MICROTARGETING EM CAMPANHAS ELEITORAIS: ANÁLISE JURÍDICA COMPARADA E PROPOSTAS REGULATÓRIAS

MICROTARGETING IN ELECTION CAMPAIGNS: COMPARATIVE LEGAL ANALYSIS AND REGULATORY PROPOSALS

Eduardo Pelella[1]

RESUMO
Este artigo realiza uma análise crítica do fenômeno do *microtargeting* em campanhas eleitorais sob uma perspectiva jurídica comparada, avaliando os marcos regulatórios existentes nos Estados Unidos, na União Europeia e no Brasil, bem como discutindo propostas de regulamentação para mitigar seus riscos à democracia. Por meio de pesquisa bibliográfica e análise normativa, examina-se como o uso de dados pessoais e técnicas de segmentação comportamental para influenciar eleitores desafia a proteção de dados, a transparência e a igualdade de condições no processo eleitoral. O estudo evidencia lacunas na legislação vigente e aponta a necessidade de normas específicas que promovam maior transparência na veiculação de propaganda política personalizada, imponham limites ao microdirecionamento de eleitores e assegurem mecanismos eficazes de fiscalização. Conclui-se que uma regulamentação equilibrada do *microtargeting* político é imprescindível para resguardar a integridade democrática, conciliando a inovação tecnológica com os princípios de privacidade e equidade eleitoral.
Palavras-chave: *microtargeting*; campanhas eleitorais; proteção de dados; regulação; democracia.

ABSTRACT
This article provides a critical analysis of the phenomenon of microtargeting in electoral campaigns from a comparative legal perspective, evaluating the regulatory frameworks in the United States, the European Union, and Brazil, as well as discussing regulatory proposals to mitigate its risks to democracy. Through bibliographic research and normative analysis, it examines how the use of per-

[1] Mestre em Direito, Procurador Regional da República, Ex-Procurador Regional Eleitoral.

sonal data and behavioral targeting techniques to influence voters challenges data protection, transparency, and equality in the electoral process. The study highlights gaps in current legislation and points out the need for specific rules that foster greater transparency in the dissemination of personalized political advertising, impose limits on voter microtargeting, and ensure effective oversight mechanisms. It concludes that balanced regulation of political microtargeting is essential to safeguard democratic integrity, reconciling technological innovation with the principles of privacy and electoral fairness.
Keywords: microtargeting; electoral campaigns; data protection; regulation; democracy.

Sumário

1 INTRODUÇÃO

Nos últimos anos, o uso do *microtargeting* - termo que designa o microdirecionamento de propaganda política a eleitores específicos com base em dados pessoais - emergiu como estratégia controversa em campanhas eleitorais. Plataformas digitais e ferramentas de *big data* permitiram a partidos e candidatos segmentar o eleitorado em nível individual, adaptando mensagens de acordo com perfis psicográficos e comportamentais. O caso *Cambridge Analytica*, revelado em 2018, ilustrou esse fenômeno ao mostrar que milhões de perfis de eleitores foram indevidamente coletados do Facebook e empregados para influenciar preferências de voto nos EUA e no Reino Unido (Cadwalladr; Graham-Harrison, 2018). Esses métodos inauguram possibilidades inéditas de engajamento político, mas também levantam sérios alertas quanto à manipulação do debate público, à privacidade e à equidade do processo eleitoral.

Do ponto de vista jurídico, o *microtargeting* desafia marcos regulatórios tradicionais. Em democracias consolidadas, observa-se um vácuo normativo específico: nos Estados Unidos, a publicidade política é amplamente protegida pela Primeira Emenda como forma de liberdade de expressão, não havendo restrições legais quanto à segmentação de eleitores. Já na União Europeia, embora não exista ainda uma lei específica sobre propaganda personalizada, aplicam-se

normas gerais de proteção de dados (como o *General Data Protection Regulation* - GDPR) que impõem certos limites ao uso de informações pessoais em campanhas. No Brasil, o tema ganha relevância recente, com discussões sobre como conciliar a inovação tecnológica das campanhas digitais com os princípios da legislação eleitoral e da tutela de dados pessoais. Pesquisadores alertam que, sem ajustes normativos, as técnicas de *microtargeting* podem acarretar riscos significativos à democracia representativa. Diante desse contexto, este artigo tem por objetivo analisar comparativamente as abordagens regulatórias adotadas (ou em construção) nos EUA, na UE e no Brasil, bem como apresentar propostas de regulamentação para mitigar os riscos do *microtargeting* ao processo democrático.

Metodologicamente, procede-se a um exame bibliográfico e jurídico-comparado, confrontando opções legislativas e estudos acadêmicos relevantes. Inicialmente, conceitua-se o *microtargeting* e discutem-se seus potenciais benefícios e malefícios ao processo eleitoral. Em seguida, avaliam-se as respostas jurídicas nas três esferas geográficas mencionadas, evidenciando lacunas e avanços normativos. Por fim, são sugeridas medidas regulatórias aptas a promover maior transparência, responsabilidade e *fairness*[2] eleitoral no uso de técnicas de *microtargeting* em campanhas políticas.

2 O MICROTARGETING ELEITORAL E SEUS IMPACTOS

2.1 DEFINIÇÃO E FUNCIONAMENTO

Microtargeting político pode ser definido como uma forma de comunicação personalizada que envolve a coleta de informações detalhadas sobre eleitores e o uso desses dados para exibir anúncios políticos direcionados sob medida. Na prática, campanhas coletam uma variedade de dados - demográficos, comportamentais, históricos de navegação e interações em redes sociais - para segmentar o público em nichos específicos. Algoritmos de análise permitem inferir preferências políticas ou traços de personalidade dos eleitores, de modo que as mensagens possam ser calibradas para maximizar sua ressonância junto a cada perfil. Por exemplo, eleitores identificados como indecisos em determinado tema podem receber anúncios enfatizando essa pauta específica, enquanto eleitores fortemente alinhados a uma causa podem ser estimulados a mobilizar seus pares em torno dela (Saura Garcia, 2024; Bayer, 2020).

[2] Equidade, lisura e integridade.

O *microtargeting*, nesta acepção contemporânea[3], tornou-se notório nas eleições norte-americanas, onde é empregado em larga escala desde os anos 2000, e gradualmente se dissemina em outros países com a popularização do marketing político digital. Técnicas de psicometria e *big data* prometem identificar inclinações e até vulnerabilidades individuais, ajustando o tom e o conteúdo das mensagens para causar o máximo impacto persuasivo em cada eleitor. Conforme revelado no caso *Cambridge Analytica*, modelos preditivos podem explorar as fragilidades psicológicas dos indivíduos para direcionar propaganda altamente personalizada - o próprio arquiteto da estratégia admitiu que a empresa «explorou o Facebook para colher milhões de perfis" e construir modelos para mirar nos "demônios internos" dos eleitores. Esse relato expõe o potencial manipulativo dessas táticas hipersegmentadas no ambiente eleitoral (Berghel, 2018).

