/noticia/2023/11/14/campanha-presidencial-na-argentina-usa-ia-em-grande escala.ghtml>. Acesso em 28 de setembro de 2024.

JORNAL DA USP. Relatório da OCDE mostra que brasileiros são os piores em identificar notícias falsas. Disponível em: < https://jornal.usp.br/radio-usp/relatorio-da-ocde-mostra-que-brasileiros-sao-os-piores-em-identificar-noticias-falsas/> Acesso em 30 de setembro de 2024.

MELLO, Daniel. Quase 90% dos brasileiros admitem ter acreditado em fake News. Agência Brasil, 01 de abr.2024. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2024-04/quase-90-dos-brasileiros-admitem-ter-acreditado-em-fake-news> Acesso em 25 de setembro de 2024.

MIT TECHNOLOGY REVIEW BRASIL. O Pioneiro em Inteligência Artificial (IA) Geoff Hinton afirma: "O *depp learning* será capaz de fazer tudo". 04 dez.2020. Disponível em: < O pioneiro em Inteligência Artificial (IA), Geoff Hinton afirma: "O *deep learning* será capaz de fazer tudo" - MIT

Technology Review (mittechreview.com.br)> Acesso em 01 de outubro de 2024.

MPF. Deepfake e inteligência artificial: saiba o que pode e o que é proibido nas campanhas eleitorais. Disponível em: <https://www.mpf.mp.br/pgr/noticias-pgr2/2024/deepfake-e-inteligencia-artificial-saiba-o-que-pode-e-o-que-e-proibido-nas-campanhas-eleitorais>. Acesso em 30 de setembro de 2024.

NASCIMENTO, OLIVEIRA. Ingrid, Cristina. Deepfake nas eleições e a importância da proteção de dados. 02 de fev.2024. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/401249/deepfake-nas-eleicoes-e-a-importancia-da-protecao-de-dados> Acesso em 01 de outubro de 2024.

O GLOBO. Justiça Eleitoral remove publicações irregulares com IA, e deepfakes de teor sexual são investigados". O globo, 30 de set de 2024. Disponível em: <https://oglobo.globo.com/politica/noticia/2024/09/30/justica-eleitoral-remove-publicacoes-irregulares-com-ia-e-deepfakes-de-teor-sexual-sao-investigados.ghtml> Acesso em 30 de setembro de 2024.

PUCPR. A diferença entre machine learning e deep learning. disponível em: <https://posdigital.pucpr.br/blog/machine-learning-deep-learning>. Acesso em 28 de setembro de 2024.

TRIBUNAL SUPERIOR ELEITORAL. Programa de Enfrentamento à Desinformação do TSE tem mais de 150 parcerias. Disponível em <https://www.tse.jus.br/comunicacao/noticias/2022/Julho/programa-de-enfrentamento-a-desinformacao-do-tse-tem-mais-de-150-parcerias-659181> Acesso em 30 de setembro de 2024.

TRIBUNAL SUPERIOR ELEITORAL. TSE proíbe uso de

inteligência artificial para criar e propagar conteúdos falsos nas eleições. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes>. Acesso em 30 de setembro de 2024.

TRIBUNAL SUPERIOR ELEITORAL. TSE Proíbe uso de Inteligência Artificial para Criar e Propagar conteúdos falsos nas eleições. 28 de fev.2024. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes> Acesso em 01 de outubro de 2024.

URIBE, Gustavo. Pesquisa aponta aumento da polarização e queda de civilidade no Brasil. CNN Brasil, 18 abr.2023. Disponível em: <https://www.cnnbrasil.com.br/politica/pesquisa-aponta-aumento-da-polarizacao-e-queda-da-civilidade-no-brasil/> Acesso em 23 de setembro de 2024.

LGPD NAS ELEIÇÕES: A INDICAÇÃO DO ENCARREGADO PELA PROTEÇÃO DE DADOS PESSOAIS (DPO) COMO ELO NECESSÁRIO ENTRE CANDIDATURAS, ELEITORES E AUTORIDADES

Newton Moraes[1]

1. INTRODUÇÃO

A democracia se fortalece quando a cidadania confia nas instituições e participam ativamente dos processos políticos. Nesse cenário, a exemplo do que ocorre nas demais searas como a consumerista, a proteção de dados pessoais é parte integrante dessa confiança, garantindo que a informação seja utilizada para promover o bem comum e não para manipulação ou controle indevido, o que somente ocorrerá se as candidaturas cumprirem os preceitos normativos, notadamente indicando encarregado pela proteção de dados pessoais efetivamente competente e dedicado a garantir a densificação dos direitos dos titulares.

Tal situação, embora não seja nova, porquanto o tratamento de dados pessoais é a própria essência de uma campanha política, uma vez que permite maior assertividade entre os investimentos na divulgação dos candidatos e a recepção das informações pelos eleitores, como forma legítima de influenciar no exercício do direito de escolha, a era digital e informacional instrumentaliza uma revolução na forma como a informação é produzida, compartilhada e consumida.

1 DPO de Porto Alegre, RS, Mestre em Direito e especialista em Direito Público pela FMP/RS, advogado licenciado, professor de Direito Constitucional na Faculdade de Direito da UNIFTEC, palestrante em cursos de pós-graduação em Direito Digital e disciplinas da LGPD. Autor de artigos.

No contexto democrático, especialmente durante os processos eleitorais, essa transformação tem implicações profundas na relação entre eleitores, partidos políticos e candidatos, percebendo-se que a proteção de dados pessoais emergiu como um direito fundamental, reconhecido constitucionalmente em diversos países, incluindo o Brasil. A garantia desse direito é essencial para a preservação da cidadania e da democracia, uma vez que o uso indevido de informações pessoais pode comprometer a integridade do processo eleitoral e a liberdade de escolha dos eleitores.

Este ensaio, portanto, busca analisar o direito fundamental à proteção de dados pessoais no contexto das eleições, explorando os aspectos que permeiam o tema. Para tanto, com breve passeio pela normativa brasileira, com ênfase à Lei Geral de Proteção de Dados (LGPD), Resoluções do Tribunal Superior Eleitoral (TSE) referentes às eleições de 2024 em sumário paralelo com normas de autoridades de proteção de dados pessoais do Brasil e de outros países, pretendendo demonstrar como a proteção de dados pessoais é intrinsecamente ligada aos princípios democráticos e à efetivação da cidadania, com relevo à indicação do DPO, mandatória nos colégios eleitorais com mais de 200 mil eleitores, o que será o caso das eleições gerais de 2026, quando os brasileiros vão eleger deputados estaduais, deputados federais, senadores, governadores e presidente da república, ou seja, todas as candidaturas disputarão mais de 200 mil eleitores.

Isso porque, é inegável o liame indissolúvel entre o tratamento de dados pessoais, notadamente no meio digital, como parte essencial da vida democrática, demonstrado pela capacidade dos candidatos de comunicar ideias, difundir ideologias, e, com isso, conquistar os eleitores.

Todavia, assume, também, cada vez mais relevo a conquista da confiança dos eleitores que, na condição de titulares dos dados pessoais serão influenciados, também, pela integridade no uso de seus dados pessoais e no pro-

cesso eleitoral, valendo ressaltar que a propaganda eleitoral irregular pode implicar severas sanções aos candidatos que descumprirem as normas e violarem os direitos dos titulares, como, ao que se tem notícia até a finalização do presente texto, ocorreu em Londrina, Estado do Paraná, em relação a candidatura a prefeito municipal[2].

2. A PROTEÇÃO DE DADOS NAS CAMPANHAS POLÍTICAS

Nos últimos anos, as campanhas políticas tornaram-se cada vez mais sofisticadas, à medida que novas tecnologias digitais e ferramentas de comunicação se desenvolveram rapidamente e foram incorporadas às campanhas, permitindo o alcance instantâneo da maioria dos eleitores, mas com o potencial de violações aos direitos dos titulares e o desequilíbrio no direito de escolha, atraindo olhares jurídicos na elaboração de normas e orientações para que se mantenha o equilíbrio democrático.

De pronto cumpre reconhecer os propósitos das campanhas políticas como as atividades em apoio aos candidatos, difundindo ideias, ideais e ideologias das federações, dos partidos políticos, das candidaturas e mesmo pelos partidários na concorrência aos cargos eletivos, sendo que a proteção de dados pessoais é reconhecida como um direito fundamental em diversos ordenamentos jurídicos, decorrente da necessidade de salvaguardar a privacidade e a dignidade humana.

No Brasil, a Emenda Constitucional nº 115, de 2022, inseriu o inciso LXXIX ao artigo 5º da Constituição Federal,

2 Vale observar que a análise da decisão se deu com base em matérias jornalísticas veiculadas na internet porquanto o processo segue em segredo de justiça, como se vê em FOLHA DE LONDRINA. Justiça concede liminar contra campanha de Tiago Amaral. Disponível em: <https://www.folhadelondrina.com.br/politica/justica-concede-liminar-contra-campanha-de-tiago-amaral-3265284e.html?d=1> Acessado em: 07 ago. 2024.

reconhecendo expressamente a proteção de dados pessoais como direito fundamental:

> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Essa inserção reflete a crescente preocupação com o uso de informações pessoais na era digital e a necessidade de garantir que os indivíduos mantenham controle sobre seus dados. Os titulares, a partir da vigência das normas reconhecedoras do direito fundamental, assumem, efetivamente o protagonismo do processo, até porque, inerentes à própria personalidade.

Assim, a proteção de dados pessoais está ligada ao princípio da autodeterminação informativa, conceito desenvolvido pela doutrina alemã e incorporado em diversos sistemas jurídicos, que assegura ao indivíduo o poder de decidir sobre o uso de suas informações pessoais, como já reconhecido no Brasil pelo STF na ADI-DF 6.387[3].

Com efeito, a proteção de dados pessoais relaciona-se com a teoria do contrato social e os direitos naturais do indivíduo, uma vez que os direitos individuais devem ser protegidos pelo Estado para garantir a liberdade e a igualdade. As informações pessoais, na era digital, tornaram-se extensão da identidade do indivíduo, e seu controle é essencial para a manutenção da autonomia pessoal, notadamente no exercício do direito ao voto.

Percebe-se, também, que a sociedade da informação trouxe novos desafios para a privacidade e a interação social, a exigir constante renegociação das relações entre o indivíduo e as instituições, contexto em que a proteção de dados pessoais é ainda mais fundamental para evitar a manipulação e o controle social indevido, especialmente em processos eleitorais, em que a opinião pública do eleitor é a própria

3 https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false

essência do processo.

Nesse cenário é vital em qualquer sociedade democrática que partidos políticos e ativistas sejam capazes de se comunicar efetivamente com os eleitores. Mas é igualmente vital para a integridade das eleições e da democracia que todas as organizações envolvidas em campanhas políticas tratem os dados pessoais em conformidade com as normas de proteção de dados, o que somente é viável com a participação de um DPO indicado em conformidade com a LGPD, preceitos ANPD e normas do TSE.

Isso porque a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabeleceu no Brasil um marco regulatório para o tratamento de dados pessoais, alinhado às melhores práticas internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. A LGPD tem como finalidade proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade do indivíduo, e determina, de modo expresso, a observância de princípios como da finalidade, adequação, necessidade, transparência e segurança devem nortear o tratamento dos dados pelas candidaturas, sempre evitando práticas que possam comprometer a livre manifestação da vontade popular, uma vez que as campanhas políticas se tornam cada vez mais sofisticadas, à medida que novas tecnologias digitais e ferramentas de comunicação se desenvolve, com a aplicação de tecnologias e técnicas de marketing comercial para tentar entender eleitores em potencial e comunicar mensagens políticas.

Todavia, a natureza frequentemente invisível dessas técnicas pode afetar a confiança das pessoas naturais em como seus dados pessoais estão sendo tratados, incrementando riscos à integridade do processo democrático, pois os eleitores só podem fazer escolhas verdadeiramente informadas sobre em quem votar se tiverem certeza de que suas decisões não foram influenciadas injustamente.

O envio de mensagens e tecnologias usadas por partidos políticos e ativistas podem variar e mudar ao longo do tempo. Mas todos devem seguir as mesmas regras quando se trata de leis de proteção de dados e marketing direto, independentemente do método ou desenvolvimentos tecnológicos futuros.

Tal se dá para que se evite a repetição de casos como Cambridge Analytica, um dos escândalos mais emblemáticos, apurado a partir de denúncia feita pelos jornais The New York Times e The Guardian, que levantou dúvidas sobre a transparência e o compromisso da empresa com a proteção de dados dos usuários relacionados ao uso indevido de dados pessoais no contexto eleitoral.

No caso, a Cambridge Analytica[4], uma empresa de consultoria política, foi envolvida em práticas que levaram ao acesso não autorizado de dados de milhões de usuários do Facebook, que também foram utilizados para criar perfis psicológicos detalhados, empregados para direcionar propaganda política personalizada, influenciando eleições e referendos em vários países, destacando a maneira como dados pessoais podem ser usados para manipular a opinião pública, como ocorreu com a coleta de dados pessoais de cerca de 87 milhões de usuários do Facebook sem o consentimento adequado, utilizando-os para construir perfis de eleitores, segmentando eleitores com mensagens políticas altamente personalizadas, que podiam acentuar medos, preconceitos e preferências individuais, influenciando diretamente o comportamento eleitoral.

No Brasil, já se tem decisão da Justiça Eleitoral do Estado do Paraná, Junta Eleitoral da Comarca de Londrina, em que, no âmbito de Ação de Investigação Eleitoral foi concedida liminar para que o candidato comprovasse a lici-

4 BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>acessado em 07 ago. de 2024.

tude da campanha consistente no disparo massivo de mensagens por redes sociais, sob pena de bloqueio das redes. Segundo notícias apuradas pela internet, uma vez que o caso segue protegido por segredo de justiça, houve "operação de disparo em massa de mensagens eleitorais não autorizadas, por meio de agendas de contatos fornecidas por candidatos a vereador", bem como o candidato teria utilizado de "informações pessoais de eleitores sem o consentimento dos destinatários". Também foi noticiada a utilização de "robôs para entrar em contato com potenciais eleitores em todo município", o que fora percebido em razão de que as mensagens seguiam sempre o mesmo padrão, pedindo às pessoas mais dados pessoais. Em complemento, a magistrado determinou a informação, "em 48 horas contadas da intimação de qualquer deles pelo sistema as empresas e as produtoras terceirizadas das quais receberam dados pessoais para a execução de atividades de comunicação, com qualificação, através de planilha simples". Até a conclusão do presente estudo, seguia mantido o sigilo porquanto não encerrada a fase postulatória[5].

Essa decisão permite, também, perceber que a Justiça Eleitoral, como já ocorrera no exercício do poder regulamentar, pela edição de resoluções, em casos concretos também guarneça a relevância da LGPD e demais normas de proteção de dados pessoais.

Tanto que um dos tópicos da decisão consiste na determinação de que o consentimento é a base legal que legitima, de modo principal, o tratamento dos dados pessoais sensíveis de eleitores, ao lado da incidência do legítimo interesse, em determinados, e controversos, casos.

Como já dito, esse movimento brasileiro dá-se para

5 FOLHA DE LONDRINA. Justiça concede liminar contra campanha de Tiago Amaral. Disponível em: <https://www.folhadelondrina.com.br/politica/justica-concede-liminar-contra-campanha-de-tiago-amaral-3265284e.html?d=1> Acessado em: 07 ago. 2024.

manter o país como inserido no contexto internacional que privilegia a proteção dos dados pessoais ao garantir aos titulares o direito fundamental como se pode exemplificar com a União Europeia e o GDPR, regulamento geral pertinente à proteção de dados pessoais, cabendo reiterar que o grau normativo de regulamento, naquele bloco, implica que a norma ostente caráter vinculante a todos os estados-membros, e, no âmbito interno, cada país trate dos temas no âmbito de suas particularidades, com protagonismo das autoridades nacionais, as DPAs que disciplinam o tratamento dessas informações no contexto eleitoral.

3. AS AUTORIDADES DE PROTEÇÃO DE DADOS E O CONTEXTO ELEITORAL

A propósito, a Agência Espanhola de Proteção de Dados (AEPD)[6] destaca a necessidade de transparência e consentimento explícito dos eleitores para o uso de seus dados pessoais. Segundo as normas da AEPD, as campanhas devem informar claramente os eleitores sobre como seus dados serão coletados, utilizados e protegidos. Além disso, medidas robustas de segurança devem ser implementadas para evitar acessos não autorizados e vazamentos de dados.

Por seu turno, a Comissão Nacional de Informática e Liberdades (CNIL) – autoridade de proteção de dados da França enfatiza que os dados pessoais devem ser utilizados exclusivamente para fins eleitorais, com base no consentimento explícito dos eleitores. A transparência também é inafastável, e os eleitores devem ser informados sobre qualquer tratamento automatizado de seus dados, como a criação de perfis. A CNIL também reforça a importância de respeitar os direitos dos titulares de dados, permitindo-lhes acessar, corrigir e excluir suas informações pessoais, sendo que, para o pleito de 2024, instalou observatório relativo ao tratamento

6 https://www.aepd.es/, acessado em 10 out. 2024.

de dados pessoais, examinando relatórios ou possíveis reclamações que lhe foram enviadas no âmbito das campanhas permitindo reagir rapidamente a práticas que pudessem revelar desrespeito à regulamentação em matéria de proteção de dados pessoais e, se necessário, investigar e aplicar as competentes sanções.