2.2 EFEITOS PARA A DEMOCRACIA

Defensores do *microtargeting* argumentam que a personalização das mensagens tende a aumentar a eficácia da comunicação política e engajar eleitores apáticos, ao fornecer informações sob medida aos interesses de cada segmento. De fato, há quem veja nessa estratégia uma forma de otimizar o alcance de eleitores com pautas específicas, potencialmente elevando a participação política e o conhecimento do público sobre determinados temas (Rauch, 2022; Borgesius *et al.*, 2018).

Daniel Rauch, por exemplo, em *Customized Speech and the First Amendment* (2022), propõe uma defesa abrangente e sistemática do discurso customizado

[3] Da Empoli (2019) observa que o microdirecionamento sempre foi utilizado com maior ou menor habilidade por candidatos no curso das campanhas eleitorais. Ele aponta, por exemplo, que Arthur Finkelstein, hoje um dos principais conselheiros políticos e estrategistas do 1º ministro húngaro Viktór Orban, utilizava-se de escrupulosas sondagens demográficas já nos anos 80 para dirigir candidaturas nos EUA, sendo a mais notória a de Ronald Reagan à presidência da República. Através de tais sondagens, Finkelstein era capaz de calibrar o discurso eleitoral de seu candidato a determinado conjunto de indivíduos ou comunidades. Isto possibilita que as mensagens sejam baseadas no receptor e não no tema da campanha e permitem a calibragem do discurso nesse critério. Este tipo de estratagema não é novidade. Porém, continua o autor, "em termos políticos, a chegada do Big Data poderia ser comparada à invenção do microscópio. No passado, a partir de sondagens sempre aleatórias, os comunicadores políticos podiam atingir grandes aglomerados demográficos ou profissionais (...)". Hoje, com o advento dos Big Data é "possível enviar mensagens personalizadas a cada eleitor com base nas características individuais" a partir de dados coletados de formas ostensivas ou não, como ocorreu no caso *Cambridge Analytica*. Da Empoli (2019) soma os fatores e apresenta como resultado o fato de que a tônica das campanhas é agora a emissão de mensagens políticas com conteúdo automatizado, distinto e muitas vezes entre si contraditório, se visto no seu conjunto, a depender de quem recebe a mensagem.

como prática constitucionalmente protegida nos Estados Unidos. Para o autor, adaptar mensagens com base em dados da audiência constitui não apenas um fenômeno onipresente na vida política contemporânea, mas um exercício legítimo e central da liberdade de expressão. Doutrinariamente, Rauch argumenta que tanto a escolha do conteúdo quanto a seleção do público-alvo fazem parte do núcleo protegido da Primeira Emenda. A coleta de dados, embora sujeita a menor proteção, só poderia ser regulada mediante leis neutras em conteúdo e de aplicação geral (*content-neutral, generally applicable laws*), o que na prática ainda não ocorre. Com base nos princípios de *Speaker Autonomy* (autonomia do orador) e *Uncapped Persuasive Efficacy* (eficácia persuasiva irrestrita), Rauch sustenta que o Estado não pode restringir o uso de recursos - cognitivos, materiais ou sociais - pelos oradores para maximizar a eficácia persuasiva de seus discursos. Mesmo diante dos riscos associados à personalização digital - como fragmentação, manipulação ou desigualdade no acesso -, o autor defende que a proteção constitucional ao discurso customizado deve ser mantida, por seus potenciais benefícios à inclusão, à mobilização cívica e ao controle do poder estatal. Nesse sentido, Rauch minimiza a relevância normativa de casos emblemáticos como o escândalo *Cambridge Analytica*, que, segundo ele, teve impacto narrativo desproporcional à sua real eficácia, funcionando mais como símbolo distorcido de práticas hoje comuns na política americana.

Todavia, as críticas e preocupações em torno do *microtargeting* são abundantes.

Por um lado, a segmentação excessiva pode fragmentar o debate público e até permitir que um candidato adote discursos distintos (ou contraditórios) para grupos diferentes, apresentando-se de forma enganosa como um "candidato de uma causa" diferente para cada eleitor. Essa capacidade de moldar mensagens conforme o interlocutor escapa ao escrutínio público e dificulta a cobrança de coerência dos candidatos. Por outro lado, a coleta massiva de dados pessoais para fins eleitorais suscita graves preocupações de privacidade, envolvendo muitas vezes informações sensíveis obtidas sem consentimento ou ciência dos cidadãos (Borgesius *et al.*, 2018; Bayer, 2020).

Outra preocupação é a opacidade: mensagens microdirecionadas não são facilmente conhecidas ou verificadas por quem está fora do público-alvo, ao contrário da propaganda em mídia tradicional. Isso dificulta a detecção de notícias falsas ou de promessas inconsistentes difundidas setorialmente, minando a *accountability*[4] dos candidatos. Ademais, o *microtargeting* pode ser

[4] Em termos simples, princípio segundo o qual agentes públicos ou privados devem prestar contas de seus atos, assumir as consequências de suas decisões e se submeter a mecanismos de controle e responsabilização, garantindo transparência, legalidade e integridade institucional.

instrumentalizado para manipular eleitores vulneráveis com desinformação sob medida. Nas eleições de 2016 nos EUA, por exemplo, investigações apontaram esforços deliberados de difusão de conteúdo falso voltados especificamente a comunidades afro-americanas, com o intuito de desencorajá-las a votar. Tais práticas configuram uma forma de *redlining* digital[5], segregando o eleitorado e potencialmente excluindo certos grupos do discurso político (UK Parliament DCMS Committee, 2019; Berghel, 2018; Bayer, 2020; Farias; Melo Neto, 2022).

Há ainda o fator da desigualdade econômica: campanhas orientadas por *microtargeting* tendem a favorecer candidatos ou partidos com maiores recursos financeiros e acesso a grandes bases de dados, aprofundando a disparidade na competição eleitoral. O desenvolvimento e implementação de estratégias sofisticadas de análise de dados possuem custo elevado, o que pode consolidar a vantagem dos partidos grandes e bem financiados e dificultar a emergência de novas vozes políticas. No nível coletivo, temem-se efeitos de fragmentação da esfera pública: se cada eleitor recebe uma versão distinta e altamente filtrada da mensagem política - focada apenas em temas de seu interesse pessoal - perde-se a visão de conjunto das propostas e diminui-se o espaço de debate sobre

[5] *Redlining* eleitoral refere-se à prática de exclusão sistemática de determinados grupos sociais do processo democrático, por meio de estratégias territoriais ou digitais que limitam seu acesso à representação, à informação política ou ao próprio exercício do voto. Originalmente associado à negação de crédito ou serviços com base na localização geográfica – prática recorrente nos Estados Unidos durante o século XX –, o *redlining* assumiu novas configurações no contexto eleitoral contemporâneo. Hoje, não se trata apenas da manipulação física de zonas eleitorais, como no fechamento de seções em comunidades vulneráveis, mas também da segmentação algorítmica em campanhas digitais, nas quais certos públicos são deliberadamente omitidos de mensagens políticas, convocações ao voto ou debates relevantes. Essa segmentação seletiva, fundamentada em dados demográficos, étnico-raciais ou socioeconômicos, caracteriza uma forma de *redlining* discursivo, que restringe a circulação de informação política e compromete a igualdade de participação no espaço público. Embora distintos em sua configuração jurídica e operacional, conceitos como *gerrymandering* (manipulação das fronteiras distritais), *vote suppression* (supressão do voto) e *disparate impact* (impacto desproporcional de normas aparentemente neutras) guardam relação funcional com o *redlining*, na medida em que todos operam por meio de mecanismos de distorção ou limitação seletiva da participação eleitoral. O *gerrymandering* consiste na manipulação deliberada do desenho dos distritos eleitorais, com o objetivo de favorecer determinado partido ou grupo, muitas vezes gerando efeitos excludentes semelhantes aos do *redlining* territorial. Já a vote suppression se refere ao conjunto de práticas - formais ou informais - voltadas a dificultar ou desencorajar o exercício do voto por segmentos específicos da população, como minorias raciais, jovens ou populações periféricas, seja por meio de exigências documentais desproporcionais, seja por campanhas de desinformação. Por sua vez, o *disparate impact* corresponde a normas ou políticas aparentemente neutras que, na prática, produzem efeitos desiguais sobre grupos vulneráveis - como ocorre, por exemplo, com requisitos de alistamento eleitoral que afetam desproporcionalmente indivíduos com menor acesso à documentação civil. Todos esses instrumentos, inclusive o *redlining*, operam segundo uma lógica de restrição seletiva da cidadania política e, em diferentes graus, contribuem para a erosão dos princípios democráticos da universalidade, da igualdade e da representatividade.

pautas comuns. Essa fragmentação, potencializada por fenômenos como *filter bubbles*[6] (Pariser, 2011), pode comprometer a formação de uma opinião pública informada e plural.

Mesmo a liberdade de expressão dos cidadãos pode ser indiretamente afetada. A mera consciência de estar sendo monitorado e perfilado para fins políticos pode gerar um efeito inibidor (*chilling effect*): indivíduos podem alterar seu comportamento on-line ou deixar de expressar opiniões políticas por receio de estarem sendo observados e catalogados. Em suma, os riscos do *microtargeting* eleitoral à integridade democrática são substanciais. Diversos autores enfatizam que, sem controles adequados, essas práticas podem distorcer o jogo eleitoral ao manipular preferências de voto de forma invisível e violar princípios básicos como a transparência, a igualdade de oportunidades entre candidatos e a autonomia do voto (Farias; Melo Neto, 2022; Borgesius *et al.*, 2018).

3 ANÁLISE JURÍDICA COMPARADA

3.1 ESTADOS UNIDOS

A doutrina constitucional norte-americana relativa à liberdade de expressão repousa sobre uma arquitetura teórica e jurisprudencial profundamente marcada pela desconfiança em relação à ação regulatória do Estado, especialmente quando se trata de discurso político. No centro dessa estrutura encontra-se a distinção entre *content-based restrictions* e *content-neutral restrictions*. Restrições baseadas no conteúdo da mensagem (*content-based*) ou na identidade do emissor (*speaker-based*) são submetidas à mais rigorosa forma de controle judicial - o chamado *strict scrutiny* - e são, em regra, consideradas presumivelmente inconstitucionais, salvo se o estado demonstrar um interesse público imperioso (*compelling state interest*) e provar que a medida é estritamente necessária

[6] O conceito de *filter bubbles*, desenvolvido por Eli Pariser em sua obra *The Filter Bubble: What the Internet Is Hiding from You* (2011), refere-se ao ambiente informacional personalizado e isolado criado por algoritmos que filtram conteúdos com base no comportamento prévio do usuário - como cliques, curtidas e buscas. Em português, o termo pode ser traduzido como "bolhas de filtragem algorítmica", expressão que destaca o papel dos sistemas automatizados na construção de uma experiência informacional restrita. Esse processo leva cada indivíduo a receber informações compatíveis com suas crenças e interesses, enquanto conteúdos divergentes são progressivamente excluídos de sua experiência on-line. Pariser alerta que essa bolha algorítmica reduz o pluralismo informativo, limita o confronto com ideias diferentes e compromete a formação de uma esfera pública democrática, uma vez que os cidadãos passam a viver em realidades paralelas e cognitivamente fechadas. Ao contrário da promessa inicial de internet aberta e diversificada, os algoritmos de personalização -especialmente em plataformas como Google e Facebook -constroem universos informacionais assimétricos e opacos, nos quais o usuário não tem consciência do que está sendo ocultado.

(*narrowly tailored*) à realização desse fim, sem alternativas menos restritivas disponíveis.

Essa configuração doutrinária encontra aplicação direta nos debates contemporâneos sobre a possibilidade de regulação do uso de dados para fins eleitorais, particularmente no que diz respeito ao *microtargeting* digital. Em primeiro lugar, deve-se reconhecer que há um obstáculo de fundo, relacionado ao próprio escopo da Primeira Emenda, conforme interpretada pela Suprema Corte. Em decisões relativamente recentes, como *Sorrell v. IMS Health Inc.* (2011), a Corte afirmou que o uso, a análise e a comercialização de dados - mesmo pessoais - podem estar protegidos pela cláusula da liberdade de expressão. Naquele caso, foi invalidada uma lei de Vermont que limitava a venda de dados sobre prescrições médicas para fins de marketing, sob o argumento de que tal restrição era tanto *content-based* quanto *speaker-based*, e, portanto, sujeita ao mais alto escrutínio judicial.

Esse entendimento já estava presente em *Citizens United v. FEC* (2010), quando a Suprema Corte deixou claro que a Primeira Emenda protege não apenas o conteúdo do discurso, mas também o orador e as ideias que dele fluem. A partir disso, consolidou-se a compreensão de que os dados - inclusive os utilizados em estratégias eleitorais - podem ser considerados parte integrante do *speech* (discurso), sendo, portanto, objeto de tutela constitucional. Como observa Krotoszynski (2020), essas decisões tornaram a capacidade do Estado de regular o uso de dados para influenciar eleições substancialmente limitada: qualquer tentativa de restrição ampla à coleta ou uso desses dados para fins políticos seria presumivelmente inconstitucional, por configurar uma limitação baseada no conteúdo e/ou no emissor. A legislação correspondente, para sobreviver, teria de satisfazer os requisitos de *strict scrutiny*, desafio que se mostra, na prática, quase sempre fatal às tentativas regulatórias.

Além dos entraves jurídicos de natureza substantiva, há ainda o contexto político-institucional que reforça o ceticismo em relação à regulação. O uso estratégico de dados eleitorais interessa profundamente às máquinas partidárias, tanto democratas quanto republicanas. Presumir que esses atores centrais se comportariam de forma altruísta - voluntariamente abrindo mão de instrumentos tão eficazes de controle e mobilização de seus eleitorados - sem a existência de estímulos externos ou fortes imposições legais, seria, no mínimo, ingênuo. O controle granular do eleitorado por meio de microsegmentação informacional é hoje um ativo essencial na disputa intra e interpartidária, o que reduz drasticamente a viabilidade política de reformas regulatórias mais ambiciosas (Krotoszynski, 2020).

Por essas razões, propostas de regulação substancial - como a proibição do uso de dados pessoais para fins eleitorais, ou a limitação de conteúdos direcionados - esbarram tanto em obstáculos jurídicos de fundo (por serem *content-based*, *speaker-based* e, por vezes, restrições prévias ao discurso, ou *prior restraints*), quanto em barreiras institucionais de ordem política e estratégica. A imposição de censura governamental ativa sobre o discurso político digital, como adverte Krotoszynski, criaria suas próprias patologias institucionais, e dificilmente seria admitida pelas cortes federais em qualquer configuração normativa ampla.