Vale notar que, na esteira da decisão referida, no âmbito da Justiça Eleitoral de Londrina, PR, também, segundo a CNIL, a grande maioria dos relatos dos titulares, consistiram e chamadas telefônicas e mensagens de texto (93%) e os restantes a e-mails (6%) e cartas (1%), o que foi replicado por aqui, no primeiro turno das eleições municipais de 2024, conforme a decisão[7].

No Reino Unido, o Information Commissioner's Office (ICO)[8] – também determina que as candidaturas devem coletar apenas os dados estritamente necessários para suas atividades e garantir a proteção desses dados por meio de medidas de segurança adequadas. A transparência no uso de dados e a garantia dos direitos dos titulares, como acesso e exclusão de dados, são aspectos fundamentais ressaltados pelo ICO.

Na Itália, o Garante per la Protezione dei Dati Personali[9] destaca a importância de limitar o uso de dados pessoais ao mínimo necessário para as campanhas eleitorais. A transparência e a segurança dos dados são prioridades, e os eleitores devem ser claramente informados sobre o uso de seus dados e ter a capacidade de exercer seus direitos de maneira eficaz.

Já o European Data Protection Board (EDPB) fornece

7 https://www.cnil.fr/fr/elections-europeennes-2024-le-plan-daction-de-la-cnil-pour-proteger-les-donnees-des-electeurs, acessado em 11 ou. 2024.

8 https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf

9 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9105201

diretrizes gerais que destacam a necessidade de transparência e segurança no tratamento de dados pessoais em campanhas eleitorais. Recomendações incluem a limitação da coleta de dados ao necessário e a proteção adequada desses dados contra acessos não autorizados. O EDPB também enfatiza a importância de informar os eleitores sobre qualquer criação de perfis ou segmentação.

Fora do âmbito do GDPR, interessante ver que o Uruguai, por intermédio da Unidad Reguladora y de Control de Datos Personales – URCDP[10] estabelece que durante as campanhas eleitorais, o tratamento de dados pessoais deve ser feito com o consentimento explícito dos eleitores, garantindo transparência sobre o uso e proteção desses dados. As campanhas devem informar claramente como os dados serão utilizados, implementar medidas de segurança para protegê-los e respeitar os direitos dos titulares, como o acesso e a correção de informações. A URCDP também fiscaliza o cumprimento dessas diretrizes e pode aplicar sanções em casos de descumprimento.

Ainda, em comum, autoridades, densificando as normas, determinam a indicação de encarregado pela proteção dos dados pessoais pelas candidaturas, conforme ocorre no Brasil, nos termos do Guia Orientativo Aplicação da Lei Geral De Proteção de Dados Pessoais (LGPD) por Agentes de Tratamento no Contexto Eleitoral, elaborado conjuntamente pela Autoridade Nacional de Proteção de Dados Pessoais – ANPD e Tribunal Superior Eleitoral – TSE[11].

No documento, com o objetivo fornecer diretrizes para partidos políticos, candidatos e outros agentes envolvidos no processo eleitoral sobre como cumprir a LGPD durante as campanhas, há destaque da importância do consentimento informado dos eleitores para o tratamento de dados

10 https://www.gub.uy/unidad-reguladora-control-datos-personales/buscar?search_api_fulltext=elecci%C3%B3n&search-in-site=URCDP

11 https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf.

pessoais, especialmente quando esses dados são utilizados para direcionar propaganda política. O guia também enfatiza a transparência das campanhas em relação ao uso de dados pessoais, recomendando que sejam adotadas medidas para que os eleitores saibam como seus dados estão sendo tratados e para quais finalidades, e orienta sobre a implementação de medidas de segurança para proteger os dados pessoais contra acessos não autorizados e incidentes de segurança, e, claro, indiquem o DPO nos termos do art. 41 da LGPD como sendo o profissional ou empresa dedicados a serem os elos entre os titulares e os controladores, bem como as autoridades que tenham por objeto a proteção dos direitos fundamentais como o inscrito no inciso LXXIX do art. 5º da CF/88.

Todos esses procedimentos têm o objetivo de efetivar os direitos dos titulares como o direito de acesso, retificação e exclusão, que devem ser respeitados pelas campanhas também são destacados, ao lado do reforço da necessidade de conformidade com as disposições da LGPD para garantir a integridade e a confiança no processo eleitoral, bem como de não serem importunados indevidamente com disparos em massa de mensagens eletrônicas ou o tratamento automatizado dos dados pessoais como ocorreu no caso de Londrina, PR.

Nessa senda, a indicação de DPO é inafastável, notadamente nos municípios com mais de 200 mil eleitores, sendo que nos de menor colégio eleitoral, tal indicação configura boa prática porquanto, além de cumprir o disposto na norma, confere mais segurança às próprias candidaturas.

Com efeito, a indicação de profissional qualificado, sem conflitos de interesse, deve observar o disposto na Resolução 18 de 2024 da ANPD[12], com a referência às obrigações do experto nas campanhas eleitorais, que inclui garantir a conformidade com a LGPD, atuar como ponto de contato

12 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074, acessado em 09 out. 2024.

com a ANPD, e promover a conscientização e treinamento interno sobre proteção de dados.

Ainda merecem destaque os trechos em que o Guia elaborado pela ANPD e TSE esclarece sobre o tratamento automatizado de dados pessoais e o imperioso respeito às disposições da LGPD para o estabelecimento de uma relação de confiança entre candidatas ou candidatos e eleitoras ou eleitores, bem como para assegurar as condições necessárias para uma escolha autônoma e bem-informada, porquanto o tratamento irregular de dados pessoais e, notadamente de dados pessoais sensíveis, no âmbito das campanhas políticas, pode gerar impactos negativos sobre a lisura do processo eleitoral e sobre a igualdade de oportunidades entre candidatas e candidatos.

Outro tópico que informa a imperiosidade da indicação do DPO é a sensibilidade dos dados relacionados à opção política do titular, reconhecida pela ANPD e pelo TSE em relação à opinião política e à filiação a organização de caráter político, uma vez que as federações, partidos e candidaturas, também por intermédio dos militantes, realizarão o tratamento de dados pessoais lidando diretamente com essas informações que identifiquem ou tornem identificáveis titulares filiados a partidos políticos, ou pela formação de perfis que incluam a classificação da pessoa natural conforme suas opiniões políticas, sensibilidade que também pode decorrer do tratamento de inferência ou do cruzamento de bases de dados, conduzindo, ao menos de modo potencial à revelação ou identificação indireta de aspectos sensíveis relacionados à personalidade da pessoa titular, restringindo direitos, com a exposição de informações sobre origem racial ou étnica, convicção religiosa, em conjunto com a 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.

Na mesma senda, os bancos de dados de pessoas doa-

doras e voluntárias engajadas em determinada campanha eleitoral, ainda que contenha apenas informações cadastrais e de contato da pessoa titular deve ser monitorado pelo DPO uma vez que pode revelar opinião política, configurando dados pessoais sensíveis ao serem associados ao partido, federação ou ainda, dos próprios candidatos e candidatas.

Sendo o caso, o tratamento desses dados somente pode ocorrer nas hipóteses legais específicas previstas no art. 11 da LGPD, ou seja, casos mais restritos do que os incidentes sobre os dados pessoais não sensíveis do art. 7º da LGPD, sendo inviável a menção ao legítimo interesse do controlador, outro tema que demanda acompanhamento por encarregado que disponha de condições técnicas e operacionais para bem desenvolver suas atividades.

4. OS AGENTES DE TRATAMENTO E O ENCARREGADO

Sempre oportuno reiterar que o DPO ou encarregado de proteção de dados pessoais não é, nem pode ser, agente de tratamento, ou seja, não pode ser confundido com o controlador, que é quem decide sobre o tratamento dos dados pessoais, nem mesmo o operador que atua com as informações atendendo o disposto em cláusulas contratuais, nas quais os processos são determinados pelo controlador.

Nem mesmo pode haver a controladoria conjunta com o DPO pela incompatibilidade entre conceitos da LGPD no contexto eleitoral ao referir, partidos políticos, coligações e candidatas e candidatos serão, caso tratem dados pessoais e, observa-se, é praticamente inexistente a possibilidade de uma campanha eleitoral que não trate dados pessoais, controladores, ou seja, agentes de tratamento, bem como terceiros contratados para a realização de atividades de campanha envolvendo o tratamento de dados pessoais, reforçando a vedação do art. 31 da Resolução-TSE nº 23.610, de 18 de dezembro de 2019,

substituída pela Resolução 23.732/2024[13].

Outrossim, importa relembrar que diversos são os possíveis arranjos nas campanhas eleitorais, e, portanto, as responsabilidades de cada agente de tratamento serão percebidas em cada caso, para que sejam adequadas à LGPD, sendo, ainda, conforme adequado entendimento da ANPD, que ocorra em uma mesma operação de tratamento de dados pessoais a presença de mais de um controlador com poder de decisão sobre elementos essenciais de tratamento, no caso de controladoria conjunta, o que deve ser supervisionado pelo DPO para aferir da regularidade das avenças e protocolos estabelecidos entre os agentes de tratamento de forma que preservem adequadamente os direitos dos titulares dos dados pessoais tratados em razão dos acordos.

Na mesma senda, o DPO deve analisar a contratação de operadores, mediante documentos que contemplem a indicação precisa das responsabilidades e obrigações de cada parte, no que concerne aos dados pessoais tratados em razão do vínculo, também para que se preservem os direitos dos titulares desses dados pessoais.

Explicitando o tema, o TSE ocupou-se, no início do ano, de elaborar Resoluções que disciplinam o pleito, com destaque à Resolução 23.372/2024, sobre a propaganda eleitoral, conferindo ainda mais relevância à proteção de dados pessoais como obrigação das candidaturas, partidos federações e coligações.

Conforme a Resolução de 2024, partidos políticos, federações e candidatos que realizarem o tratamento de dados pessoais no contexto eleitoral devem garantir a transparência e segurança do processo, além de observar os direitos dos titulares, conforme previsto na LGPD. Isso inclui a necessidade de obter o consentimento explícito para o tratamento

13 https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019.

de dados pessoais, especialmente os dados pessoais sensíveis e a obrigação de criar registros detalhados das operações de tratamento de dados, que devem ser mantidos durante todo o período eleitoral, conforme orientação do próprio TSE, claro, indicar o DPO.

A resolução também estabelece que, nas eleições municipais em municípios com menos de 200 mil eleitores, os partidos e candidatos serão considerados agentes de tratamento de pequeno porte, aplicando-se as disposições da Resolução CD/ANPD nº 2 de 2022. Isso implica dispensa da nomeação de um encarregado de dados pessoais, embora ainda seja necessário disponibilizar um canal de comunicação para atender aos direitos dos titulares, o que, a contrário senso, compõe a obrigação de que, nos municípios com o número de eleitores superior a 200 mil, ou seja, em que pode ocorrer o segundo turno, a indicação, pelas candidaturas, ou seja, cada candidato majoritário ou a vereadora ou vereador, deverão indicar o encarregado pela proteção dos dados pessoais.

Além disso, a resolução impõe regras rigorosas para o uso de tecnologias digitais, como a inteligência artificial e o microdirecionamento de propaganda eleitoral, exigindo que os provedores de aplicação de internet e os responsáveis pelas campanhas garantam que essas práticas respeitem os princípios da LGPD, como a minimização de dados e a segurança, aliados à elaboração de relatórios de impacto à proteção de dados em casos de tratamento de alto risco, como o uso de dados sensíveis em larga escala, com a finalidade de garantir a conformidade com a legislação de proteção de dados.

Importa referir que o descumprimento das normas do TSE sobre a propaganda eleitoral, no que concerne à LGPD podem atrair a aplicação de sanções tanto pela Justiça Eleitoral quanto pela Autoridade Nacional de Proteção de Da-

dos (ANPD), de forma cumulativa, pois ambas as instâncias, esta administrativa e aquela, jurisdicional, possuem competências para aplicar sanções em caso de descumprimento das normas, sanções essas que podem variar dependendo da gravidade da infração e da entidade responsável pela fiscalização, o que torna o caso de Londrina, PR, já referido acima, seminal, e que, por certo, será a tônica dos próximos pleitos em relação às candidaturas.

Note-se que, em casos graves, pela Justiça Eleitoral, pode ser aplicada a cassação de registro ou mandato das candidatas e candidatos eleitos, em que o descumprimento configure como abuso de poder político ou uso indevido dos meios de comunicação social.

Também é possível a aplicação de multas para irregularidades na propaganda eleitoral, como a veiculação de conteúdos falsos ou descontextualizados, que podem afetar a integridade do processo eleitoral, no contexto de tratamento irregular de dados pessoais, conforme previsto na Lei 9.504/1997.

Tem-se, ainda, que a Justiça Eleitoral pode ordenar a cessão das propagandas em caso de condutas objetivas sejam olvidadas como a indicação do DPO, o que será compulsório no próximo pleito de 2026 por todas as candidaturas, uma vez que todos os candidatos a deputado estadual ou federal, senador, governador e presidente da república terão colégio eleitoral superior a 200 mil eleitores.

Esse fato assume grande repercussão porquanto, ao contrário das eleições municipais de 2024 em que a obrigatoriedade do DPO era restrita às capitais e grandes cidades, em 2026 a regra será de que absolutamente todas as candidaturas deverão indicar, cada uma, seu encarregado, nos termos da Resolução 18 de 2024, da ANPD[14].

E tal, vai atrair, além da atuação da Justiça Eleitoral,

14 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074.

o movimento da Autoridade Nacional de Proteção de Dados Pessoais – ANPD que poderá aplicar a candidatas, candidatos, partidos, federações e coligações, nas hipóteses de tratamento irregular de dados pessoais, como a mera omissão quanto à indicação do DPO, as sanções previstas na LGPD, no art. 52, tais como advertências para que as candidaturas adotem medidas corretivas em casos de infrações leves, multas que podem chegar a até 2% do faturamento da organização, limitada a R$ 50 milhões por infração, para casos de tratamento inadequado de dados pessoais.

Tem-se, também, a possibilidade de aplicação de bloqueio do uso de dados pessoais, até que a irregularidade seja corrigida, ou, em casos mais graves, a própria suspensão ou a proibição do tratamento de dados pessoais, por óbvio, impactando significativamente as atividades de campanha.

Em específico sobre a figura do DPO, a Resolução 18 da ANPD determina, no art. 3º que "a indicação do encarregado deve ser realizada por ato formal do agente de tratamento, do qual constem as formas de atuação e as atividades a serem desempenhadas", sendo que o § 1º menciona que se entende por "ato formal o documento escrito, datado e assinado, que, de maneira clara e inequívoca, demonstre a intenção do agente de tratamento em designar como encarregado uma pessoa natural ou uma pessoa jurídica", que, nos termos do § 2º, "deverá ser apresentado à ANPD, quando solicitado".

Outrossim, segundo o art. 4º, "nas ausências, impedimentos e vacâncias do encarregado, a função será exercida por substituto formalmente designado", não havendo escusas motivadas pela ausência do profissional porquanto tal fato não poderá consistir em obstáculos para o exercício dos direitos dos titulares ou para o atendimento às comunicações da ANPD.

Na esteira do mesmo documento, é mandatório que,

conforme o art. 9º a "identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, em local de destaque e de fácil acesso, no sítio eletrônico do agente de tratamento", ressalvada a hipótese do § 3º do preceito, sendo que a "divulgação da identidade do encarregado abrangerá, no mínimo o nome completo, se for pessoa natural, ou o nome empresarial ou o título do estabelecimento, bem como o nome completo da pessoa natural responsável, se pessoa jurídica, de modo que os dados referentes aos meios de comunicação que viabilizem o exercício dos direitos dos titulares junto ao controlador e possibilitem o recebimento de comunicações da ANPD.

De total relevo, também, a previsão do art. 10 da norma no sentido de que os agentes de tratamento, leia-se candidaturas, partidos políticos, coligações, federações, etc, deverão prover os meios necessários para o exercício das atribuições do encarregado, neles compreendidos, entre outros, recursos humanos, técnicos e administrativos, demandando, de modo formal e documentado, a assistência e orientação do encarregado quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais, além de garantir ao encarregado a autonomia técnica necessária para cumprir suas atividades, o que deve dar-se de forma livre de interferências indevidas, especialmente na orientação a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, para que se assegurem aos titulares os meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício de direitos, ao lado da garantia ao DPO de acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

Note-se que, em face do parco número de profissio-

nais aptos ao exercício dessas funções complexas e relevantes, a indicação pode recair sobre, nos termos do art. 12 da norma, pessoa natural, integrante do quadro organizacional do agente de tratamento ou externo a esse, ou pessoa jurídica, o que se revela recomendável para que se garanta a qualidade das orientações, uma vez que, conforme o art. 13 da Resolução 18, "o encarregado deverá ser capaz de comunicar-se com os titulares e com a ANPD, de forma clara e precisa e em língua portuguesa", sem que, contudo, pressuponha a inscrição em qualquer entidade nem qualquer certificação ou formação profissional específica.

Dispostas no art. 15 da Resolução, as atividades e atribuições do DPO ensejam que, ao receber comunicações da ANPD, o encarregado deverá adotar as medidas necessárias para o atendimento da solicitação e para o fornecimento das informações pertinentes, adotando, entre outras, providências como encaminhar internamente a demanda para as unidades competentes, fornecer a orientação e a assistência necessárias ao agente de tratamento, e indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado, bem como prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação, conforme o caso, de registro e comunicação de incidente de segurança, registro das operações de tratamento de dados pessoais, relatório de impacto à proteção de dados pessoais, mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais, medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, processos e políticas internas que assegurem o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, e dos regulamentos e orien-

tações da ANPD, instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais, nos casos de transferências internacionais de dados, bem como em relação às regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da Lei nº 13.709, de 14 de agosto de 2018.