Em contraste, o espaço normativo mais promissor encontra-se nas regras de *transparência* e *divulgação* obrigatória (*disclosure requirements*), que permanecem, conforme a jurisprudência consolidada, em um terreno constitucional muito mais sólido. Medidas que obrigam campanhas a informar o uso de dados, identificar os responsáveis por conteúdos patrocinados, ou revelar os critérios de segmentação, não implicam censura do conteúdo, mas sim a promoção da *accountability* informacional - o que tende a ser compatível com a Primeira Emenda, desde que formulado de forma não discriminatória quanto ao conteúdo ou ao emissor.

Em síntese, qualquer tentativa de regular o uso de dados e o *microtargeting* na esfera eleitoral dos Estados Unidos deverá necessariamente transitar por um estreito corredor constitucional: de um lado, evitando as armadilhas de restrições *content-based* e *speaker-based*; de outro, promovendo mecanismos de transparência que preservem a integridade informacional do processo democrático sem incorrer em censura disfarçada. Trata-se de um desafio normativo e político de grande magnitude, cujo equacionamento exigirá precisão técnica, consenso institucional e, sobretudo, respeito às balizas estruturantes da liberdade de expressão constitucionalmente protegida.

Exatamente por isso, lá o *microtargeting* eleitoral é amplamente tolerado e integrado às estratégias de campanha modernas. O ordenamento jurídico norte-americano não possui leis federais específicas que restrinjam a segmentação de eleitores na propaganda política, reflexo de uma tradição legal fortemente pautada pela Primeira Emenda da Constituição dos EUA. A comunicação política - incluindo os anúncios eleitorais - é considerada uma forma essencial de discurso protegido, gozando de nível elevado de proteção em comparação, por exemplo, à publicidade comercial. Tentativas de proibir ou limitar diretamente o *microtargeting* enfrentariam, como já referidos, barreiras constitucionais, sendo vistas como potenciais violações à liberdade política de expressão, pois equiparadas a *content based restrictions*. Consequentemente, não há vedações quanto ao uso, por campanhas, de dados demográficos ou comportamentais para direcionar mensagens eleitorais a grupos específicos (Borgesius *et al.*, 2018; King, 2022; Dobber, Ó Fathaigh & Borgesius, 2019).

A legislação eleitoral federal dos EUA impõe apenas exigências genéricas de transparência, como a identificação do patrocinador em peças publicitárias e relatórios de gastos de campanha, mas não regula os critérios de audiência nem o conteúdo distribuído de forma personalizada. Inexiste, até o momento, uma lei geral de proteção de dados pessoais nos EUA em nível federal - lacuna que inclui a atividade dos partidos políticos -, o que significa que a coleta e uso de informações de eleitores para fins de campanha permanecem amplamente autorregulados pelas próprias campanhas e pelas plataformas digitais (Bennett, 2016). De fato, especialistas observam que os partidos norte-americanos construíram gigantescas bases de dados de eleitores ao longo das últimas décadas, sem equivalentes em outras democracias, graças à ausência de restrições legais comparáveis às europeias.

Diante da ausência de regulação estatal específica, as próprias plataformas de mídia social adotaram algumas políticas internas após as controvérsias recentes. Em 2019, o X (antigo Twitter) anunciou a proibição total de anúncios políticos em sua plataforma, citando preocupações éticas com os efeitos do *microtargeting*. No mesmo ano, o Google impôs limites ao direcionamento de propaganda eleitoral em suas redes: conforme política implementada às vésperas do ciclo de 2020, os anúncios políticos no Google e no YouTube passaram a poder ser segmentados apenas por três categorias gerais - idade, gênero e localização (em nível de código postal) - vedando-se o uso de informações mais granulares, como afiliação ou preferências políticas inferidas. Essa mudança ocorreu em meio à pressão pública e depois de o X ter optado por banir completamente as propagandas eleitorais, enquanto o Facebook, por sua vez, enfrentava cobranças para rever suas práticas. O Facebook acabou adotando medidas mais brandas: criou uma biblioteca on-line de anúncios políticos para consulta pública e eliminou algumas opções de segmentação consideradas sensíveis, mas manteve a possibilidade de microdirecionamento baseado em interesses e comportamentos, inclusive via ferramentas como *Custom Audiences*.

No plano legislativo, propostas como o *Honest Ads Act* - que buscava equiparar a transparência das propagandas on-line à das propagandas televisivas, exigindo divulgações e arquivos públicos de anúncios - foram introduzidas no Congresso dos EUA, mas não avançaram. Até o presente, não há normas federais aprovadas que regulem especificamente o *microtargeting* político. Em síntese, o cenário norte-americano caracteriza-se por grande permissividade ao *microtargeting* eleitoral, sustentada pela tutela constitucional do discurso político e atenuada apenas por iniciativas voluntárias das empresas de tecnologia (King, 2022). Esse modelo contrasta com a preocupação regulatória mais acentuada observada em outras jurisdições, como se verá a seguir.

3.2 UNIÃO EUROPEIA

Ao contrário dos EUA, a União Europeia trilhou um caminho regulatório pautado pela proteção de dados pessoais e pela salvaguarda da integridade do processo eleitoral. Segundo Witzleb, Peterson e Richardson (2020), em termos gerais são os países europeus que defendem mais ativamente a atividade regulatória, ao contrário dos EUA, Canadá ou Austrália que permanecem numa postura mais passiva. Para eles, os países europeus conseguiram caminhar mais no tema porque *puderam se basear em sua vasta jurisprudência sobre direitos humanos. Além dos direitos democráticos, os valores de direitos humanos mais relevantes no contexto dos big data e do processo político são o direito à liberdade de expressão e o direito à privacidade.* Em virtude disso, os sistemas europeus estão acostumados a lidar com áreas de fricção, *empregando o princípio da proporcionalidade para equilibrar os direitos humanos concorrentes.* Diferentemente sucede no sistema americano, prosseguem, onde priorizou-se a *liberdade de expressão a ponto de se tolerar o discurso de ódio.* Esta diferença seminal de abordagem justifica metodologicamente que sejam relevados alguns pontos centrais que apartam os dois sistemas.

No contexto da União Europeia, até recentemente não existia uma legislação dedicada exclusivamente à propaganda política on-line. No entanto, as campanhas eleitorais sempre estiveram submetidas a um arcabouço normativo geral robusto - sobretudo ao Regulamento Geral de Proteção de Dados (GDPR), em vigor desde 2018 - que impõe, mesmo que de forma indireta, restrições importantes a determinadas práticas de *microtargeting*. O GDPR estabelece princípios rigorosos para o tratamento de dados pessoais, exigindo, entre outros requisitos, o consentimento explícito do titular para o uso de dados sensíveis, categoria que inclui informações sobre opiniões políticas. Dessa forma, o uso de dados de eleitores para fins de segmentação deve obedecer a bases legais bem definidas e respeitar princípios como finalidade específica, minimização e transparência, sob pena de sanções significativas impostas pelas autoridades de proteção de dados (Blasi Casagran; Vermeulen, 2021).