Na mesma esteira, deve atuar o DPO dos agentes de tratamento da seara eleitoral no sentido de garantir que sejam adotados padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades, além, claro, de outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais, tudo conforme o art. 16 da Resolução.

Por fim, no art. 18, tem-se severa determinação quanto ao eventual conflito de interesses que deve ser afastado sob pena de responsabilização dos agentes de tratamento, uma vez que o DPO "deverá atuar com ética, integridade e autonomia técnica, evitando situações que possam configurar conflito de interesse", sendo viável o acúmulo de funções e o exercício das atividades para mais de um agente de tratamento, desde que seja possível o pleno atendimento de suas atribuições relacionadas a cada agente de tratamento e inexista conflito de interesse, conforme o art. 19, segundo o qual, também, pode configurar conflito de interesse entre as atribuições exercidas internamente em um agente de tratamento, o que ocorre com a indicação do advogado da candidatura, partido político, coligação, federação, etc, ou por responsáveis pela área da segurança da informação ou TI, decorrente do acúmulo de atividades de encarregado com outras que envolvam a tomada de decisões estratégicas sobre o tratamento de dados pessoais pelo controlador, ressalvadas as operações com dados pessoais inerentes às atribuições do encarregado.

Note-se que, também segundo o art. 19, "a existência de conflito de interesse será objeto de verificação no caso concreto e poderá ensejar a aplicação de sanção ao agente de tratamento" nos termos do art. 52 da LGPD, cumprindo, segundo o art. 20, que o indicado declare ao agente de tratamento "qualquer situação que possa configurar conflito de interesse, responsabilizando-se pela veracidade das informações prestadas", cumprindo ao agente de tratamento "atentar para que o encarregado não exerça atribuições que acarretem conflito de interesse".

Portanto, em virtude do papel fundamental das campanhas políticas na democracia, devem os agentes de tratamento, em especial para o próximo pleito de 2026, em que todos os candidatos disputarão vagas em colégio eleitoral superior a 200 mil eleitores, configurando todos agentes de tratamento de grande porte, indicar DPO em conformidade com a Resolução CD/ANPD Nº 018, DE 16.07.2024, pena de violação grave da normativa pertinente ao direito fundamental à proteção dos dados pessoais, ou seja, violando o direito dos titulares na condição de eleitores, promovendo ambiente eleitoral injusto e não confiável, rompendo a confiança na integridade do processo eleitoral e no uso de suas informações pessoais, sendo que somente o tratamento de dados pessoais de forma ética e responsável, contribui para a legitimidade das eleições e o fortalecimento da democracia e, portanto, a conformidade das candidaturas às normas vigentes.

REFERÊNCIAS

AEPD. Agência Espanhola de Proteção de Dados. Disponível em: <https://www.aepd.es/>.

BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>

FOLHA DE LONDRINA. Justiça concede liminar contra campanha de Tiago Amaral. Disponível em: <https://www.folhadelondrina.com.br/politica/justica-concede-liminar-contra-campanha-de-tiago-amaral-3265284e.html?d=1> Acessado em: 11 set. 2024.

IMPACTOS DO MARCO CIVIL DA INTERNET NAS ELEIÇÕES

Oscar Valente Cardoso[15]

5. INTRODUÇÃO

A internet transformou profundamente as dinâmicas sociais, políticas e econômicas em todo o mundo. No Brasil, a promulgação do Marco Civil da Internet, por meio da Lei nº 12.965/2014, representa uma base regulatória com princípios, garantias, direitos e deveres para o uso da internet no país. Essa lei também trouxe implicações significativas para a proteção de direitos fundamentais, como a liberdade de expressão, a privacidade e a proteção de dados pessoais. De forma específica, as eleições brasileiras passaram a enfrentar novas dificuldades em função da crescente digitalização das campanhas eleitorais e da disseminação de informações on-line.

Assim, a relevância deste artigo está na necessidade de compreender como o Marco Civil da Internet impacta diretamente o processo eleitoral, um aspecto central da democracia. A regulação da internet e suas implicações para a liberdade de expressão e a disseminação de informações durante as eleições são temas de crescente importância, especialmente em um contexto no qual as notícias falsas e a manipulação de dados se tornaram preocupações globais. Nesse contexto, o artigo busca contribuir para o debate acadêmico ao examinar as consequências do Marco Civil no contexto

15 Doutor em Direito (UFRGS), Especialista em Direito Processual Civil, em Inteligência Artificial e em Ciência de Dados e *Big Data Analytics*, Coordenador do Comitê Gestor de Proteção de Dados do TRF4, Professor no Mestrado da Universidade Europeia de Lisboa, Juiz Federal.

eleitoral brasileiro, bem como propor possíveis melhorias para o seu aprimoramento.

Para esse fim, o artigo é dividido em seções que seguem uma lógica progressiva. Inicialmente, será apresentado um panorama geral do Marco Civil da Internet e seus principais aspectos, seguido por uma análise específica do impacto dessa legislação no processo eleitoral. Na sequência, será examinada a proteção de dados pessoais dos eleitores, para, ao final, indicar propostas e desafios futuros no equilíbrio entre liberdade de expressão e moderação de conteúdo no meio digital.

6. MARCO CIVIL DA INTERNET: PRINCIPAIS ASPECTOS

A importância do Marco Civil da Internet (Lei nº 12.965/2014) transcende a simples regulação do espaço cibernético, pois estabelece normas que moldam o comportamento de usuários, provedores de serviço e o próprio Estado na administração do ambiente digital.

A lei estabelece princípios fundamentais que orientam a regulação do uso da internet no Brasil, a fim de assegurar que o ambiente digital seja um espaço de liberdade, privacidade e respeito aos direitos individuais. Esses princípios, listados no art. 3º, são essenciais para a interpretação e aplicação das normas contidas no Marco Civil.

Um dos princípios mais destacados é a garantia da liberdade de expressão (art. 3º, I), que tem fundamento no art. 5º, IX, da Constituição e é um dos direitos individuais mais valorizados em uma sociedade democrática. O Marco Civil consagra o direito de os usuários se expressarem livremente na internet, sem censura prévia, o que reforça o compromisso com a pluralidade de ideias e opiniões. Esse princípio é essencial em um ambiente digital, no qual a comunicação é instantânea e de alcance global, e permite que todos os cidadãos possam participar ativamente do debate público, inclu-

sive por meio da criação e compartilhamento de conteúdo. O Marco Civil assegura que os usuários da internet tenham o direito de se expressar livremente, sem censura prévia, em todas as plataformas digitais[16]. No contexto eleitoral, a liberdade de expressão é vital para garantir que candidatos e eleitores possam debater ideias, criticar governos e promover suas opiniões sem interferências indevidas. No entanto, esse direito (como qualquer outro) não é absoluto. O Marco Civil, ao garantir a liberdade de expressão, também impõe a responsabilização por abusos e pela prática de atos ilícitos. Assim, a lei busca equilibrar o direito de se expressar livremente com a necessidade de proteger outros direitos individuais, como, por exemplo, a honra e a privacidade.

Outro princípio fundamental é a neutralidade da rede (art. 3º, IV), que assegura que todo tráfego de dados na internet seja tratado de forma isonômica, sem discriminação por conteúdo, origem, destino, serviço ou aplicação. Esse princípio, regulado pelo art. 9º, impede que provedores de internet possam priorizar ou limitar o acesso a determinados conteúdos, a fim de garantir que a internet permaneça um espaço aberto e acessível a todos, independentemente de seu poder econômico ou interesses comerciais. No âmbito eleitoral, a neutralidade da rede assegura que todos os candidatos e partidos políticos possam acessar as mesmas ferramentas digitais para disseminar suas mensagens, sem que haja privilégios para determinados conteúdos em detrimento de outros. Esse princípio evita que interesses econômicos ou políticos interfiram na livre circulação de informações durante o processo eleitoral, e busca garantir que o debate público on-line ocorra em condições justas e igualitárias. Além disso, a neutralidade da rede protege os eleitores, para garantir que eles possam acessar todas as informações

16 Sobre o assunto, ver capítullo 6 de: CASTELLS, Manuel. *A galáxia da internet:* reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

disponíveis sobre candidatos e propostas, sem que seu acesso seja restringido ou influenciado por terceiros. Essa garantia é especialmente relevante em um no qual as redes sociais e outras plataformas digitais se tornaram as principais fontes de informação para muitos eleitores.

A proteção da privacidade e dos dados pessoais dos usuários também são princípios que compõem os pilares do Marco Civil da Internet (art. 3º, II e III), mesmo antes da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). A Lei nº 12.965/2014 estipula que os dados pessoais só podem ser tratados na internet mediante o consentimento expresso do titular (o que foi ampliado pela LGPD com outras bases legais), e que devem ser protegidos contra acessos não autorizados e usos indevidos. Estes princípios são especialmente relevante no contexto das eleições, em que a privacidade dos eleitores e o uso lícito de seus dados são questões de extrema importância. Durante as eleições, os dados dos eleitores, como suas preferências políticas, comportamentos de voto e informações demográficas, podem ser utilizados de maneira indevida para influenciar o resultado das eleições (quando não forem tratados de acordo com as normas legais). A coleta massiva e o uso não autorizado de dados para fins de marketing político ou para a criação de campanhas segmentadas representam uma ameaça significativa à integridade do processo eleitoral. O Marco Civil da Internet, ao proteger os dados pessoais, impõe deveres aos provedores de internet, que devem garantir a segurança e a confidencialidade das informações extraídas dos dados pessoais dos usuários. Esses deveres são complementados pela LGPD, que introduziu medidas adicionais para a proteção dos dados pessoais.

O Marco Civil também enfatiza como princípio a responsabilidade dos provedores de aplicação conforme as suas atividades (art. 3º, VI), segundo o qual, em regra, eles não podem ser responsabilizados pelo conteúdo gerado por terceiros, exceto se não cumprirem as determinações (legais ou

judiciais) que determinem a remoção de conteúdos ilegais. Esse princípio visa proteger a liberdade de expressão, ao evitar a censura arbitrária por parte dos provedores, ao mesmo tempo em que responsabiliza aqueles que facilitam ou incentivam a disseminação de conteúdos ilícitos.

Esses princípios, ao lado de outras normas legais, fornecem a base para a regulação do uso da internet no Brasil, ao buscar o equilíbrio entre a proteção dos direitos dos usuários e a promoção de um ambiente digital livre e inclusivo. No contexto eleitoral, esses princípios têm implicações diretas sobre como a informação circula, como os dados dos eleitores são protegidos e como a liberdade de expressão é exercida, sendo essenciais para a análise do impacto do Marco Civil nas eleições brasileiras.

7. IMPACTOS DO MARCO CIVIL DA INTERNET NO PROCESSO ELEITORAL

A digitalização da comunicação e a popularização das redes sociais transformaram radicalmente a forma como as campanhas eleitorais são conduzidas e como os eleitores interagem com o processo político. Nesse novo cenário, o Marco Civil da Internet desempenha um papel relevante, ao estabelecer o arcabouço jurídico que regula o uso da internet e protege os direitos fundamentais dos cidadãos no ambiente digital[17].

Com o avanço da tecnologia e a crescente dependência da internet para a comunicação política, entender o impacto do Marco Civil da Internet no processo eleitoral é fundamental para avaliar a sua eficácia e identificar áreas que ainda necessitam de aprimoramento. O impacto dessa lei nas eleições brasileiras é multifacetado, pois abrange desde a garantia da liberdade de expressão nas campanhas até a proteção dos dados pessoais dos eleitores e o combate à

17 RAIS, Diogo (coord.). *Direito eleitoral digital*. 3. ed. São Paulo: RT, 2022.

desinformação. À medida que as tecnologias digitais se tornam cada vez mais centrais para a dinâmica eleitoral, o Marco Civil se apresenta como uma lei essencial para garantir que o processo eleitoral permaneça justo, transparente e acessível, sem restringir de forma indevida a liberdade de expressão no meio digital.

A liberdade de expressão é um dos direitos fundamentais mais valorizados em uma democracia, essencial para a realização de eleições livres e justas. Nas campanhas eleitorais, esse direito contém uma relevância ainda maior, pois garante que candidatos, partidos políticos e eleitores possam debater ideias, expor propostas e criticar adversários de forma aberta e sem censura. Ao regulamentar o uso da internet no Brasil, o Marco Civil da Internet reafirma e protege a liberdade de expressão no ambiente digital, para que as campanhas eleitorais possam ser conduzidas de maneira transparente.

Como visto, o Marco Civil da Internet inclui a liberdade de expressão como um de seus princípios fundamentais, o que garante que todos os usuários da internet tenham o direito de se expressar livremente, sem a interferência de censura prévia. Esse princípio é particularmente relevante durante as campanhas eleitorais, quando há um crescimento do fluxo de informações e opiniões sobre questões políticas. No ambiente digital, essa liberdade permite que candidatos e eleitores utilizem diversas plataformas, como redes sociais, blogs e sites de notícias, para compartilhar e debater conteúdos políticos.

Porém, a liberdade de expressão nas campanhas eleitorais não é absoluta e deve ser exercida de forma lícita, sob pena de gerar a responsabilidade (civil, penal e/ou administrativa) por eventuais violações e danos. O Marco Civil da Internet estabelece que, embora os provedores de serviços de internet não sejam responsáveis pelo conteúdo gerado por

terceiros (arts. 3º, VI, e 18)[18], eles têm o dever de remover conteúdos que violem direitos e causem danos, em determinadas situações.

De forma específica, conforme as regras do Marco Civil e a jurisprudência do Superior Tribunal de Justiça, o provedor de aplicação tem o dever legal de remoção de conteúdo da internet gerado por terceiro quando:

(a) o conteúdo contiver cenas de nudez ou de atos sexuais de caráter privado, o provedor for notificado por um dos participantes (ou seu representante legal) para efetuar a remoção, mas deixar de realizá-la (art. 21 do Marco Civil da Internet);

(b) o conteúdo não se enquadrar nas situações descritas no item anterior, o provedor for intimado por decisão judicial (em processo movido por eventual vítima) para efetuar a remoção, mas deixar de realizá-la (art. 19 do Marco Civil da Internet).

A determinação judicial de remoção do conteúdo só é válida se contiver a "identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material" (art. 19, § 1º, do Marco Civil). Da mesma forma, no entendimento do STJ, é necessária a "(...) indicação clara e específica do localizador URL do conteúdo infringente para a validade de comando judicial que ordene sua remoção da internet." (REsp 1698647/SP, 3ª Turma, rel. Min. Nancy Andrighi, DJe 15/02/2018). No mesmo sentido: AgInt nos EDcl nos EDcl no REsp 1890786/DF, 4ª Turma, rel. Min. Marco Buzzi, j. 30/10/2023, DJe 03/11/2023.

Além disso, o provedor de aplicação também pode realizar, de forma preventiva ou repressiva, a denominada

18 Acerca da interpretação dos referidos dispositivos legais, no STJ: "(...) 1. Segundo a jurisprudência do Superior Tribunal de Justiça, os sites de buscas não são responsáveis pelas informações disponibilizadas na internet por terceiros" (AgInt no REsp 1938063/RJ, 3ª Turma, rel. Min. Marco Aurélio Bellizze, j. 19/06/2023, DJe 21/06/2023).

"moderação de conteúdo", que consiste na análise e gerenciamento das postagens realizadas por usuários em suas plataformas, com o objetivo de garantir que os conteúdos disponibilizados estejam de acordo com as políticas internas da aplicação e com a legislação. Por exemplo, um texto que contenha fatos que em tese possam caracterizar crime contra a honra (calúnia, injúria ou difamação) contra terceiros pode ser bloqueado ou retirado pelo próprio provedor de aplicação, independentemente de notificação da vítima ou de decisão judicial. Essa moderação pode ser exercida de maneira automatizada, por meio de inteligência artificial, ou por equipes humanas que avaliam manualmente o conteúdo considerado sensível ou potencialmente ilícito.

No âmbito eleitoral, essa prática adquire especial relevância, uma vez que a disseminação de notícias falsas, a prática de atos ilícitos contra a honra de candidatos e outros atos (civil ou penalmente) ilícitos podem comprometer a integridade do processo democrático. Ao atuarem de maneira preventiva, os provedores buscam identificar e neutralizar essas ameaças antes que atinjam um grande público. Já no aspecto repressivo, a moderação envolve a remoção de conteúdos publicados que forem considerados inadequados ou ilegais, por decisão própria da plataforma.

A moderação de conteúdo, contudo, apresenta desafios consideráveis, especialmente no que se refere ao equilíbrio entre a proteção da liberdade de expressão e a necessidade de garantir um ambiente digital seguro e livre de abusos. Por isso, sua aplicação requer critérios claros e transparentes (previamente definidos nos termos e condições de uso do provedor de aplicação, divulgado de forma clara e em um acesso fácil), além de mecanismos gratuitos e acessíveis de contestação, para que os usuários possam questionar moderações que considerem injustas ou equivocadas.