De modo mais estrutural, o GDPR permanece como a espinha dorsal da regulação europeia sobre o uso de dados, inclusive no contexto eleitoral. Dois vetores principais sustentam esse sistema: o consentimento e a transparência. A norma exige que o tratamento de dados pessoais ocorra com base em consentimento explícito ou especial, a depender da categoria e da sensibilidade dos dados. Como sublinha McDonagh (2020), essa exigência representa o núcleo da regulação, tendo em vista que o tratamento de dados com finalidade de prever preferências de voto é "muito problemático, especialmente quando aqueles

que podem ser objeto de análise são coletados em plataformas de mídia social ostensivamente com o consentimento do titular".

Na ausência de consentimento, o art. 6º do GDPR permite, com certos limites, o tratamento com base no interesse público (art. 6º, 1, e) ou nos interesses legítimos do controlador (art. 6º, 1, f). O art. 9º, por sua vez, admite exceções ao tratamento de dados sensíveis, especialmente nas hipóteses do inciso 2, alínea "d", que autoriza o processamento no curso de atividades legítimas por órgãos com finalidade política, e da alínea "g", que admite o tratamento por razões de interesse público substancial. Isso significa que partidos políticos e candidatos dispõem de maior margem legal para tratar dados pessoais com fins eleitorais do que *data brokers*, plataformas digitais e empresas de análise de dados, ainda que estas últimas não estejam automaticamente excluídas dessa possibilidade (McDonagh, 2020).

Adicionalmente, a aplicação dos direitos conferidos aos titulares pelo Capítulo 2 do GDPR sofre certas limitações que podem afetar o tratamento de dados eleitorais. O art. 14, que impõe deveres de transparência no caso de coleta indireta de dados, prevê exceções, entre elas a chamada "*disproportionate effort exception*", cuja aplicabilidade ao contexto eleitoral é reconhecida (McDonagh, 2020). Os Estados-Membros também podem legislar exceções específicas ao artigo. De forma mais ampla, as exigências de transparência previstas no art. 14 enfrentam desafios práticos quando aplicadas ao perfilamento eleitoral, uma vez que essas práticas frequentemente envolvem a geração de dados inferidos - ou seja, "novos dados pessoais que não foram fornecidos diretamente pelos próprios titulares" (McDonagh, 2020).

O direito de oposição previsto no artigo 21, n.º 1, deve ser aplicável ao tratamento de dados pessoais em atividades eleitorais, ainda que possa ser neutralizado por interesses legítimos prevalentes do processador. Nesse contexto, invoca-se com frequência o interesse na liberdade de expressão política, o que pode "permitir a anulação do direito de objeção do titular dos dados" (McDonagh, 2020). Quanto ao direito de oposição ao marketing direto, previsto no artigo 21, n.º 2, sua eficácia no âmbito das campanhas políticas digitais é duvidosa, dada a ausência de definição clara sobre o que constitui marketing direto no GDPR. Como destaca McDonagh (2020), "não está claro se a definição de marketing direto no projeto de regulamento inclui técnicas de campanha política on-line comumente utilizadas, como publicidade na web, por meio de plataformas de mídia social ou em websites, ou publicidade comportamental".

Por fim, o art. 22 garante ao titular dos dados "o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automati-

zado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar". Todavia, persiste certa incerteza sobre a aplicabilidade dessa cláusula no contexto eleitoral. Ainda que o tratamento automatizado seja, em princípio, limitado, os Estados-Membros podem introduzir exceções legislativas específicas para autorizar a definição de perfis com fins eleitorais (McDonagh, 2020).

A estrutura normativa do GDPR condicionou fortemente o ambiente europeu para o uso de dados pessoais em campanhas. Conforme observa Bennett (2016), partidos políticos de outras democracias "olharam com grande inveja" para as práticas de *microtargeting* desenvolvidas nos Estados Unidos, mas enfrentaram obstáculos jurídicos relevantes para replicá-las em território europeu, em razão da presença de regras de privacidade mais rigorosas. Embora a propaganda eleitoral também constitua, na Europa, uma forma de expressão política protegida, tal proteção não é absoluta. Do ponto de vista do direito europeu dos direitos humanos, admite-se a imposição de restrições proporcionais à publicidade política, desde que destinadas à preservação da integridade do pleito e de outros interesses fundamentais à democracia. Em diversos países europeus, como França e Reino Unido, são admitidas restrições à veiculação de anúncios políticos pagos em rádio e televisão durante campanhas eleitorais - medidas que não são consideradas violações à liberdade de expressão (Dobber; Ó Fathaigh; Borgesius, 2019).

A crescente preocupação com os efeitos potencialmente manipulativos do *microtargeting* levou a União Europeia à adoção, em 2024, do Regulamento de Transparência e *Targeting* da Publicidade Política (UE, 2024), concebido com o objetivo de coibir práticas de interferência indevida nos processos eleitorais. Este novo regulamento, cuja entrada em vigor está prevista para o ciclo eleitoral do Parlamento Europeu de 2024, estabelece obrigações inéditas de transparência e limites mais estritos ao *microtargeting* em toda a União.

Entre as disposições mais relevantes, destaca-se a exigência de que todo anúncio político on-line seja acompanhado de um rótulo de transparência claramente visível, informando tratar-se de publicidade política e incluindo dados essenciais, como o nome do patrocinador, o valor gasto, o pleito ao qual se refere e, sobretudo, uma descrição dos critérios de segmentação utilizados. As plataformas digitais, por sua vez, deverão disponibilizar um aviso de transparência com essas informações, permitindo ao cidadão compreender por que está recebendo determinada propaganda (Ascensão, 2024).

No tocante às práticas de *microtargeting*, o novo regulamento impõe restrições substanciais: a segmentação de anúncios políticos com base em dados

pessoais só será permitida quando os dados tiverem sido coletados diretamente do próprio titular e mediante consentimento específico e prévio para essa finalidade. Em outras palavras, o eleitor deverá ter autorizado, de maneira expressa, o recebimento de propaganda direcionada. Ademais, mesmo quando houver consentimento, o uso de categorias sensíveis de dados - como informações sobre origem étnica, convicções religiosas, estado de saúde ou opinião política - permanecerá proibido para fins de perfilamento e direcionamento publicitário. Trata-se, assim, de uma vedação praticamente absoluta ao uso de dados sensíveis em campanhas digitais, o que inviabiliza, por exemplo, a compra de anúncios em plataformas como o Facebook para segmentar usuários com base em sua inclinação política ou pertencimento a grupos minoritários.

A implementação dessas regras na UE deverá, em tese, ser acompanhada de fiscalização rigorosa. Autoridades nacionais e europeias (como comissões eleitorais e órgãos de proteção de dados) terão competência para supervisionar o cumprimento do novo regulamento. Vale lembrar que, na esteira do escândalo *Cambridge Analytica*, órgãos como o *Information Commissioner's Office* (ICO), do Reino Unido, realizaram investigações de grande envergadura sobre uso indevido de dados em campanhas. A investigação do ICO relativa ao referendo do *Brexit* tornou-se a maior já conduzida por uma autoridade de dados, envolvendo análise de plataformas digitais e consultorias em escala inédita. Esse engajamento regulatório exemplifica a disposição europeia de coibir abusos.