Sobre o assunto, o Superior Tribunal de Justiça entende que a moderação de conteúdo é uma atividade líci-

ta do provedor de aplicação, considerando que o art. 19 do Marco Civil da Internet não proíbe que este tenha a iniciativa de impedir a publicação ou de remover conteúdo ilícito ou em contrariedade com o contrato firmado com o usuário. Contudo, o "*shadow banning*" que consiste na moderação de conteúdo de difícil detecção pelo usuário (em virtude da assimetria informacional existente na relação jurídica e da hipossuficiência técnica deste), que gera a restrição ou o bloqueio do conteúdo publicado por ele, caracteriza, em tese, ato ilícito do provedor de aplicação (REsp 2139749/SP, 3ª Turma, rel. Min. Ricardo Villas Bôas Cueva, j. 27/08/2024, DJe 30/08/2024).

Assim, o ambiente digital apresenta desafios específicos para a liberdade de expressão nas campanhas eleitorais. A velocidade e o alcance da internet facilitam a propagação de informações, mas também tornam mais difícil o controle de conteúdos eventualmente ilícitos. A disseminação de desinformação e notícias falsas, muitas vezes amplificada por algoritmos de plataformas digitais, pode distorcer o debate público e influenciar indevidamente o processo eleitoral.

8. IV. PROTEÇÃO DE DADOS PESSOAIS DOS ELEITORES

A proteção de dados pessoais dos eleitores é uma questão central das eleições modernas, especialmente em um cenário no qual a coleta e as atividades subsequentes de tratamento de dados digitais se tornaram práticas comuns nas campanhas eleitorais.

O Marco Civil da Internet, em conjunto com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), contêm normas que devem ser aplicadas em conjunto para garantir que os dados pessoais dos eleitores sejam tratados com segurança e em conformidade com os requisitos legais, a fim de assegurar a licitude das operações

em um ambiente digital cada vez mais intrusivo[19].

Nas campanhas eleitorais contemporâneas, os dados pessoais dos eleitores são utilizados para uma variedade de finalidades, desde a segmentação de campanhas até a análise de comportamento e a personalização de mensagens políticas. Essas práticas, embora potencialmente eficazes para alcançar eleitores de maneira mais direcionada, levam a questões sobre a proteção de dados e o tratamento lícito dos dados pessoais.

Como visto, o Marco Civil da Internet garante a proteção dos dados pessoais dos usuários da internet, ao estabelecer que a coleta, uso, armazenamento e compartilhamento desses dados (entre outras atividades) devem ser realizados com o consentimento expresso do titular e para finalidades legítimas e específicas (art. 7º, IX).

Em complemento, a LGPD introduz princípios (art. 6º) e um conjunto mais detalhado de deveres para o tratamento de dados pessoais, além de inserir diversas outras bases legais (além do consentimento) que podem ser indicadas pelo agente para iniciar as operações de tratamento (arts. 7º e 11). No contexto eleitoral, a LGPD deve ser observada especialmente sobre como os dados pessoais dos eleitores podem ser coletados e utilizados pelas campanhas e pelos partidos políticos.

Além disso, a LGPD impõe a necessidade de medidas de segurança, técnicas e administrativas, robustas para proteger os dados contra acessos não autorizados, vazamentos e outros incidentes de segurança (arts. 46/47 e 49/51).

A transparência é um dos princípios de tratamento de dados pessoais previstos na LGPD (art. 6º, VI), o que impõe que os eleitores sejam informados sobre como seus dados estão sendo tratados, quem tem acesso a eles, e quais são

19 Sobre a LGPD: CARDOSO, Oscar Valente. *Introdução à Lei Geral de Proteção de Dados Pessoais*. Xangri-Lá: Edição do autor, 2020.

os seus direitos em relação a esses dados. Esse nível de transparência é essencial para manter a confiança dos eleitores e assegurar que os seus dados e informações pessoais não sejam explorados de forma indevida durante as campanhas eleitorais.

Um dos principais desafio está na falta de conscientização dos eleitores sobre os direitos relativos aos dados. Os titulares não têm conhecimento de como os dados pessoais são tratados pelas campanhas, o que pode resultar em consentimentos conferidos de forma inadequada ou sem a compreensão clara de suas consequências.

Adicionalmente, a crescente sofisticação das técnicas de coleta e análise de dados, como o uso de inteligência artificial para a criação de perfis e para prever comportamentos eleitorais (como o tratamento de dados pessoais dos eleitores para fins de segmentação e *microtargeting* nas campanhas), leva a questões sobre o grau de influência que essas tecnologias podem exercer sobre o processo democrático.

Apesar das garantias legais oferecidas pelo Marco Civil da Internet e pela LGPD, a proteção de dados dos eleitores enfrentam desafios significativos na era digital. A natureza descentralizada e global da internet dificulta a fiscalização efetiva e a aplicação das normas, especialmente quando as campanhas eleitorais envolvem a participação de empresas de tecnologia e provedores de serviços de internet localizados fora do país.

Portanto, a aplicação efetiva das normas legais requer não apenas um marco regulatório, mas também a conscientização dos eleitores e a capacidade das autoridades de fiscalização de atuar em um ambiente digital cada vez mais complexo e difuso.

9. LIBERDADE DE EXPRESSÃO E MODERAÇÃO DE CONTEÚDO

A aplicação do Marco Civil da Internet nas eleições

contribui para a proteção dos direitos dos eleitores e para a promoção de um ambiente digital mais seguro e transparente. Esses impactos refletem os avanços na regulação do uso da internet no contexto eleitoral, bem como os esforços dos provedores de aplicação em implementar e cumprir as normas estabelecidas pela legislação.

Um dos impactos mais significativos do Marco Civil foi o fortalecimento da liberdade de expressão no ambiente digital durante as eleições. A legislação assegura que candidatos, partidos políticos e eleitores possam utilizar as redes sociais, os aplicativos de mensagens e outras plataformas digitais para se expressar livremente, sem censura prévia. Esse fortalecimento da liberdade de expressão na internet permitiu um debate público mais amplo e diversificado, em que diferentes visões e opiniões passaram a ser apresentadas e discutidas abertamente, em um grau e alcance sem precedentes.

Além disso, o Marco Civil proporcionou um ambiente no qual a diversidade de opiniões foi capaz florescer, ao permitir que opiniões dissonantes tivessem uma plataforma para se expressar e participar ativamente do processo eleitoral. Essa abertura contribuiu para uma maior inclusão digital e para a democratização do acesso à informação durante as campanhas eleitorais.

A aplicação do Marco Civil da Internet em conjunto com a Lei Geral de Proteção de Dados também produz impacto positivos, ao fortalecer a proteção dos dados pessoais dos eleitores durante as campanhas eleitorais. Essa proteção contribui para aumentar a confiança dos eleitores no processo eleitoral digital, reduz o risco de manipulação e uso indevido de seus dados informações. As campanhas eleitorais, ao se adequarem às exigências legais, passaram a adotar práticas mais responsáveis no tratamento de dados pessoais, o que fortaleceu a integridade e a legitimidade do processo eleitoral.

O Marco Civil também promoveu maior transparência e fiscalização das atividades digitais relacionadas às eleições. As plataformas digitais passaram a adotar práticas mais transparentes na moderação de conteúdos e na comunicação com os usuários sobre suas políticas de uso, o que facilitou a fiscalização por parte das autoridades eleitorais e aumentou a confiança pública no processo. A transparência nas ações dos provedores de aplicação, como a divulgação de relatórios sobre a remoção de conteúdos e a cooperação com as autoridades eleitorais, ajudou a criar um ambiente mais confiável e monitorado.

Outro impacto da regulação legal foi a definição de responsabilidades para os provedores de aplicação, que passaram a desempenhar um papel mais ativo na moderação de conteúdos e na remoção de informações falsas ou ilícitas, nas hipóteses previstas em lei ou em contrato. Essa responsabilização ajudou a reduzir a disseminação de notícias falsas e conteúdos prejudiciais, a fim de proteger a integridade do processo eleitoral.

Embora o Marco Civil da Internet contenha normas claras acerca da responsabilização dos provedores de aplicação, a sua aplicação prática apresenta desafios e áreas cinzentas. A moderação de conteúdo em larga escala é uma tarefa complexa e as plataformas digitais muitas vezes enfrentam dificuldades em garantir que suas ações sejam consistentes e justificáveis. A falta de transparência em alguns casos sobre os critérios usados para a moderação e a remoção de conteúdo pode levar a acusações de censura ou de aplicação desigual das normas, com a judicialização das controvérsias.

Além disso, a localização de muitos provedores de aplicação fora da jurisdição brasileira cria dificuldades para o cumprimento de ordens judiciais e a responsabilização efetiva dessas plataformas. A cooperação internacional, embora existente, ainda enfrenta limitações que dificultam a aplicação uniforme das disposições do Marco Civil da Internet,

especialmente durante o período eleitoral.

10. CONSIDERAÇÕES FINAIS

Os provedores de aplicações da internet (redes sociais, aplicativos de mensagens e outras plataformas digitais) desempenham uma função central na aplicação prática das garantias e limitações à liberdade de expressão durante as campanhas eleitorais. O Marco Civil impõe a esses atores a responsabilidade de agir em conformidade com a lei, especialmente no que se refere ao cumprimento de ordens judiciais para a remoção de conteúdos ilegais. Contudo, o papel desses provedores vai além da mera execução de ordens judiciais, tendo em vista que eles também desempenham um papel ativo na moderação de conteúdos, o que pode impactar diretamente a visibilidade das informações durante as eleições.

Por isso, a transparência e a prestação de contas por parte dos provedores de aplicação são essenciais para garantir que suas ações não comprometam a liberdade de expressão. Medidas como a elaboração de relatórios de transparência, a divulgação de políticas claras sobre moderação de conteúdo e a cooperação com autoridades eleitorais são práticas que podem contribuir para a proteção dos direitos dos usuários e a manutenção de um ambiente digital democrático durante as eleições.

A liberdade de expressão nas campanhas eleitorais, protegida pelo Marco Civil da Internet, é um elemento vital para a democracia brasileira. Embora o ambiente digital ofereça novas formas para o exercício desse direito, ele também impõe desafios significativos, que exigem uma regulação e equilibrada. A Lei nº 12.965/2014, ao garantir a liberdade de expressão e estabelecer mecanismos para combater abusos, desempenha um papel fundamental na proteção da integridade das eleições e na promoção de um debate público aberto e inclusivo.

Para concluir, recomenda-se para o aperfeiçoamento da aplicação do Marco Civil da Internet no período eleitoral:

- Criação de mecanismos de resposta rápida: a introdução de mecanismos processuais que permitam a remoção rápida de conteúdos prejudiciais, especialmente durante o período eleitoral, poder mitigar os efeitos negativos da desinformação antes que causem danos significativos e irreversíveis;

- Fortalecimento da cooperação internacional: considerando a natureza global das plataformas digitais, é preciso fortalecer a cooperação internacional, para garantir que as ordens judiciais brasileiras sejam cumpridas por provedores de aplicação sediados fora do país;

- Aprimoramento da transparência nos provedores de aplicação: a exigência de maior transparência por parte das plataformas digitais, tanto em suas políticas de moderação quanto na prestação de contas sobre a moderação de conteúdos, pode aumentar a confiança pública e a eficácia da legislação;

- Atualização contínua das normas jurídicas: diante da rápida evolução das tecnologias digitais, o Marco Civil da Internet e outras normas correlatas precisam ser revisados e atualizados regularmente para abordar novos desafios, como o uso de inteligência artificial e *big data* nas campanhas eleitorais.

REFERÊNCIAS

CARDOSO, Oscar Valente. *Introdução à Lei Geral de Proteção de Dados Pessoais*. Xangri-Lá: Edição do autor, 2020.

CASTELLS, Manuel. *A galáxia da internet:* reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

RAIS, Diogo (coord.). *Direito eleitoral digital*. 3. ed. São Paulo: RT, 2022.

PROPAGANDA ELEITORAL DIGITAL: REGRAS, LIMITAÇÕES E INOVAÇÃO NAS CAMPANHAS ONLINE

Rafael A. Carneiro de Castilho[1]

1. INTRODUÇÃO

Tratar de um tema como a propaganda eleitoral em meio digital representa desafiadora tarefa por envolver diferentes esferas sociais que se encontram em ebulição, isto é, encontram-se profunda transformação e colidem entre si no atual momento da história.

Para desenvolver o objeto deste artigo precisamos compreender o atual estado das coisas, para que apenas então seja possível alcançarmos algumas conclusões sobre a necessidade de regras e limitações, de modo a propiciar o desenvolvimento da inovação em meio à propaganda eleitoral digital.

Para tanto, devemos avaliar três principais eixos de modo que seja possível o desenvolvimento da temática no presente artigo, sendo eles: a democracia; a tecnologia; e a legislação.

2. DEMOCRACIA

A democracia tem sua origem na Grécia antiga, tendo o seu primeiro registro em Atenas, por volta do século

1 Rafael Augusto Carneiro de Castilho, Advogado, pós-graduado em Direito Digital e Proteção de Dados pela Escola Brasileira de Direito, pós-graduado LLM em Proteção de Dados, titulação Brasil e Portugal, pela Fundação Escola Superior do Ministério Público e Faculdade de Direito da Universidade de Lisboa, com extensão em Direito Imobiliário pela Fundação Getúlio Vargas e extensão em Processo Civil pela DAMÁSIO.

V a.C., e se desenvolve durante a República Romana, entrando posteriormente em um período de recessão com a queda do Império do Romano e a ascensão da Idade Média e os sistemas feudais, para renascer apenas entre os séculos XIV e XVIII culminando na Revolução Americana, de 1776, e na Revolução Francesa, de 1789.

Contudo, apenas recentemente, após as duas grandes guerras mundiais e o fim da Guerra Fria, com o colapso da União Soviética, é que conhecemos o atual sistema democrático que conhecemos.

Assim, podemos observar o longo trajeto de lapidação da democracia, contudo precisamos compreender a essência da democracia para que possamos analisar o seu estado atual, e para tanto podemos lançar mão do exemplo manifestado por Dahl (2001, p. 47), em que "todos nós temos objetivos que não conseguimos atingir sozinhos. No entanto, cooperando com outras pessoas que visam a objetivos semelhantes, podemos atingir alguns deles"[2].

Dahl prossegue exemplificando a criação de uma associação entre indivíduos para o alcance desses objetivos, e que para o seu funcionamento será necessário o desenvolvimento de uma constituição para o seu regramento e que durante as discussões chega-se ao seguinte contexto, nas palavras de um dos participantes da assembleia:

> Nas questões mais importantes de que esta assembleia tratará, nenhum de nós é tão mais sábio do que os outros, para que automaticamente prevaleçam as ideias de um ou de outro. Ainda que alguns membros saibam mais sobre uma questão em determinado momento, somos todos capazes de aprender o que precisamos saber.[3]

O trecho mencionado retrata exatamente a essência

2 DAHL. Robert A. *Sobre a Democracia*. Tradução de Beatriz Sidou. Brasília: Editora Universidade de Brasília, 2001, p. 47.

3 DAHL, op. cit., p. 48.

da democracia, onde cada indivíduo tem poder de voz e detém uma perspectiva divergente sobre o mesmo contexto, tornando imprescindível a necessidade de discussão das ideias para a tomada de decisões em nível coletivo.

Assim, podemos compreender que a essência da democracia é a divergência de ideias e a convergência de debates para que então se decida por um caminho a ser seguido por todos, como uma única entidade.

No atual estado das coisas, a ideia de democracia parece estar entrando em um período de regressão, com nações democráticas passando por períodos de turbulência interna, tendo entre as suas causas a polarização de ideias, em que grupos com visões diferentes toleram cada vez menos opiniões divergentes.

Esses sintomas têm sido observados ao redor do mundo, em que ano após ano tem se observado a deterioração da democracia e a ascensão de regimes autoritários, criando uma polarização global entre democracias e ditaduras[4], e que segundo Diamond (2024, tradução livre) "talvez a dimensão mais preocupante da recessão democrática tenha sido o declínio da eficácia, energia e autoconfiança democrática no Ocidente, incluindo os Estados Unidos"[5].

No Brasil o estado da democracia não é menos complexo, vez que é possível observar o embate cada vez mais agressivo entre indivíduos de espectros ideológicos distintos, esvaziando-se quase que por completo a possibilidade de composição de ideias, tendo como plano de fundo três fenômenos que podem ser citados: o populismo, o

4 Freedom House. Global Freedom Status. Disponível em: <https://freedomhouse.org/explore-the-map?type=fiw&year=2024>. Acesso em: 15 set. 2024.

5 DIAMOND, Larry. Democracy in Retreat: The Revolt of the Middle Class and the Worldwide Decline of Representative Government. Stanford University, 2024. Disponível em: <https://www.v-dem.net/en/news/democracy-in-retreat>. Acesso em: 15 set. 2024.

extremismo e o autoritarismo[6].

Esses eventos estão diretamente ligados a percepção social de insuficiência dos governos e a sua expressão pública por cada indivíduo, tendo a sua voz potencializada pelas redes sociais. O Brasil, como o segundo país que mais consume mídia social no mundo[7], tem esses efeitos potencializados, através do reforço de viés ideológico pelo notório fenômeno das bolhas de informação, o que nos leva à esfera seguinte da temática.

3. TECNOLOGIA

A tecnologia é uma ferramenta que utilizamos para simplificar tarefas, sendo o ser humano quem a controla na execução das suas atividades, contudo o que se verifica na atualidade é uma perceptível inversão desses polos, no qual a tecnologia passou a ter influência direta sobre o comportamento humano, e que em última consequência nos conduz às rupturas sociais que verificamos até aqui.

O primeiro grande ponto do tema neste artigo abordado, é a manipulação algorítmica e os seus reflexos na democracia, vez em que as plataformas de rede social detém papel preponderante no modo como as informações são distribuídas, o que é feito através de algoritmos, de modo a determinar quais conteúdos serão exibidos para os usuários.

Esse modelo prioriza o engajamento dos usuários, que em outras palavras pode-se dizer que são aqueles conteúdos que geram mais interação, como as curtidas,

6 BARROSO. Luís Roberto. A democracia sob pressão: o que está acontecendo no mundo e no Brasil. CEBRI, 2023. Disponível em: <https://cebri.org/revista/br/artigo/23/a-democracia-sob-pressao-o-que-esta-acontecendo-no-mundo-e-no-brasil>. Acesso em: 15 set. 2024.

7 COMSCORE. Um olhar em Social media – Insights 2023 x 2024. COMSCORE, 2024. Disponível em: <https://www.comscore.com/por/Insights/Apresentacoes-e-documentos/2024/Um-olhar-em-Social-media-Insights-2023-x-2024>. Aceso em: 16 set. 2024.

compartilhamentos e comentários.

Ocorre que essa metodologia tem o potencial de criar um ciclo de retroalimentação, no qual informações sensacionalistas ou que detém maior teor de polarização, são promovidas, em prejuízo de conteúdos com maior qualidade. Esse controle de quais informações os usuários terão acesso pode conduzir para disseminação de desinformação, vez em que conteúdos com reforço de viés do usuário são facilmente repassados adiante, criando uma potente cadeia de impulsionamento desses conteúdos.

Esse contexto implica na própria capacidade de formação de opinião dos usuários, vez em que uma informação dúbia, mas com teor de reforço do viés ideológico do usuário, é mais facilmente transmitida adiante do que a informação real, criando o cenário ideal para campanhas de desinformação, que podem ser orquestradas por grupos de interesse específico ou até mesmo agentes políticos, de modo a influenciar a opinião pública.

Soma-se esse contexto à utilização de outras tecnologias como o uso de *bots*, para amplificar a disseminação de informações distorcidas, ou até mesmo para a coleta de informações pessoais através das redes, como o uso da técnica de *web scraping*, que nada mais é do que a raspagem de informações da internet para sua análise, com a construção de bancos de dados estruturados e desenvolvimento de perfil dos usuários.

Em âmbito político, essa atividade pode ser utilizada de forma prejudicial, como a disseminação de fatos distorcidos ou informações falsas para que opositores políticos sejam desacreditados, afetando severamente o debate público.

Essa ação pode ser potencializada através da técnica de *microtargeting*, no qual anúncios políticos podem ser direcionados especificamente para públicos segmentados com mensagem personalizadas, reforçando ainda mais crenças pré-existentes dos usuários, inserindo-os em bolhas de in-

formações e reduzindo a sua propensão ao debate e o contato com visões divergentes de mundo.

De modo geral, todos nós acreditamos possuir controle sobre a nossa própria vontade, contudo técnicas de manipulação, por sua própria natureza, são sutis e geralmente indetectáveis à vítima. Podemos traçar paralelo com a engenharia social, voltada a promover influência psicológica sobre indivíduos, explorando vulnerabilidades humanas como as crenças pessoais, de modo que tomem decisões ou realizem ações que não fariam de outro modo, beneficiando o atacante.

O Brasil tem vivenciado esse contexto na medida em que grandes campanhas de desinformação realizadas de tempos em tempos passaram a impactar diretamente sobra a confiança nas instituições democráticas. Nesse sentido, estudos sugerem que esse modelo de manipulação algorítmica pode impactar na confiança dos usuários em relação a veracidade das informações que consomem, comprometendo a legitimidade do debate político e o desenvolvimento da democracia[89].

Existem ainda diversos outros elementos que somam para o estado atual das coisas dentro do campo tecnológico como a utilização de dados pessoais e influenciadores digitais, havendo especial atenção à inteligência artificial generativa, que detém capacidade de criar conteúdo ainda mais personalizado, como as *deepfakes*, capazes de replicar voz e aparência de pessoais reais, elevando ainda mais o nível de preocupação sobre as informações que trafegam na rede.

Para o funcionamento de todos esses contextos exis-

8 Tucker, J. A., et al. (2018). Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature. SSRN. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139>. Acesso em: 21 set. 2024.

9 Lazer, D. J., et al. (2018). The Science of Fake News. Disponível em: <https://scholar.harvard.edu/files/mbaum/files/science_of_fake_news.pdf>. Acesso em: 21 set. 2024.

te um elemento essencial em todos eles, os dados pessoais, sem qual não é possível a personalização das campanhas e o consequente atingimento do seu objetivo, que é alcançar e compelir indivíduos a adotarem determinada ação, tronando a privacidade e a segurança dos dados pessoais um elemento central no estado atual das coisas.

Por fim, podemos concluir que o estado atual da tecnologia representa um desafio sem precedente à sociedade como um todo, pois o seu rápido desenvolvimento está nos conduzindo a contextos inexplorados e com resultados desconhecidos, enquanto legisladores e a comunidade acadêmica buscam soluções para tais questões.

Necessário mencionar ainda, que todas essas tecnologias não servem essencialmente e exclusivamente para prejuízo da sociedade, havendo espaço para grandes inovações e maior aproximação entre as pessoas, contudo a sua utilização de forma mal-intencionada por diversos atores da sociedade, tem reverberado de modo preocupante na coletividade.

4. LEGISLAÇÃO

Diante desse cenário, tanto o legislador quanto o Poder Judiciário vêm enfrentando desafios significativos impostos pela acelerada evolução da tecnologia, em especial relativo ao uso de redes sociais e serviços de comunicação no contexto das campanhas eleitores em meio digital, obrigando à criação de regras para a mitigação do uso irrestrito das mencionadas tecnologias.

Para tanto, algumas legislações podem ser relacionadas, como a Lei das Eleições, o Código Eleitoral, a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet e a Resolução TSE n° 23.610/19, que são os alicerces principais do ordenamento em relação à campanha eleitoral em meio digital.

O Código Eleitoral, Lei n° 4.737/65, muito embora seja uma norma anterior ao surgimento da própria internet, o mesmo vem sendo atualizado ao longo dos anos de modo a incorporar

a nova realidade dos meios de comunicação, como é o caso do artigo 323, incluído pela Lei n° 14.192/21[10], que trata da disseminação de informações inverídicas com aumento de pena em caso de cometimento através dos meios digitais, conforme a redação do artigo 323[11].

Outros artigos do código ainda possuem aplicação efetivas a condutas exercidas em meio virtual, muito embora não o tragam explicitamente em seu texto, como é o caso das redações: do artigo 243, que estabelece normas gerais sobre a propaganda eleitoral com a proibição de prática que possam ser prejudiciais à sociedade; do artigo 222, que trata da possibilidade de anulação da votação quando houver emprego de meios de propaganda proibidos por lei; e do artigo 237, que estabelece condições sobre a interferência de poder econômico e o desvio ou abuso de poder de autoridade que possam comprometer as eleições.

Contudo, a maior parte das regras que delimita o desenvolvimento da propaganda eleitoral em meio digital encontra-se respaldada através da Lei das Eleições, Lei n° 9.504/97, que detém seção própria para o tema, através dos artigos 57-A ao 57-I, e da Resolução TSE n° 23.610/19, que trata o tema especificamente.

A Lei das Eleições regulamenta aspectos como o início da propaganda eleitoral na internet, que se dá a partir do dia 16 de

10 BRASIL. Lei n° 14.192, de 04 de ago. de 2021. Estabelece normas para prevenir, reprimir e combater a violência política contra a mulher e altera a Lei n° 4.737, de 15 de julho de 1965 (Código Eleitoral). Diário Oficial da União, Brasília, DF, 04 ago. 1965. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14192.htm#art4>. Acesso em: 21 set. 2024.

11 BRASIL. Lei n° 4.737, de 15 de jul. de 1965. Institui o Código Eleitoral. Art. 323. Divulgar, na propaganda eleitoral ou durante período de campanha eleitoral, fatos que sabe inverídicos em relação a partidos ou a candidatos e capazes de exercer influência perante o eleitorado: [...] § 2º Aumenta-se a pena de 1/3 (um terço) até metade se o crime: I - é cometido por meio da imprensa, rádio ou televisão, ou por meio da internet ou de rede social, ou é transmitido em tempo real. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4737.htm. Acesso em: 21 set. 2024.

agosto do ano eleitoral[12], sendo vedada qualquer tipo de publicidade antes dessa data, além de delimitar os veículos permitidos, tais como: site oficial do candidato, partido ou coligação; blogs; redes sociais; e aplicativos de mensagens instantâneas, desde que respeitem as regras eleitorais e estejam devidamente identificados, com endereço eletrônico comunica à Justiça Eleitoral.

O artigo 57-B ainda traz importante regramento em relação ao uso adequado do impulsionamento de conteúdo, tendo como um dos pontos principais a obrigação de que o provedor de aplicação utilizado para a veiculação de propaganda deva estar localizado em território brasileiro, garantindo que a Justiça Eleitoral detenha jurisdição para a efetiva fiscalização da campanha digital.

Além disso, o mencionado artigo também veda o impulsionamento de conteúdo por pessoais naturais, inclusive jurídicas, restringindo essa atividade apenas para os candidatos, partidos e coligações.

Essas restrições representam medidas capazes de garantir a eficácia das decisões da Justiça Eleitoral, que em se tratando de ambiente virtual é questão tormentosa, além de mitigar a disseminação de informações por terceiros, constituindo alguma forma de controle na utilização das redes sociais para fins eleitorais, coibindo práticas abusivas como o financiamento de propaganda por via indireta.

O código ainda faz paralelo com o Marco Civil da Internet[13], ao assegurar que os provedores de aplicação apenas serão responsabilizados após o descumprimento de ordem judicial[14], de modo que seja possível assegurar a liberdade de expressão e

12 BRASIL. Lei n° 9.504/97, de 30 de set. de 1997. Estabelece normas para as eleições. Art. 57-A. Diário Oficial da União, Brasília, DF, 22 set. 2018.

13 BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Art. 19. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

14 BRASIL. Lei n. 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. Art. 57-F. Diário Oficial da União, Brasília, DF, 1º out. 1997.

afastar a censura prévia.

Contudo, a Resolução TSE n° 23.610/19 oferece maior definição sobre a propaganda eleitoral, incluído o uso da internet, regulamentando a divulgação da propaganda eleitoral em plataformas online, como redes sociais, sites e aplicativos de mensagens, além de estabelecer regras para o impulsionamento de conteúdo, de modo a garantir a transparência através da identificação dos candidatos, partidos e coligações, além de estabelecer regras para a sua execução.

Uma das principais questões diretamente ligada a expressão através da internet, é a sua execução de forma anônima, vez em que usuários mal-intencionados podem se utilizar de contas falsas para a disseminação de conteúdo prejudicial, como informações inverídicas ou expressão de ofensas. Assim, uma das vedações que a resolução traz é o anonimato, especialmente em relação a veiculação de propaganda eleitoral, no qual estabelece que os conteúdo publicados devem ser expressamente atribuídos a seus responsáveis.

Outro mecanismo virtual regulamentado pela resolução, é a priorização paga de conteúdo em aplicativos de busca, possibilitando que a campanha se utilize da ferramenta para benefício da candidatura, possibilitando a disseminação de informações a respeito do candidato, mas com expressa vedação em relação promoção de conteúdo negativo de outros candidatos e adversários, de modo que a ferramenta sirva para impulsionar a candidatura e não como arma para ataque ou disseminação de informações inverídicas.

A contratação de pessoas físicas para a divulgação de produto e conteúdo em seus perfis, é uma prática comum no ambiente virtual, sendo muito utilizado por empresas para a promoção da sua marca, contudo a resolução veda a contratação desses meios para a divulgação de propaganda eleitoral, incluído pessoas jurídicas.

Para além da utilização das redes sociais, outra ferramenta poderosa de comunicação da atualidade são os aplicativos de

mensagens, que poderão ser utilizados pelas campanhas, mas não de modo irrestrito, devendo haver a identificação de quem remete a comunicação, além de possibilitar que o destinatário possa requerer a remoção do seu cadastro da lista de contato com a eliminação dos dados pessoais, devendo o remetente atender ao requerimento no prazo de quarenta e oito horas[15].

Considerando a natureza da campanhas eleitorais, bem como o perfil de diversos candidatos, em especial aqueles relacionados aos pleitos municipais, a normativa trouxe importante delimitação sobre o uso do serviços de mensagem, contudo a sua operacionalização em campanhas com menor grau técnico e financeiro poderá ficar obstado, demandando maior fiscalização para o seu cumprimento.

Contudo, a norma possibilita que mensagens enviadas de modo consensual por pessoa física, na figura do apoiador legítimo da candidatura, de forma privada ou em grupos restritos, não estão submetidos a mencionada restrição, beneficiando campanhas de candidatos que já tenham alguma base de eleitor.

Outro fenômeno que cresceu significativamente com o desenvolvimento das tecnologias, como a inteligência artificial, e se tornou um problema social é a prática do *spam*, que se resumo no bombardeio indiscriminado de ligações e mensagens, realizados por empresas, causando significativos transtornos para os indivíduos.

Essa prática encontra-se prevista na resolução, através do seu artigo 34[16], e veda a utilização de marketing, em qualquer horário, para a realização de propaganda, além de proibir o

15 BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 18 de dezembro de 2019. Dispõe sobre a propaganda eleitoral nas eleições de 2020. Art. 33. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 06 out. 2024

16 BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 18 de dezembro de 2019. Dispõe sobre a propaganda eleitoral nas eleições de 2020. Art. 34. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 06 out. 2024.

disparo em massa de mensagens instantâneas sem o consentimento da pessoa destinatária.

No centro de todo esse sistema os dados pessoais desempenham um papel fundamental na manutenção e funcionamento desse ecossistema digital, tal qual o capital financeiro é essencial para o sistemas bancários, os dados fluem através dos meios digitais como ativo que sustenta os algoritmos e plataformas que executam campanhas de marketing. Na ausência desse valioso recurso, praticamente decretaria o colapso de todos esses sistemas, nivelando a realização de uma campanha digital aos meios tradicionais de mídia.

Para tanto, a Justiça Eleitoral, em conjunto com a Autoridade Nacional de Proteção de Dados (ANPD), não só trouxe o regramento da proteção de dados pessoais para a Resolução 23.610/2019, como cooperou para o desenvolvimento do Guia Orientativo para Aplicação da Lei Geral de Proteção de Dados Pessoais no contexto eleitoral[17], de modo a possibilitar que os agentes de tratamento adotem as medidas adequadas para a salvaguarda dos direitos dos titulares eleitores.

A resolução por sua vez, traz o regramento específico sobre as obrigações dos agentes políticos, adotando regras gerais a partir do seu artigo 10, parágrafos 4° ao 8°, ambos incluídos pela Resolução n° 23.732/2024[18], no qual exige que o tratamento de dados pessoais no contexto de propaganda eleitoral respeite a finalidade pelo qual foram coletados, além de impor que os agentes de tratamento, que nesse contexto são os candidatos, partidos e coligações, disponibilizem canal de fácil acesso para que os

17 BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Aplicação da Lei Geral de Proteção de Dados Pessoais por Agentes de Tratamento no Contexto Eleitoral. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf>. Acesso em: 06 out. 2024.

18 BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 30 de maio de 2024. Altera a Resolução TSE nº 23.610/2019, que dispõe sobre propaganda eleitoral. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em: 06 out. 2024.

eleitores possam exercer seu direito de conhecimento sobre o tratamento de dados pessoais e demais direitos, como oposição e até eliminação das informações pessoais.

A mencionada obrigação inevitavelmente obriga a constituição de um encarregado de dados, que é a ponte entre o agente de tratamento, o titular e a ANPD, podendo haver a centralização dessas atividades em um encarregado de dados por partidos e coligações.

Para além do acesso facilitado e da constituição do encarregado de dados, a resolução ainda estabeleceu que os provedores de aplicação informem de modo claro aos usuários sobre a possibilidade de tratamento de dados para fins de propaganda eleitoral, de acordo com as peculiaridades de cada plataforma, devendo haver a identificação de toda a publicidade eleitoral.

De mesmo modo, também restou definida as responsabilidades dos provedores, candidatos e partidos em relação ao tratamento de dados pessoais no contexto eleitoral, no qual devem garantir acesso facilitado às informações sobre o uso dos dados pessoais e adotar medidas de segurança eficazes para proteger as informações, além da incumbência de notificar incidentes de segurança às autoridades e aos titulares afetados.

Verifica-se a atribuição da responsabilidade aos agentes de tratamento pelo uso dessas informações, devendo esses atores fiscalizar os serviços contratados e garantir o atendimento das obrigações previstas na LGPD, bem como garantir o cumprimento dos direitos dos titulares.

Uma das inovações mais importantes para as eleições de 2024, é a constituição do registro de tratamento de dados que partidos e candidatos devem adotar, atribuindo a obrigação de conter os detalhes, como tipo de dados, origem, finalidade e medidas de segurança adotadas[19]. A constituição de inventário de dados

19 BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 18 de dezembro de 2019. Dispõe sobre a propaganda eleitoral nas eleições de 2020. Art. 33-C. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 06 out. 2024.

poderá revelar tratamentos de alto risco, o que poderá conduzir à elaboração do Relatório de Impacto à Proteção de Dados, em especial nas eleições de cargos com maior relevância, como presidente, governador, senador e prefeitos de capitais, podendo o registro exigido pela Justiça Eleitoral[20].