Em suma, a UE caminha para um modelo de regulação robusta do *microtargeting* eleitoral, combinando a aplicação de princípios gerais de privacidade com normas específicas de transparência e limitação de técnicas de segmentação. Trata-se de um paradigma que privilegia a proteção dos eleitores enquanto sujeitos de direitos, mesmo que tensione a liberdade das campanhas – praticamente o oposto do modelo norte-americano permissivo.

3.3 BRASIL

No Brasil, a regulação do *microtargeting* em campanhas eleitorais encontra-se em fase incipiente, embora alguns passos importantes tenham sido dados recentemente. Historicamente, a legislação eleitoral brasileira vedava a propaganda eleitoral paga na internet. Esse cenário mudou com a Reforma Eleitoral de 2017: a Lei nº 13.488/2017 alterou a Lei das Eleições (Lei nº 9.504/1997) para permitir o impulsionamento de conteúdos nas redes sociais, desde que identificado de forma inequívoca e contratado exclusivamente por partidos, federações, coligações, candidatos ou seus representantes. Em outras palavras, passou a ser legal que candidatos pagassem plataformas como Facebook, Instagram ou

Google para promover suas postagens a um público maior, contanto que essa publicidade digital estivesse claramente marcada como propaganda eleitoral e constasse do relatório de gastos de campanha. Essa mudança abriu espaço para o uso de segmentação de público nas campanhas on-line brasileiras, pois as ferramentas de impulsionamento oferecidas pelas plataformas permitem definir características da audiência-alvo (como localização geográfica, faixa etária, interesses, entre outros).

O Tribunal Superior Eleitoral (TSE), ao regulamentar a propaganda na internet, estabeleceu salvaguardas específicas de transparência diretamente relacionadas ao *microtargeting*. A Resolução TSE nº 23.610/2019, com as alterações introduzidas pela Resolução nº 23.732/2024, determinou expressamente, no artigo 27-A, que os provedores de aplicação que prestem serviço de impulsionamento eleitoral são obrigados a manter um repositório atualizado contendo, para todos os anúncios impulsionados eleitoralmente, o conteúdo completo do anúncio, a identificação do contratante, especificações detalhadas sobre o impulsionamento (público-alvo, valor investido, data de início e término), e indicação clara de que se trata de propaganda eleitoral. Além disso, é exigida a disponibilização de ferramenta de consulta pública, gratuita e de fácil navegação, permitindo que qualquer cidadão ou a Justiça Eleitoral possa verificar facilmente quais propagandas foram veiculadas, por quem e com qual alcance - uma medida alinhada às tendências internacionais de transparência. Cabe notar que é proibida no Brasil qualquer propaganda eleitoral paga na internet fora do impulsionamento permitido; ou seja, não é lícito que terceiros (como empresas ou apoiadores individuais) comprem anúncios políticos on-line, visando reduzir o risco de propaganda sombria financiada por atores não identificados.

No tocante à proteção de dados pessoais, o Brasil aprovou em 2018 a Lei Geral de Proteção de Dados (LGPD, Lei n. 13.709/2018), cujo escopo abrange também as atividades de tratamento de dados por partidos políticos e candidatos. A LGPD classifica dados sobre convicção política como dados sensíveis, exigindo consentimento específico do titular para seu uso (salvo hipóteses legais de exceção) e impondo princípios como os da finalidade, adequação e necessidade. Em tese, portanto, a elaboração de perfis de eleitores e o *microtargeting* deveriam submeter-se às salvaguardas da LGPD. O próprio TSE, em normativos recentes, condicionou certas práticas de campanha à observância da LGPD - por exemplo, o envio de mensagens eletrônicas a eleitores por candidatos só é permitido se presente uma das bases legais de tratamento previstas na lei de proteção de dados. Na prática, porém, a fiscalização do uso de dados em campanhas ainda é incipiente. Até o momento, a Autoridade Nacional de Proteção de Dados (ANPD) não editou diretrizes específicas voltadas ao contexto político, e há pouca atuação concreta da ANPD ou do Ministério Público visando verificar a

conformidade das campanhas com a LGPD (por exemplo, checando se eleitores cuja informação foi utilizada para *targeting* consentiram com tal uso).

Atualmente, portanto, não existe no Brasil uma disciplina legal pormenorizada dirigida exclusivamente ao *microtargeting* político. As condutas potencialmente abusivas nessa seara teriam que ser enquadradas de forma indireta em disposições já existentes - como eventualmente abuso de poder econômico ou uso indevido de meios de comunicação, na esfera eleitoral, ou infrações à LGPD, na esfera de proteção de dados. O debate sobre a necessidade de normas explícitas ainda está em curso. A comunidade acadêmica e os *policymakers* em geral têm se mostrado preocupados: estudos recentes apontam que as salvaguardas vigentes podem não ser suficientes para conter práticas de manipulação algorítmica do eleitorado (Farias; Melo Neto, 2022). Nos últimos anos, a Justiça Eleitoral implementou programas de enfrentamento à desinformação e firmou parcerias com plataformas digitais para promover maior transparência e controle de conteúdo durante as eleições (como a criação de canais de denúncia de notícias falsas e a rotulagem de conteúdo impulsionado), mas tais iniciativas operam mais no campo administrativo e de cooperação voluntária do que em obrigações legais rígidas, descambando episodicamente para providências de cunho voluntarista e descoordenado.

Assim, o ordenamento brasileiro encontra-se em um ponto intermediário: possui princípios e algumas regras que tangenciam o *microtargeting* (como as exigências de identificação e repositório de anúncios, e a proteção de dados pela LGPD), porém carece de um regime abrangente que aborde de forma específica os limites e responsabilidades no uso de segmentação comportamental em campanhas. Essa lacuna normativa motiva a reflexão sobre quais medidas adicionais poderiam ser adotadas para prevenir os riscos do *microtargeting* no contexto nacional, tema que será explorado a seguir.

4 PROPOSTAS REGULATÓRIAS

4.1 TRANSPARÊNCIA E DIREITO À INFORMAÇÃO

Uma das principais frentes para mitigar os problemas do *microtargeting* é aumentar a transparência das comunicações eleitorais segmentadas. A opacidade das técnicas atuais – em que somente o anunciante e a plataforma sabem exatamente quem recebeu determinada mensagem – pode ser enfrentada com a imposição de deveres legais de informação, tanto para as campanhas quanto para os intermediários digitais (Borgesius *et al.*, 2018; União Europeia, 2024).

Nesse sentido, as proposições mais comuns remetem à criação de mecanismos de transparência ativa: todas as propagandas eleitorais veiculadas on-line, especialmente as direcionadas por critérios de perfilamento, deveriam ser compiladas em bancos de dados públicos e acessíveis (Erga, 2022; União Europeia, 2024). Esses repositórios – a exemplo do que já exige em termos mais restritos no TSE (TSE, 2019; TSE, 2024) e do modelo previsto no novo regulamento europeu (União Europeia, 2024) – permitiriam que eleitores, jornalistas e autoridades fiscalizadoras soubessem quais mensagens estão sendo disseminadas, por quem, e a quais públicos-alvo. Cada anúncio político exibido nas redes poderia vir acompanhado de informações como: patrocinador/financiador, período de veiculação, quantidade de pessoas alcançadas e parâmetros de segmentação utilizados (faixa etária, localização geral, interesses selecionados etc.) (União Europeia, 2024; TSE, 2024).