Estipuladas as delimitações para o uso de dados pessoais para as campanhas, a ANPD disponibilizou o Guia Orientativo para o tratamento de dados no contexto eleitoral, que define de modo mais específico a definição dos agentes de tratamento nesse contexto e das bases legais cabíveis, como: o consentimento[21]; a obrigação legal[22]; e o legítimo interesse[23].

O guia ainda disponibiliza informações práticas para o desenvolvimento das medidas de proteção de dados pelos agentes de tratamento, como a prestação de contas, transparência, prevenção e segurança.

5. CONCLUSÕES

Diante do contexto esmiuçado, resta evidente a necessidade de intervenção dos poderes estatais para a regulamentação dos meios digitais nas campanhas eleitorais,

20 BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 18 de dezembro de 2019. Dispõe sobre a propaganda eleitoral nas eleições de 2020. Art. 33-D. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 06 out. 2024.

21 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral. Brasília, 2021. p. 21. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf>. Acesso em: 06 out. 2024

22 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral. Brasília, 2021. p. 26. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf>. Acesso em: 06 out. 2024

23 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral. Brasília, 2021. p. 27. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf>. Acesso em: 06 out. 2024

de modo a assegurar que a inovação tecnológica seja incorporada de maneira responsável, mitigando abusos e desvios na finalidade dessas ferramentas.

Tecnologias como assistentes virtuais, *microtargeting*, plataformas de *crowdsourcing*, direcionamento de conteúdo, redes sociais e diversas outras, não necessariamente são prejudiciais, pois são ferramentas que servem para serem utilizadas, tendo como questão fundamental como é feito o seu uso.

É exatamente nesse ponto que entra a necessidade de regulamentação, pois tanto as empresas por trás desses sistemas quanto os usuários que as utilizam na ponta, possuem percepções diferentes sobre o próprio objetivo dessas ferramentas, inclusive motivações diferentes, motivo pelo qual nos encontramos no atual estado das coisas, em que democracias aparentemente estão ruindo, enquanto sistemas autoritários ascendem, e tudo isso está diretamente ligado ao exercício democráticos nas redes, em outras palavras, nas campanhas eleitorais que definirão o futuro das nações.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral. Brasília, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf>. Acesso em: 06 out. 2024.

BARROSO, Luís Roberto. A democracia sob pressão: o que está acontecendo no mundo e no Brasil. CEBRI, 2023. Disponível em: <https://cebri.org/revista/br/artigo/23/a-democracia-sob-pressao-o-que-esta-acontecendo-no-mundo-e-no-brasil>. Acesso em: 15 set. 2024.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 18 de dezembro de 2019. Dispõe sobre a propagan-

da eleitoral nas eleições de 2020. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 06 out. 2024.

COMSCORE. Um olhar em Social media – Insights 2023 x 2024. COMSCORE, 2024. Disponível em: <https://www.comscore.com/por/Insights/Apresentacoes-e-documentos/2024/Um-olhar-em-Social-media-Insights-2023-x-2024>. Acesso em: 16 set. 2024.

DAHL. Robert A. Sobre a Democracia. Tradução de Beatriz Sidou. Brasília: Editora Universidade de Brasília, 2001.

DIAMOND, Larry. Democracy in Retreat: The Revolt of the Middle Class and the Worldwide Decline of Representative Government. Stanford University, 2024. Disponível em: <https://www.v-dem.net/en/news/democracy-in-retreat>. Acesso em: 15 set. 2024.

FREEDOM HOUSE. Global Freedom Status. Disponível em: <https://freedomhouse.org/explore=-the-map?type-fiw&year=2024>. Acesso em: 15 set. 2024.

LAZER, D. J.; et al. The Science of Fake News. 2018. Disponível em: <https://scholar.harvard.edu/files/mbaum/files/science_of_fake_news.pdf>. Acesso em: 21 set. 2024.

TUCKER, J. A.; et al. Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature. SSRN, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139>. Acesso em: 21 set. 2024.

RESPONSABILIDADE DAS PLATAFORMAS DIGITAIS: MODERAÇÃO DE CONTEÚDO ELEITORAL E O PAPEL DAS REDES SOCIAIS

Silvio Maciel e Silva Junior[1]

1. INTRODUÇÃO

Nos últimos anos, as plataformas digitais, especialmente as redes sociais, tornaram-se arenas centrais para o debate político e eleitoral. Com a crescente digitalização das campanhas e do engajamento cívico, essas plataformas assumiram um papel significativo na disseminação de informações, e, infelizmente, de desinformações.

Diante desse cenário, a responsabilidade das plataformas em moderar conteúdo eleitoral tornou-se um dos principais temas de debate tanto no Brasil quanto em várias partes

1 Advogado com certificações da ***EXIN Privacy and Data Protection Essentials based on LGPD (PDPE LGPD)*** e da **CertiProf Fundamentos Na Lei Geral De Proteção De Dados LGPDF™**. Analista de Proteção de Dados Pessoais e de Direito Digital da Empresa Municipal de Informática S.A. (IPLANRIO) e da Secretaria Municipal de Integridade, Transparência e Proteção de Dados / SMIT (órgão responsável pela implementação da LGPD no Município do Rio de Janeiro). Consultor Especialista de LGPD e de Direito Digital da Empresa TechWise.Rio. Pós-graduado LL.M em Proteção de Dados: LGPD & GDPR pela FACULDADE DE DIREITO - UNIVERSIDADE DE LISBOA (PORTUGAL) e pela FUNDAÇÃO ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DO RIO GRANDE DO SUL – FMP. Pós-graduado *Lato sensu* em Direito Digital pela FUNDAÇÃO ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DO RIO GRANDE DO SUL – FMP). Pós-Graduação *Lato Sensu* em LGPD, Privacidade e Proteção de Dados pela Universidade Cândido Mendes. Pós-Graduado *Lato Sensu* em Direito Processual Civil na Universidade Candido Mendes. Pós–Graduado *Lato sensu* em Processo Civil e Processo do Trabalho na Universidade Veiga de Almeida. Pós-Graduado *lato sensu* em Direito Privado na Universidade Gama Filho. Bacharelado em Direito na Faculdade Moraes Júnior (Faculdade Presbiteriana Mackenzie Rio). Atualmente, cursando MBA em Governança Pública da ESCOLA BRASILEIRA DE DIREITO (EBRADI). Contato: https://www.linkedin.com/in/silvio-jr

do mundo.

Neste contexto, Yuval Noah Harari[2] afirma, com propriedade que, ao invés de alocar recursos em estratégias de autocorreção que favorecessem a propagação da verdade, as grandes plataformas de redes sociais criaram sistemas inovadores que intensificam equívocos, premiando inverdades e fantasias.

Neste trabalho, será destacado o desafio específico gerador da problemática, objeto de pesquisa qualitativa, exploratória e aplicada, com posterior análise interpretativa documental, a ser feita neste artigo. O objetivo é entender de que maneira o ordenamento jurídico pátrio pode contribuir para a mitigação dos riscos relativos à propagação de desinformação eleitoral e de discursos de ódio nas redes sociais.

Para tanto, nos itens a seguir, serão apresentadas uma breve contextualização sobre as plataformas digitais, bem como as iniciativas de regulamentação ocorridas no Brasil e Europa, para, posteriormente, adentrar à temática quanto à responsabilidade destes atores de proceder à moderação de conteúdo eleitoral, além de consignar quais os papéis das redes sociais neste campo.

2. PLATAFORMAS DIGITAIS – REDES SOCIAIS

Previamente, é forçoso apresentar um breve contexto sobre as plataformas digitais, a fim de indicar uma definição deste ator central da problemática a ser estudada neste artigo. Segundo lições de Roberta Battisti[3],

---

2 HARARI, Yuval Noah. **Nexus: Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial.** Tradução: Berilo Vargas e Denise Bottmann. 1 . ed. São Paulo : Companhia das Letras, 2024. P. 271.

3 BATTISTI, Roberta. **Regulação das Big Techs**. São Paulo: Grupo Almedina, 2023. *E-book.* ISBN 9786556277707. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556277707/. Acesso em: 13 set. 2024. P. 45/46.

> as plataformas não são uma novidade introduzida pelo ambiente digital; são, na verdade, antigas formas de negócio utilizadas nos mais diversos setores da sociedade, como, por exemplo, no mercado romano, em casas de leilões, bazares, listas telefônicas ou shopping centers. No século XX, as indústrias utilizavam-se do modelo linear de negócio, no qual a criação do valor ocorre na criação de bens ou serviços, que são posteriormente vendidos para um cliente. (...) As antigas plataformas tornaram-se digitais à medida que vivenciamos a reconfiguração da economia capitalista durante a explosão informacional-tecnológica da Quarta Revolução Industrial.

Assim, as plataformas digitais se tornaram um modelo de negócio tão poderoso a ponto de criar um "capitalismo de plataforma"[4] como um espaço em que empresas se utilizam cada vez mais de *big data* e algoritmos eficientes para dominar o espaço e majorar seus lucros.

José Van Dijck, Thomas Poell e Martijn de Waal apontam o fenômeno acima descrito como a "plataformização da sociedade", em que as plataformas passam a ser produtoras das estruturas sociais em que a sociedade vive na atualidade, e, neste contexto, "as *big techs* assumem cada vez mais posições de poder para mediar as mais diversas interações de nossa vida cotidiana[5]".

Desta maneira, as interações econômicas e sociais ocorrem por intermédio de uma infraestrutura digital que

---

4 Autores citados por Roberta Battisti *in* **Regulação das Big Techs,** 2023, que cunharam essa expressão: SRNICEK, Nick. **Capitalismo de plataformas**. Buenos Aires: Caja Negra, 2018. MARCIANO, Alain; NICITA, Antonio; RAMELLO, Giovanni Battista. **Big data and big techs: understanding the value of information in platform capitalism**. European Journal of Law and Econo-mics, v. 50, n. 3, p. 345–358, 2020. DOI: 10.1007/s10657-020-09675-1. MOAZED, Alex; JOHNSON, Nicholas L. **Modern monopolies: what it takes to dominate te 21st century economy**. New York: St. Martin's Press, 2016.

5 *Apud* BATTISTI, Roberta. **Regulação das Big Techs**. São Paulo: Grupo Almedina, 2023. *E-book.* ISBN 9786556277707. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556277707/. Acesso em: 13 set. 2024. P. 48.

é globalmente interconectada, podendo ser citados como exemplos, na primeira onda, a *Google, Amazon, Microsoft, Yahoo,* e, em uma onda mais recente, X, *LinkedIn, Facebook, Uber, Airbnb*. Ainda segundo a autora Roberta Battisti,

> o modelo de negócio de plataforma digital faz com que as empresas atuem em múltiplos lados, gerando ecossistemas e produzindo efeitos de redes, e daí resulta parte de sua dominação econômica. Mas para além disso, veremos que, dentro desse ecossistema, vão se gerando novos conglomerados e plataformas dentro de plataformas, como é o caso, por exemplo, de algumas *big techs*, que, ao exercerem a função de intermediadoras de conteúdo, assumem o poder de informar e o poder cívico – desempenhando um papel importante na organização das sociedades e assumindo uma espécie de dominação política.

No final das contas, é possível notar que em geral, as plataformas têm como objetivo conectar indivíduos e organizações em um propósito comum. Neste contexto, a professora Ana Frazão[6] leciona que "as plataformas são um modelo de negócio próprio que possibilita a criação de sistemas de interações escaláveis, com efeitos de rede e de conectividade".

Apesar de não haver consenso sobre a definição do termo plataformas digitais, é possível indicar a apresentada por Jonas Valente[7]:

> [...] mais do que apenas intermediários, as plataformas operam uma mediação ativa e que se expande por cada vez mais atividades

6 FRAZÃO, Ana. **Plataformas digitais e os desafios para a regulação jurídica**. *In*: Parentoni, Leonardo (Coord.); Gontijo, Bruno Miranda; Lima, Henrique Cunha (Orgs). **Direito, tecnologia e inovação**. Belo Horizonte: D'placido. 2018. p. 635-699.

7 LIMA, Marcos Francisco Urupá Moraes; VALENTE, Jonas Chagas Lucio. **Regulação de plataformas digitais: mapeando o debate internacional**. Liinc em Revista, v. 16, n. 1, e5100, maio 2020. DOI: 10.18617/liinc.v16i1.5100. Disponível em: https://revista.ibict.br/liinc/article/view/5100/4650. Acesso em: 13 set. 2024.

> sociais. As plataformas digitais são sistemas tecnológicos que funcionam como mediadores ativos de interações, comunicações e transações entre indivíduos e organizações operando sobre uma base tecnológica digital conectada, especialmente no âmbito da Internet, provendo serviços calcados nessas conexões, fortemente lastreados na coleta e processamento de dados e marcados por efeitos de rede.

Desta maneira, nos dizeres de Roberta Battisti[8], "por de trás da interface dessas ferramentas sociais, existe um sistema complexo e estruturado que molda a forma como vivemos e nos organizamos socialmente". Ainda segundo a autora[9], "no mercado das plataformas digitais, mais usuários significa mais dados", sendo que "o uso de *big data*[10] é essencial para tornar as empresas mais rápidas e poderosas".

Desta feita, nas palavras Srnicek[11],

> o diferencial das plataformas para um modelo tradicional de negócio se dá em razão de fornecerem uma infraestrutura básica para mediar diferentes grupos, assim ela se posiciona entre os usuários e se torna o "terreno" em que as atividades acontecem, podendo operar em qualquer lugar em que haja interação digital.

---

8 BATTISTI, Roberta. **Regulação das Big Techs**. São Paulo: Grupo Almedina, 2023. *E-book.* ISBN 9786556277707. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556277707/. Acesso em: 13 set. 2024. P. 50.

9 Idem, P. 57.

10 "Uma das principais diferenças entre dados em geral e da *big data* é o valor do tempo, pois ser capaz de processar uma grande quantidade de dados em tempo real é muito mais valioso do que apenas ter acesso a eles; assim, as empresas melhoram a eficiência de produção, preveem tendências de mercado, melhoram a tomada de decisões e aumentam a segmentação do consumidor por meio de publicidade direcionada e recomendações personalizadas". (OCDE. **Data-Driven Innovation: Big Data for Growth and Well-Being**. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en. Acesso em: 16 set. 2024.

11 *Apud* BATTISTI, Roberta. **Regulação das Big Techs**. São Paulo: Grupo Almedina, 2023. *E-book.* ISBN 9786556277707. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556277707/. Acesso em: 13 set. 2024. P. 61.

Embora não haja consenso sobre a definição de plataformas digitais, buscou-se apresentar um exemplo. Vale destacar que as *big techs*, hoje, exercem um crescente poder para mediar diversas interações na vida cotidiana.

Na contemporânea era da informação, caracterizada pela plataformização da *internet* e pela transição das atividades diárias para o ambiente digital, a definição de provedores de aplicação, estabelecida na Lei Nº 12.965, de 23 de abril de 2014, Marco Civil da Internet – MCI[12]), alcançou um nível tão amplo que passou a incluir, sob um único conceito, uma variedade de serviços distintos, como redes sociais, motores de busca, aplicativos de mensagens instantâneas, armazenamento em nuvem, jogos, serviços de hospedagem, comércio eletrônico e marketplaces, entre outros.

Essa falta de distinção conceitual tem gerado, progressivamente, sérios desafios e dúvidas, como exemplificado na discussão acerca da interpretação do artigo 19 do MCI pelo Supremo Tribunal Federal. Este dispositivo é fundamental no debate sobre a responsabilidade dos provedores de aplicações, principalmente em relação a danos causados por conteúdos oriundos de terceiros.

Nos últimos anos, a regra do artigo 19 do MCI tem sido debatida no Brasil através de três principais frentes[13].

A primeira delas é o Projeto de Lei 2630/2020, que

12 No Brasil, o Marco Civil da Internet, prevê no artigo 19, a responsabilização da plataformas da seguinte maneira: "O provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário". BRASIL, LEI Nº 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 01 out. 2024.

13 De acordo com o Parecer elaborado pelo Professor Ricardo Campos e anexado em 03/10/2024 nos autos do RE 1.037.396. BRASIL. STF. Disponível em https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5160549. Acesso em 05 out. 2024.

institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, conhecido como "PL das *Fake News*", visa impor mais deveres e responsabilidades para as empresas e estabelece novas diretrizes para a responsabilização dos provedores.

A segunda se refere à reforma do Código Civil, que, segundo um relatório da Subcomissão de Direito Digital, busca revogar a norma do Marco Civil da Internet para introduzir novas possibilidades de responsabilização.

Por último, desde 2017, o STF está avaliando a (in) constitucionalidade deste dispositivo, em dois casos que possuem repercussão geral: os Recursos Extraordinários (REs) nº 1.057.258 (Tema 533), sob a relatoria do Ministro Luiz Fux, e nº 1.037.396 (Tema 987), com relatoria do Ministro Dias Toffoli.

O Tema 533, sob a responsabilidade do ministro Fux, aborda a obrigação das empresas que hospedam conteúdo na *internet* de vigiar e remover materiais considerados inadequados sem a necessidade de uma decisão judicial. Em contrapartida, o Tema 987, sob a condução do ministro Toffoli, analisa a conformidade constitucional da exigência de uma ordem judicial específica e prévia para a exclusão de conteúdo, um ponto crucial para a responsabilização civil dos provedores em relação a ações ilícitas praticadas por terceiros.

Em síntese, ambos discutem a obrigação dos provedores em relação ao conteúdo criado pelos usuários e a opção de retirar materiais que ofendam direitos pessoais, promovam ódio ou espalhem informações falsas, com base em reclamações ou notificações extrajudiciais.