Além disso, as campanhas deveriam ser obrigadas a informar claramente ao destinatário quando o conteúdo exibido foi personalizado. Por exemplo, no próprio corpo do anúncio direcionado deveria constar um rótulo ou aviso indicando tratar-se de propaganda eleitoral personalizada com base em dados do usuário (União Europeia, 2024; Erga, 2022). Tal rotulagem teria o potencial informativo e educativo do eleitor sobre o fato de estar recebendo uma mensagem sob medida - possivelmente diversa da recebida por outros eleitores - e permitiria uma recepção mais crítica do conteúdo (Farias; Melo Neto, 2022). Do ponto de vista jurídico, essa medida reforçaria o direito à informação do cidadão, alinhando-se ao dever geral de identificação de propaganda já presente na legislação brasileira (TSE, 2019). Poder-se-ia viabilizar tal iniciativa via resolução do TSE, complementando as regras atuais de propaganda ao exigir essa transparência adicional nas peças impulsionadas (TSE, 2024).

Adicionalmente, seria recomendável ampliar o detalhamento das informações disponibilizadas publicamente sobre os critérios de *microtargeting* empregados. Plataformas e campanhas deveriam divulgar, por exemplo, quais segmentos ou categorias de eleitores foram escolhidos para cada anúncio (ex.: mulheres de 18-24 anos interessadas em educação, residentes na região X) e o número de indivíduos alcançados em cada segmento (União Europeia, 2024; Erga, 2022). Essa abertura de dados permitiria um escrutínio independente sobre eventuais padrões de manipulação ou exclusão de grupos (Farias; Melo Neto, 2022). Entidades da sociedade civil e centros de pesquisa poderiam auditar os bancos de anúncios para identificar desvios - por exemplo, se determinado candidato direcionou sistematicamente mensagens negativas apenas a eleitores de um grupo étnico específico, ou se excluiu deliberadamente certo segmento opositor das suas propagandas positivas. E os órgãos de controle, de forma destacada o Ministério Público Eleitoral, poderiam exercer a efetiva supervisão das práticas de campanha (TSE, 2024).

Em resumo, fortalecer a transparência impõe poucos obstáculos à livre expressão política e traz benefícios significativos para o processo eleitoral (Borgesius *et al.*, 2018; União Europeia, 2024). A maior visibilidade sobre o conteúdo e a distribuição das mensagens dificulta a propagação de informações inconsistentes ou falsas em nichos isolados, e desestimula campanhas de utilizarem discursos contraditórios para diferentes públicos (Farias; Melo Neto, 2022). Trata-se de uma medida com amplo respaldo democrático - coerente com o princípio da publicidade e já adotada, em graus variados, na UE (União Europeia, 2024; Erga, 2022) e mesmo pelo TSE (TSE, 2019; TSE, 2024) - cujo aperfeiçoamento pode ser implementado sem grandes dificuldades tecnológicas. A transparência, por si, não impede o *microtargeting*, mas lança luz sobre ele, empoderando eleitores e fiscalizadores a reagirem a eventuais abusos (Borgesius *et al.*, 2018; Farias; Melo Neto, 2022).

4.2 LIMITES AO MICROTARGETING E PROTEÇÃO DE DADOS

Outra linha de propostas foca em estabelecer limites materiais às práticas de *microtargeting*, prevenindo as formas mais nocivas de segmentação comportamental. Uma medida central seria vedar expressamente por lei o uso de determinadas categorias de dados pessoais no direcionamento de propaganda eleitoral. Assim como o regulamento europeu proibiu o uso de dados sensíveis - como origem racial, convicções religiosas ou opiniões políticas - para fins de *targeting* de anúncios políticos (União Europeia, 2024), o legislador brasileiro poderia explicitar a vedação de que campanhas segmentem propaganda com base em atributos intrinsecamente discriminatórios ou altamente privados (Farias; Melo Neto, 2022). Por exemplo, seria ilícito direcionar anúncios de campanha levando em conta a religião do usuário, sua orientação sexual, ou informações de saúde. Essa regra protegeria grupos vulneráveis contra manipulações específicas e evitaria a exacerbação de divisões sociais por meio da propaganda personalizada. Vale notar que muitos desses dados já são considerados "sensíveis" pela LGPD (BRASIL, 2018), mas uma proibição eleitoral traria maior efetividade e facilidade de fiscalização (permitindo atuação direta da Justiça Eleitoral).

Além de banir certos tipos de dados para *microtargeting*, discute-se a imposição de um grau mínimo de amplitude nas audiências dos anúncios políticos. Ou seja, poder-se-ia fixar um público-alvo mínimo para cada propaganda eleitoral paga na internet. Por exemplo, definir que nenhum anúncio poderá ser direcionado a um grupo inferior a, por exemplo, 10 mil usuários ou a uma área geográfica menor que um município. Essa exigência impediria o *microtargeting* ultra específico, no qual apenas indivíduos isolados ou microgrupos recebem determinada mensagem, forçando as campanhas a alcançarem públicos mais

amplos (Internetlab, 2022). Com isso, diminui-se a possibilidade de comunicação política oculta (*one-to-one*) e incentiva-se que as mensagens de campanha tenham relevância pública mais geral. Embora a definição de um patamar numérico exato demande estudos (para não inviabilizar a segmentação legítima por região ou faixa etária, por exemplo), o princípio seria garantir que nenhuma campanha possa, por meio de dados, "sussurrar" promessas a públicos ínfimos sem que haja visibilidade mais ampla.

De se observar que não são poucos os que defendem uma abordagem ainda mais drástica: proibir integralmente o *microtargeting* de anúncios políticos. Nessa perspectiva, candidatos e partidos só poderiam veicular publicidade digital não direcionada ou com segmentação estritamente contextual (por conteúdo ou região ampla, como estado ou país). Seria uma volta ao paradigma do discurso público comum, semelhante ao horário eleitoral gratuito em rádio e TV, em que todos os eleitores recebem as mesmas mensagens. O argumento a favor dessa proibição total é o de preservar uma esfera pública compartilhada e evitar a fragmentação extrema do eleitorado em mensagens sob medida (Borgesius *et al.*, 2018). Por outro lado, críticas a essa ideia ressaltam que ela poderia prejudicar a comunicação legítima de candidaturas de nicho ou minoritárias, que dependem de alcançar grupos específicos (por exemplo, candidatos representantes de comunidades locais ou pautas temáticas). Além disso, uma vedação absoluta levantaria questionamentos jurídicos, podendo ser vista como restrição excessiva à livre expressão política e à estratégia de campanha - sobretudo se não houver evidências claras de dano causado pelo *microtargeting* em todos os contextos.