Um aspecto crucial do debate tem sido negligenciado: a necessidade urgente de diferenciar conceitualmente os provedores de aplicação de *internet*. O MCI ao definir no artigo 5º, "conexão à internet" (inciso V) e "aplicações de internet" (inciso VII), distingue "provedores de conexão" (geralmente empresas de telecomunicações) e "provedores

de aplicações" (abrangendo diversos modelos de negócios digitais).

No entanto, ao utilizar um termo único para se referir a setores econômicos digitais com características distintas, o MCI acaba por tratá-los de forma homogênea, o que gera desafios significativos na aplicação prática de suas normas.

A legislação brasileira, baseada em instrumentos regulatórios do início do século XXI, nasceu, de certa maneira, desatualizada em certos aspectos, incluindo o reconhecimento das particularidades dos diferentes modelos de negócios digitais, os quais foram apresentados anteriormente.

Ora, ao agrupar diversos intermediários como redes sociais, ferramentas de busca e *marketplaces*[14] sob a mesma categoria, o MCI cria obstáculos para a correta identificação dos direitos dos usuários e dos deveres correspondentes das plataformas no ambiente digital. Embora compartilhem o papel de intermediários na *web* (e sejam classificadas genericamente como "provedores de aplicação" pelo MCI), plataformas como redes sociais, buscadores, serviços de streaming e marketplaces têm objetivos e funções distintos, refletindo as diversas necessidades de seus usuários.

É de se ressaltar que debates semelhantes já foram realizados no contexto brasileiro, antes mesmo da implementação do MCI.

Em 2010, no julgamento pela Terceira Turma do

14 Os *marketplaces* desempenham uma função específica, à medida que foram desenvolvidos para otimizar as transações comerciais entre quem compra e quem vende. Desta feita, não organizam nem atuam como curadores das ideias veiculadas, mas sim centralizam o procedimento de compra e venda de produtos e serviços, tornando mais simples etapas como a gestão de pagamentos e, em determinadas situações, a logística. A concepção dessas plataformas busca estabelecer um espaço prático e eficaz para a realização de negócios, possibilitando que os vendedores atinjam uma grande audiência e que os compradores descubram mercadorias de diferentes fornecedores em um só lugar. Assim, a vivência do usuário é, essencialmente, envolvendo transações econômicas, com ênfase em fatores como a diversidade de produtos, a comparação de preços e o fechamento das compras.

STJ do REsp nº 1193764 SP 2010/0084512-0, de relatoria da Ministra Nancy Andrighi, foi reconhecido cinco tipos de provedores (intermediários): (i) os de infraestrutura ou *backbone*, que possuem a rede com capacidade para processar grandes volumes de informação; (ii) os de acesso, que utilizam a estrutura dos *backbones* para revender ao consumidor; (iii) os de hospedagem, que armazenam dados de terceiros; (iv) os de informação, que geram conteúdos divulgados *online*; e (v) os de conteúdo, que disponibilizam na *internet* as informações criadas ou desenvolvidas por provedores de informação.

Destarte, no REsp. nº 1.383.354/SP, o STJ já reconhecia a diferença entre os intermediários *online* e, com base nessa distinção, aplicava um conjunto específico de direitos e deveres. A Corte decidiu que não existe a obrigação de verificar a origem de todos os produtos vendidos por terceiros através de plataformas online, uma vez que essa responsabilidade extrapolaria as funções normais do serviço de intermediação. No entanto, isso não isenta esses provedores da responsabilidade de oferecer meios para que o consumidor possa encerrar a compra caso suspeite da qualidade do produto.

No que tange às redes sociais, Ricardo Campos e Rony Vainzof[15] lecionam que,

> Redes sociais, por exemplo, são construídas em torno da ideia de compartilhamento de informações e interação social, permitindo aos usuários compartilhar uma variedade de conteúdos, incluindo textos, fotos, vídeos e mensagens pessoais.

Nesse contexto, o propósito dessas plataformas é promover a comunicação e o relacionamento entre indivíduos e

15 CAMPOS, Ricardo, VAINZOF, Rony. **STF, marketplaces e artigo 19 do Marco Civil da Internet**, disponível em: https://www.conjur.com.br/2024-jul-19/stf-marketplaces-e-artigo-19-do-marco-civil-da-internet/. Acesso em 27 set. 2024.

grupos, criando um espaço para expressão pessoal, troca de ideias e engajamento social, como se fosse um grande "mercado de ideias"[16], sendo que para esse propósito, as operações econômicas relacionadas a produtos não são o foco, ainda que a propaganda e o marketing digital exerçam uma função relevante na geração de receita nesses espaços por meio do engajamento e da atenção dos usuários.

Noutro giro, contemporaneamente, o termo "redes sociais" poderia ser conceituado, nas palavras de Regina Maria Marteleto[17], como "um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados". Ao estudar os sites de redes sociais, Tanguy Coenen, Dirk Kenis, Céline Van Damme, and Eiblin Matthys[18] apontam três características essenciais para

16 Segundo o Professor Ricardo Campos em seu Parecer elaborado e anexado em 03/10/2024 nos autos do RE 1.037.396, a noção de "mercado de ideias" remete à metáfora que sugere que as ideias devem competir entre si de forma livre, assim como os produtos em um mercado econômico. A expectativa é que, através dessa competição, a verdade e os melhores argumentos prevaleçam. Esse conceito foi apresentado pelo juiz Oliver Wendell Holmes Jr. em sua opinião dissidente no caso Abrams v. Estados Unidos, que foi decidido pela Suprema Corte dos Estados Unidos em 1919. Durante o julgamento, Holmes defendeu que a liberdade de expressão deveria ser resguardada, pois isso permitiria a troca aberta de ideias, facilitando assim a descoberta da verdade. A metáfora do "mercado de ideias" implica que, em um ambiente de livre intercâmbio, as melhores ideias se destacarão e resistirão, enquanto as menos válidas tenderão a ser descartadas. Esse conceito exerceu uma influência significativa no desenvolvimento da jurisprudência sobre liberdade de expressão não apenas nos Estados Unidos, mas também em outras regiões do mundo. Estados Unidos. Suprema Corte. Abrams v. United States, 250 U.S. 616 (1919). Disponível em: https://supreme.justia.com/cases/federal/us/250/616/. Acesso em: 05 out. 2024.

17 MARTELETO, Regina Maria. **Análise de redes sociais - aplicação nos estudos de transferência da informação.** Disponível em https://www.scielo.br/j/ci/a/6Y7Dyj4cVd5jdRkXJVxhxqN/?format=pdf&lang=pt . Acesso em 29. set. 2024.

18 *In* Knowledge Sharing over Social Networking Systems: Architecture, Usage Patterns and Their Application. Disponível em: https://www.academia.edu/376034/Knowledge_Sharing_Over_Social_Networking_Systems_Architecture_Usage_Patterns_and_Their_Application. Acesso em 29. Set. 2024, citados por CLEMENTI, Juliana Augusto, et al. **Mídias Sociais E Redes Sociais: Conceitos E Características**. Dis-

sites de redes sociais: a) possibilidade de criar grupos; b) rastreamento de conteúdo; c) permitir diferentes perspectivas.

É nítido, portanto, como os diversos tipos de plataformas trazem diferentes riscos e ameaças aos direitos dos usuários no mundo digital, sendo que as redes sociais lidam com desafios consideráveis em relação à moderação de conteúdo, como a propagação de desinformação, discursos de ódio e material extremista.

A relevância desta diferenciação conceitual é tão grande que um importante marco legislativo na Europa que visou diferenciar os provedores de aplicações foi a *Netzwerkdurchsetzungsgesetz* (NetzDG)[19] da Alemanha aprovada em 2017. Com esta norma, a Alemanha emergiu como uma das líderes na discussão sobre a regulação das plataformas digitais, com foco específico nas redes sociais.

Essa legislação é reconhecida como a primeira no mundo a adotar uma abordagem mais severa em relação à responsabilidade dos provedores de serviços *online*, impondo exigências e responsabilidades adicionais àqueles que não agissem com diligência na remoção de conteúdo ilegal, além de estabelecer sanções financeiras, mesmo considerando a proteção garantida pela Diretiva de Comércio Eletrônico da União Europeia, que isentava essas empresas de responsabilidade por conteúdos postados por terceiros, contanto que seguissem certos critérios mínimos.

Portanto, a intenção foi aplicar valores e normas fundamentais do país às plataformas que operam de maneira transnacional e que, em geral, baseiam suas práticas em seus próprios Termos de Serviço[20].

---

ponível em: https://anais.suceg.ufsc.br/index.php/suceg/article/download/80/33/185. Acesso em 29. set. 2024.

19 Disponível em: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Acesso em 05 out. 2024.

20 BELLI, Luca; VENTURINI, Jamila. **Private ordering and the rise of terms of service as cyberregulation**. Internet Policy Review, v. 5, n. 4, p. 1–17, 2019.

Posteriormente, a União Europeia abordou no recém promulgado Regulamento dos Serviços Digitais[21], diretrizes específicas para plataformas digitais (art. 3º, i) e para motores de busca (art. 3º, j). Assim, as normas são estruturadas com base nessa distinção conceitual, reconhecendo e tratando as particularidades e os efeitos de cada tipo de negócio, além de impedir imposições desmedidas e inadequadas.

A fim de lidar com os desafios apresentados pelas redes sociais, a normativa supracitada sugeriu responsabilidades que se focam, em sua maioria, na transparência e na responsabilidade referente ao conteúdo divulgado.

No item a seguir, estas recomendações apresentadas pelas normativas europeias serão analisadas como forma de acrescentar possíveis respostas a este debate tão relevante e atual.

3. RESPONSABILIDADE DAS PLATAFORMAS DIGITAIS (REDES SOCIAIS) DE MODERAÇÃO DE CONTEÚDO ELEITORAL

Antes de adentrar na questão da responsabilidade das redes sociais em moderar o conteúdo de cunho eleitoral, torna-se imperioso abrir um parêntese a fim registrar a diferença conceitual existente entre desinformação e *fake news*.

Conforme guia elaborado pelo TSE[22],

> "a expressão *fake news* é muito conhecida atualmente. Sem embargo, em diversas

21 Jornal Oficial da União Europeia. **REGULAMENTO (UE) 2022/2065 DO PARLAMENTO EUROPEU E DO CONSELHO**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065. Acesso em 29 set. set. 2024.

22 BRASIL. **Tribunal Superior Eleitoral. Guia básico de enfrentamento à desinformação [recurso eletrônico]**. – Brasília: Tribunal Superior Eleitoral, 2022. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/Anexo_2177865_Guia_basico_de_enfrentamento_a_desinformacao_WEB_SEPREVOK.pdf. Acesso em 23 set. 2024.

> ocasiões, resulta empregada de forma imprecisa. vezes, é tratada como sinônimo de "desinformação", indicando, pura e simplesmente, a existência de uma notícia falsa. Em outros casos, é lançada arbitrariamente, diante de qualquer afirmação desagradável, independentemente da procedência ou improcedência de seu conteúdo."

Neste trabalho, a palavra desinformação será tratada como um gênero, que abrange diferentes espécies, como[23]: a) informações falsas transmitidas sem consciência de sua falsidade; b) informações falsas transmitidas com consciência de sua falsidade; c) informações parcialmente verdadeiras, mas de alguma forma manipuladas para causar danos; d) levantamento sistemático de dúvidas fundadas em afirmações, premissas ou dados falsos, com a intenção de causar danos.

Neste contexto, o avanço tecnológico traz consigo o surgimento de novas formas de desinformação, como por exemplo, ferramentas de processamento de linguagem natural têm a capacidade de criar robôs (*bots*) que se comportam nas redes sociais como se fossem usuários reais, visando poluir, dificultar ou influenciar os debates. De maneira semelhante, a inteligência artificial generativa pode ser utilizada para elaborar narrativas fictícias, de maneira coerente e com argumentos altamente persuasivos, tanto em texto quanto em imagens e vídeos sintéticos que são surpreendentemente realistas.

Dentre tantas inovações, uma tem se destacado: a tecnologia utilizada na fabricação dos chamados *deepfakes*. Por oportuno, cite-se definição apontada em recentíssimo

23 Metodologia apresentada no **Guia básico de enfrentamento à desinformação do TSE**. 2022. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/Anexo_2177865_Guia_basico_de_enfrentamento_a_desinformacao_WEB_SEPREVOK.pdf. Acesso em 23 set. 2024.

Guia Ilustrado elaborado pelo STF e Data Privacy[24]:

> A expressão "deepfake" surge da união dos termos "deep" – extraída da tecnologia deep learning, "aprendizado profundo" – e "fake", que significa "falso", em inglês. Não existe uma palavra em português para descrever esse fenômeno. Contudo, em tradução livre as deepfakes nada mais são do que "falsidades profundas", ou seja, conteúdos falsos produzidos com um alto grau de elaboração.

Fecha-se o parêntese aberto para apreciar os detalhes das questões relativas à necessidade de as redes sociais procederem à moderação de conteúdo produzido neste tipo de plataforma.

Nos últimos anos, foi possível observar um aumento significativo na preocupação com a desinformação e discursos de ódios durante períodos eleitorais, podendo citar, de maneira exemplificativa, as últimas eleições ocorridas na América do Sul e dos Estados Unidos.

Max Fisher[25] já havia alertado que

> a tecnologia das redes sociais exerce uma força de atração tão poderosa na nossa psicologia e na nossa identidade, e é tão predominante na nossa vida, que transforma o jeito como pensamos, como nos comportamos e como nos relacionamos uns com os outros. O efeito, multiplicado por bilhões de usuários, tem sido a transformação da própria sociedade.

É incontestável que as redes sociais têm um papel extremamente complexo: ao mesmo tempo em que são espaços para a livre expressão, elas precisam garantir que essa

---

24 Brasil. **Guia Ilustrado Contra as Deepfakes**. Supremo Tribunal Federal; Data Privacy. Brasil. Brasília: STF, Coordenadoria de Combate à Desinformação, 2024. Disponível em https://portal.stf.jus.br/desinformacao/doc/Guia%20ilustrado%20Contra%20DeepFakes_ebook%20(1).pdf. Acesso em 05 out. 2024.

25 FISHER, Max. **A máquina do caos: Como as redes sociais reprogramaram nossa mente e nosso mundo**. Tradução Érico Assis. 1. Ed. São Paulo : Todavia, 2023. p. 21.

liberdade não seja usada para disseminar informações falsas e que possam influenciar indevidamente o processo eleitoral. Essa dualidade tem levado a um debate intenso sobre os limites da moderação de conteúdo.

Se por um lado, a moderação é necessária para proteger o processo democrático, por outro, há o risco de censura excessiva ou enviesada, que poderia suprimir a liberdade de expressão. As plataformas digitais precisam, portanto, encontrar um equilíbrio entre essas demandas conflitantes.

Nas lições irreparáveis dos Professores Chiara Spadaccini De Teffé e Carlos Affonso Souza[26], a

> moderação de conteúdo e responsabilidade civil são duas faces da mesma moeda no debate global sobre regulação das chamadas plataformas digitais. A partir do momento em que o desenvolvimento da Internet permitiu que todos os seus usuários pudessem publicar conteúdos e se comunicar em escala global, surgiu a questão sobre quem responde caso essas manifestações venham a causar danos a terceiros. Além disso, qual seria o regime de responsabilização adequado?

Assim, a moderação de conteúdo eleitoral nas plataformas digitais, em específico as redes sociais, tem se tornado um tema cada vez mais relevante e complexo.

Acerca de possíveis regulamentações sobre o tema, foi possível verificar que o TSE, no âmbito de dos competência, tem se esforçado para editar regras, sendo possível citar, as Resoluções nºs 23.714/2022 e 23.610/2019, esta última com redação dada pela 23.732/2024.

O STF também possui atuação destacada, com decisões firmes a respeito desta temática, pondo citar como exemplo, as decisões havidas na PET 12.404.

---

26 **Moderação De Conteúdo E Responsabilidade Civil Em Plataformas Digitais: Um Olhar Sobre As Experiências Brasileira, Estadunidense e Europeia *in*** MENEZES, Joyceane Bezerra de; BARBOSA, Fernanda Nunes (coord.)**. À prioridade da pessoa humana no Direito Civil-Constitucional: estudos em homenagem a Maria Celina Bodin de Moraes**. Indaiatuba SP : Editora Foco, 2024, p. 25 a 37.

Como visto, a Alemanha aprovou em 2017 uma importante norma que adotou uma abordagem mais rigorosa em relação à responsabilidade dos fornecedores de serviços online, estabelecendo exigências e obrigações extras para aqueles que não se empenhassem adequadamente a remoção de material ilícito, além da previsão de penalidades.

Já a União Europeia promulgou o Regulamento dos Serviços Digitais[27] com regras específicas para plataformas digitais (art. 3º, i) e para motores de busca (art. 3º, j).

A fim de lidar com os desafios apresentados pelas redes sociais, a normativa europeia propôs responsabilidades que se focam, em sua maioria, na transparência e na responsabilidade referente ao conteúdo divulgado[28] (arts. 15 e 24).

Ora, as redes sociais, como plataformas digitais mediadora de atividades sociais, desempenham um papel crucial na formação da opinião pública, por meio da disseminação de informações e desinformações, o que traz consigo uma grande responsabilidade.

Considerando a função dessas empresas na moldagem da opinião pública e na propagação de informações, o Regulamento dos Serviços Digitais destaca, nos artigos 15 e 35, a necessidade de sistemas efetivos de moderação de conteúdo e de uma responsabilidade clara no combate à desinformação e à divulgação de conteúdos ilegais.

Por oportuno, destaca-se a conceituação de moderação de conteúdo trazido por esta norma, em seu art. 3º, t:

27 Jornal Oficial da União Europeia. **REGULAMENTO (UE) 2022/2065 DO PARLAMENTO EUROPEU E DO CONSELHO**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065. Acesso em 29 set. 2024.

28 European Comission. **DSA: Very large online platforms and search engines**. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops. Acesso em 29 set. 2024.

> «Moderação de conteúdos», as atividades, automatizadas ou não, empreendidas por prestadores de serviços intermediários, destinadas em especial a detetar, identificar e combater os conteúdos ilegais ou informações incompatíveis com os seus termos e condições fornecidos pelos destinatários do serviço, incluindo as medidas tomadas que afetam a disponibilidade, visibilidade e acessibilidade desses conteúdos ilegais ou dessas informações, como a despromoção, a desmonetização, a desativação do acesso ou a supressão dos mesmos, ou que afetem a capacidade de os destinatários do serviço fornecerem essas informações, como a cessação ou suspensão da conta de um destinatário;

É importante ressaltar que a regulamentação estabeleceu distintas categorias para plataformas online e motores de busca de grande porte, os quais, por suas peculiaridades em alcance e riscos, requerem uma supervisão e atenção diferenciadas.

Neste contexto, o artigo 35, 1, c, do Regulamento dos Serviços Digitais prevê como atenuação de riscos que

> A adaptação dos processos de moderação de conteúdos, incluindo a rapidez e a qualidade do tratamento das notificações relativas a tipos específicos de conteúdos ilegais e, se for caso disso, a rápida supressão dos conteúdos notificados ou a rápida desativação do acesso aos mesmos, em especial no que respeita aos discursos ilegais de incitação ao ódio ou a ciberviolência, bem como a adaptação de todos os processos de tomada de decisão pertinentes e dos recursos consagrados à moderação de conteúdos;

Assim, com o objetivo de reduzir os riscos, as redes sociais deverão ajustar seus processos de moderação de conteúdos, garantindo agilidade e qualidade no tratamento das notificações referentes a categorias específicas de conteúdos ilegais, e, quando necessário, deverão agir rapidamente para remover os conteúdos denunciados ou desativar o acesso a eles, especialmente no que diz respeito a discursos ilegais que incitem ao ódio ou à violência no ambiente digital.

Além disso, é fundamental que todos os processos de tomada de decisão relacionados e os recursos destinados à moderação de conteúdos sejam adequadamente adaptados.

4. CONCLUSÕES

Desta maneira, foi possível identificar no cenário mundial, uma relevante preocupação com a necessidade de se regulamentar, de maneira mais específica e expressa, a responsabilidade das plataformas digitais, em especial das redes sociais, na moderação de conteúdo eleitoral produzido.

Na Europa, com a implementação do Regulamento dos Serviços Digitais, há certo destaque para a discussão sobre a criação de um sistema de avaliação de conteúdo mais claro e aberto, com a definição de diretrizes que devem ser seguidas por todas as plataformas de grande porte.

Neste contexto, a transparência, a responsabilidade e a liberdade de expressão, como principais pilares da abordagem da Lei de Serviços Digitais (DSA) da União Europeia, apresentam-se como referências basilares para o Brasil criar um ambiente digital integrado[29].

Neste sentido, a norma europeia pode servir como um bom ponto de partida para o Brasil, fornecendo diretrizes básicas para estabelecer um bom equilíbrio entre a manutenção da liberdade de expressão e a adoção de medidas protetivas para divulgação dos detalhes mais influentes da democracia, que é muito forte no ponto de encontrar algo muito importante. Influências externas, bem como o atual ano eleitoral.

Enquanto isso, as discussões no STF sobre a aplicação e a constitucionalidade do artigo 19 do MCI centram-se na responsabilidade dos provedores de aplicações de *internet*,

29 **Moderação De Conteúdo E Responsabilidade Civil Em Plataformas Digitais: Um Olhar Sobre As Experiências Brasileira, Estadunidense e Europeia *in*** MENEZES, Joyceane Bezerra de; BARBOSA, Fernanda Nunes (coord.)**. À prioridade da pessoa humana no Direito Civil-Constitucional: estudos em homenagem a Maria Celina Bodin de Moraes**. Indaiatuba SP : Editora Foco, 2024, p. 25 a 37.

e uma medida relevante a ser observada, é, primeiramente, determinar quais provedores devem realmente estar sujeitos à regulação ou, mais precisamente, à decisão em análise.

Em outras palavras, é necessário regular o princípio da responsabilização dos agentes em função das suas atividades e estabelecer até que ponto cada plataforma digital (rede social) deve cumprir determinadas obrigações, especialmente tendo em conta os riscos concretos e a estrutura do seu modelo de negócio.

O artigo 19 do MCI, tal como tem sido aplicado, pode constituir um obstáculo à verdadeira proteção dos direitos fundamentais, uma vez que serve de base para que as plataformas digitais se eximam em relação a informações claramente com objetivos danosos.

Deste modo, é crucial garantir uma interpretação do artigo 19 em conformidade com a Constituição Federal, que originalmente requer uma ordem judicial para a remoção de conteúdos, permitindo assim que, em certas situações, essa exigência possa ser dispensada.

Vale registrar o alerta feito por Ricardo Campos e Rony Vainzof[30]:

> O risco que se corre hoje com o julgamento do artigo 19 no STF é o de que o Tribunal mire na justa proteção da integridade da informação do mercado de ideias sob curadoria das redes sociais, mas acabe impactando negativamente em indivíduos que utilizam plataformas de comércio eletrônico — quer como espaços de empreendedorismo, quer como alternativa para compras e transações cotidianas —, justamente em razão da indiferenciação conceitual sobre "provedores de aplicações". Um dos desafios para a corte no julgamento das ações sobre o MCI reside, assim, em interpretar e aplicar a Lei de forma que reconheça as especificidades e os

30 CAMPOS, Ricardo, VAINZOF, Rony. **STF, marketplaces e artigo 19 do Marco Civil da Internet**. Disponível em: https://www.conjur.com.br/2024-jul-19/stf-marketplaces-e-artigo-19-do-marco-civil-da-internet/. Acesso em 27 set. 2024.

> modelos de negócios emergentes no ambiente digital, responsabilizando os agentes de acordo com suas atividades. Se considerar experiências internacionais como a do DSA, o STF tem ainda a oportunidade de sinalizar ao legislador nacional um horizonte conceitual que promova uma diferenciação mais precisa entre os diversos tipos de provedores de aplicação.

Em relação à possibilidade de realizar uma moderação de conteúdo eleitoral mais eficaz, através da eliminação de publicações sobre desinformação ou discurso de ódio, independente de ordem judicial prévia, é importante destacar que esta abordagem não representa uma ameaça à liberdade de expressão; pelo contrário, ela fortalece a integridade das informações divulgadas no espaço virtual e contribui para a salvaguarda dos direitos fundamentais, do sistema democrático e da própria liberdade de expressão.

À medida que o Brasil promove novas eleições em outubro de 2024, o debate sobre uma possível inconstitucionalidade deste dispositivo do MCI e uma nova regulamentação do conteúdo *online* se intensifica, especialmente no que diz respeito ao combate à desinformação e discursos de ódio.

A possível declaração de inconstitucionalidade do artigo 19 do MCI poderia abrir caminho para uma regulamentação mais específica e eficaz, alinhada com as melhores práticas internacionais. Isso permitiria a criação de um arcabouço legal que exija das plataformas uma postura mais proativa na moderação de conteúdo, especialmente durante períodos eleitorais, sem, contudo, conferir-lhes poder irrestrito de censura.

Neste cenário, o PL 2.630/20, aparenta ter os mesmos objetivos da Lei de Serviços Digitais (DSA) da União Europeia. Portanto, a relação entre a DSA da UE e o PL 2630/20 pode ser vista como parte da crescente tendência global para uma regulamentação eficaz do espaço digital, sendo que ambas procuram enfrentar desafios semelhantes, embora de maneiras diferentes.

É essencial que este projeto, em sua versão final, incorpore mecanismos de transparência, responsabilidade e devido processo na moderação de conteúdo, inspirando-se nas lições aprendidas com a implementação do Regulamento dos Serviços Digitais na União Europeia.

É notório que a era digital trouxe consigo desafios significativos para a integridade dos processos democráticos, especialmente no que tange à disseminação de desinformação e discursos de ódio em períodos eleitorais. Neste contexto, a responsabilidade das redes sociais na moderação de conteúdo eleitoral emerge como uma questão crucial, que demanda um equilíbrio delicado entre a proteção da liberdade de expressão e a salvaguarda da integridade democrática.

A análise realizada neste estudo revela que a implementação de medidas efetivas de moderação de conteúdo por parte das plataformas digitais não apenas é possível, mas imperativa. Contudo, é fundamental que tais medidas sejam executadas de forma transparente, responsável e proporcional, evitando qualquer semelhança com atos de censura ou limitação indevida do direito à livre expressão.

Por fim, é imperativo reconhecer que a responsabilidade pela integridade do processo democrático não recai exclusivamente sobre as plataformas digitais. Um ecossistema digital saudável e democrático requer o engajamento ativo de múltiplos atores, incluindo o poder público, a sociedade civil, a academia e os próprios usuários. Somente através de um esforço colaborativo e multissetorial será possível construir um ambiente online que promova o debate público construtivo, proteja a liberdade de expressão e, simultaneamente, preserve a integridade dos processos democráticos.

Em última análise, o desafio que se apresenta é o de criar um marco regulatório que responsabilize efetivamente as redes sociais pela moderação de conteúdo eleitoral, sem que isso represente uma ameaça à liberdade de expressão. Este equilíbrio é, não apenas possível, mas essencial para a

saúde de nossa democracia na era digital.

O caminho a seguir deve ser pautado pela busca constante deste equilíbrio, através de uma regulação inteligente, adaptativa e fundamentada em evidências, que coloque os direitos fundamentais e a integridade democrática no centro de suas preocupações.

REFERÊNCIAS

BATTISTI, Roberta. Regulação das Big Techs. São Paulo: Grupo Almedina, 2023. *E-book.* ISBN 9786556277707. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556277707/. Acesso em: 13 set. 2024.

BELLI, Luca; VENTURINI, Jamila. Private ordering and the rise of terms of service as cyberregulation. Internet Policy Review, v. 5, n. 4, p. 1–17, 2019.

BRASIL. Guia Ilustrado Contra as Deepfakes. Supremo Tribunal Federal; Data Privacy. Brasil. Brasília: STF, Coordenadoria de Combate à Desinformação, 2024. Disponível em https://portal.stf.jus.br/desinformacao/doc/Guia%20ilustrado%20Contra%20DeepFakes_ebook%20(1).pdf. Acesso em 05 out. 2024.

BRASIL. PL 2360/202. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983&filename=PL%202630/2020. Acesso em 01 out. 2024.

BRASIL. STF. Pet 12404. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6888934. Acesso em 05 out. 2024.

BRASIL. STF. RE nº 1.037.396. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987.

Acesso em 29. set. 2024.

BRASIL. STF. RE nº 1.057.258 Disponível em: https://portal.stf.jus.br/jurisprudenciarepercussao/verAndamentoProcesso.asp?incidente=5217273&numeroProcesso=1057258&classeProcesso=RE&numeroTema=533. Acesso em 29. set. 2024.

BRASIL. STJ. REsp nº 1193764 SP 2010/0084512-0. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201000845120&dt_publicacao=08/08/2011. Acesso em 29. set. 2024.

BRASIL. STJ. REsp. nº 1.383.354/SP. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201300742989&dt_publicacao=26/09/2013. Acesso em 29. set. 2024.

BRASIL. TSE. Guia básico de enfrentamento à desinformação do TSE. 2022. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/Anexo_2177865_Guia_basico_de_enfrentamento_a_desinformacao_WEB_SEPRE-VOK.pdf. Acesso em 23 set. 2024.

CAMPOS, Ricardo. PARECER anexado em 03/10/2024 nos autos do RE 1.037.396. BRASIL. STF. Disponível em https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5160549. Acesso em 05 out. 2024.

CAMPOS, Ricardo; VAINZOF, Rony. STF, marketplaces e artigo 19 do Marco Civil da Internet, disponível em: https://www.conjur.com.br/2024-jul-19/stf-marketplaces-e-artigo-19-do-marco-civil-da-internet/. Acesso em 27 set. 2024.

Estados Unidos. Suprema Corte. Abrams v. United States, 250 U.S. 616 (1919). Disponível em: https://supreme.justia.com/cases/federal/us/250/616/. Acesso em: 05 out. 2024.

European Comission. DSA: Very large online platforms and search engines. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops. Acesso em 29 set. 2024.

FALBO, Milton Leal. Avaliação Do Modelo De Negócio Marketplace No Varejo Online Brasileiro: Um Estudo De Caso. Miguel Lima, orientador. Niterói, 2021. Disponível em https://app.uff.br/riuff/bitstream/handle/1/32683/TCC%20-%20Milton%20Falbo_Final%20Revisado.pdf?-sequence=1&isAllowed=y . Acesso em 29. set. 2024.

FISHER, Max. A máquina do caos: Como as redes sociais reprogramaram nossa mente e nosso mundo. Tradução Érico Assis. 1. Ed. São Paulo : Todavia, 2023.

FRAZÃO, Ana. Plataformas digitais e os desafios para a regulação jurídica. *In*: Parentoni, Leonardo (Coord.); Gontijo, Bruno Miranda; Lima, Henrique Cunha (Orgs). Direito, tecnologia e inovação. Belo Horizonte: D'placido. 2018. p. 635-699.

HARARI, Yuval Noah. Nexus: Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial. Tradução: Berilo Vargas e Denise Bottmann. 1 . ed. São Paulo : Companhia das Letras, 2024. P. 271.

Jornal Oficial da União Europeia. REGULAMENTO (UE) 2022/2065 DO PARLAMENTO EUROPEU E DO CONSELHO. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065. Acesso em 29 set. set. 2024.

Jornal Oficial da União Europeia. REGULAMENTO (UE) 2022/2065 DO PARLAMENTO EUROPEU E DO CONSELHO. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065. Acesso em 29 set. 2024.

KENIS, Tanguy Coenen, Dirk; DAMME, Céline Van; MATTHYS, Eiblin. Knowledge Sharing over Social Networking Systems: Architecture, Usage Patterns and Their Application. Disponível em: https://www.academia.edu/376034/Knowledge_Sharing_Over_Social_Networking_Systems_Architecture_Usage_Patterns_and_Their_Application. Acesso em 29 set. 2024.

LIMA, Marcos Francisco Urupá Moraes; VALENTE, Jonas Chagas Lucio. Regulação de plataformas digitais: mapeando o debate internacional. Liinc em Revista, v. 16, n. 1, e5100, maio 2020. DOI: 10.18617/liinc.v16i1.5100. Disponível em: https://revista.ibict.br/liinc/article/view/5100/4650. Acesso em: 13 set. 2024.

MARCIANO, Alain; NICITA, Antonio; RAMELLO, Giovanni Battista. Big data and big techs: understanding the value of information in platform capitalism. European Journal of Law and Econo-mics, v. 50, n. 3, p. 345–358, 2020. DOI: 10.1007/s10657-020-09675-1.

MARTELETO, Regina Maria. Análise de redes sociais - aplicação nos estudos de transferência da informação. Disponível em https://www.scielo.br/j/ci/a/6Y7Dyj4cVd5jdRkXJVxhxqN/?format=pdf&lang=pt . Acesso em 29. set. 2024.

MOAZED, Alex; JOHNSON, Nicholas L. Modern monopolies: what it takes to dominate te 21st century economy. New York: St. Martin's Press, 2016.

OCDE. Data-Driven Innovation: Big Data for Growth and Well-Being. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en. Acesso em: 16 set. 2024.

SHIFFRIN, Steven H. The First Amendment, Democracy, and Romance. Princeton: Princeton University Press, 1990.

INGBER, Stanley. “The Marketplace of Ideas: A Legitimatizing Myth.” Duke Law Journal (1984): 1 – 91.

SRNICEK, Nick. Capitalismo de plataformas. Buenos Aires: Caja Negra, 2018.

Teffé, Chiara Spadaccini de; Souza, Carlos Affonso. Moderação De Conteúdo E Responsabilidade Civil Em Plataformas Digitais: Um Olhar Sobre As Experiências Brasileira, Estadunidense e Europeia *in* MENEZES, Joyceane Bezerra de; BARBOSA, Fernanda Nunes (coord.). À prioridade da pessoa humana no Direito Civil-Constitucional: estudos em homenagem a Maria Celina Bodin de Moraes. Indaiatuba SP : Editora Foco, 2024, p. 25 a 37.

COORDENAÇÃO:
Ana Paula Canto de Lima
Newton Moraes

Ana Paula Canto de Lima
Adrianne Lima
Beatriz de Andrade Junque
Camila Henning Salmoria
Carolina Elisa Margonari
Caroline Vivas Gonçalves
Daiana Allessi Nicoletti Alves
Eloá de Azevedo Caixeta
Érica Costa
Flavia Alcassa
Geysa Camara
Gisele Truzzi
Iasmin Palotta
João Victor Barcellos Machado Correia
Letícia Zampieri
Mariana Gomes Lopes
Newton Moraes
Oscar Valente Cardoso
Rafael A. Carneiro de Castilho
Silvio Maciel e Silva Junior

EDITORA IMPÉRIO