Como caminho intermediário, sugere-se permitir a segmentação apenas por critérios demográficos amplos e neutros, restringindo os demais. Por exemplo, adotar na legislação brasileira algo semelhante à política implementada pelo Google Ads (Montellaro, 2019), autorizando segmentação de anúncios eleitorais somente por idade, gênero e localização genérica (Meio & Mensagem, 2024). Dados comportamentais inferidos - como interesses, hábitos de consumo ou histórico de navegação - ficariam vedados para fins de direcionamento de propaganda política. Essa solução buscaria um equilíbrio: as campanhas ainda poderiam direcionar suas mensagens a públicos relativamente pertinentes (por exemplo, ajustar o conteúdo para eleitores jovens ou idosos, ou para determinadas regiões do país), mas sem recorrer a microperfilizações profundas baseadas em preferências pessoais ou tendências psicológicas. A consequência esperada seria reduzir significativamente o potencial de manipulação oculta e *microtargeted* de vulnerabilidades individuais, ao mesmo tempo mantendo alguma eficácia de segmentação legítima. Tudo que estivesse fora desse trilho seria ilegal e desafiaria a reação da Justiça Eleitoral.

Por fim, é essencial reforçar a dimensão da proteção de dados dentro das propostas regulatórias. As normas de proteção de dados já fornecem um arcabouço para coibir abusos - requerendo consentimento, definindo finalidades e impondo segurança no tratamento de informações pessoais (ANPD, 2024). No entanto, é preciso garantir sua aplicação efetiva no contexto eleitoral. Uma proposta é exigir que partidos e candidatos obtenham consentimento informado dos eleitores para inclusão em cadastros de propaganda direcionada, tornando explícito (por exemplo, no momento de um cadastro em site ou assinatura de apoiadores) que seus dados poderão ser usados para envio de mensagens de campanha (TSE; ANPD, 2021). Hoje, na prática, grande parte dos eleitores desconhece como seus dados chegaram às mãos de campanhas. Outra hipótese ainda mais radical é, de fato, incluir os partidos políticos sob supervisão direta da autoridade de dados - medida que o Canadá chegou a discutir, ao recomendar estender sua lei de privacidade para abranger as atividades dos partidos (Gaumond, 2020). No Brasil, isso significaria a ANPD atuar mais proximamente dos processos eleitorais, ainda que com foco nos períodos não eleitorais, em coordenação com a Justiça Eleitoral: podendo auditar bancos de dados eleitorais, emitir recomendações específicas e até aplicar sanções a partidos que tratem dados de maneira irregular (como vazar informações de eleitores ou usá-las fora da finalidade permitida).

4.3 FISCALIZAÇÃO E RESPONSABILIZAÇÃO

Não menos importante que criar normas é assegurar sua efetiva fiscalização e cumprimento. Assim, outra vertente fundamental das propostas diz respeito ao fortalecimento dos mecanismos de *enforcement* no que tange ao *microtargeting* eleitoral. Uma iniciativa inicial seria aprimorar a cooperação entre a Justiça Eleitoral e a Autoridade Nacional de Proteção de Dados (ANPD), de modo a fiscalizarem de forma coordenada o uso de dados de eleitores em campanhas. Já há uma atuação conjunta cristalizada no *Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) Por Agentes de Tratamento no Contexto Eleitoral* (ANPD; TSE, 2022), mas ainda há diversos outros campos a aprimorá-la. Neste sentido, a cooperação poderia envolver atuação adicional para monitorar as práticas de tratamento de dados antes, durante e após o período eleitoral (Privacy International, 2021). Por exemplo, identificadas evidências de uso indevido de cadastros de eleitores (como compra de bases de dados vazadas ou uso de dados pessoais sem consentimento) para *microtargeting*, a ANPD poderia instaurar procedimento sancionador e o Ministério Público Eleitoral poderia acionar a Justiça Eleitoral por violação da legislação eleitoral (Brasil, 2018). Essa atuação em dupla perspectiva ampliaria o risco para quem descumprisse as regras e daria uma resposta mais completa ao problema. De se ressaltar que a

atuação da ANPD e da Justiça Eleitoral deverá ser coordenada a partir da correta definição das atribuições de cada uma das esferas, o que passa necessariamente pela discussão dos limites entre o que está contido nos discursos e atividades estritamente eleitorais - diretamente submetidos ao escrutínio da Justiça Eleitoral, e o que não está.

Igualmente, sugere-se dotar a Justiça Eleitoral de ferramentas técnicas e equipes capacitadas para auditar campanhas on-line em tempo real (Privacy International, 2021). Isso pode envolver a criação efetiva, no âmbito do TSE, de uma unidade especializada em fiscalização de propaganda digital, com atribuição de analisar os relatórios de anúncios fornecidos pelas plataformas e os repositórios de anúncios impulsionados (TSE, 2024). Atualmente, o TSE tem seu foco nas atividades mais estritamente ligadas à desinformação e depende em grande medida das plataformas para fornecer informações; com uma equipe interna dedicada, seria possível cruzar dados, identificar comportamentos atípicos e requisitar esclarecimentos às campanhas de maneira ágil (International Idea, 2020). Tecnologias de monitoramento automatizado (inclusive inteligência artificial) podem ser aliadas: por exemplo, algoritmos podem vasculhar as bibliotecas de anúncios em busca de mensagens que contenham desinformação flagrante direcionada a certos públicos, sinalizando esses casos para revisão humana e eventual ação rápida (remoção do conteúdo ou direito de resposta).

No campo normativo, uma medida de responsabilização salutar seria explicitar sanções eleitorais para o uso ilícito de *microtargeting*. Atualmente, punir campanhas por abusos nessa seara requer enquadramentos genéricos, como abuso de poder econômico, ilícitos de propaganda ou mesmo corrupção eleitoral, dependendo do caso (Farias; Melo Neto, 2022). Seria mais eficaz inserir na legislação eleitoral dispositivos que tipifiquem condutas como: utilizar, em propaganda, dados pessoais de eleitores obtidos em desacordo com a lei; deixar de fornecer informações obrigatórias de transparência sobre anúncios segmentados; ou difundir deliberadamente desinformação mediante *microtargeting* (Bayer, 2020). Tais condutas poderiam acarretar penalidades proporcionais à gravidade - desde multas elevadas (no caso de simples descumprimento de transparência) até cassação do registro ou diploma (se comprovado que uma campanha venceu mediante uso massivo e irregular de dados para manipular eleitores). A existência de tipos sancionatórios claros teria um efeito pedagógico e dissuasório. A experiência internacional sugere que a ameaça de sanções concretas impulsiona o cumprimento: por exemplo, no Reino Unido, a investigação do ICO sobre *Cambridge Analytica* resultou na aplicação da multa máxima ao Facebook por violação da lei de dados, demonstrando que as autoridades estão dispostas a punir gigantes tecnológicos por complacência com abusos (ICO, 2018; NPR, 2019). A perspectiva de enfrentar penalidades eleitorais severas

certamente levaria campanhas e partidos a terem mais cautela no uso de *microtargeting*. Seria prudente, portanto, o redesenho de algumas infrações eleitorais previstas em lei para direcionar especificamente o seu foco às infrações eleitorais cometidas através das redes sociais (mas não só), tendentes a desequilibrar a igualdade e minar a autodeterminação política, admitindo que os esquemas tradicionais de responsabilização, baseados em noções como abuso de poder econômico e político, estão defasadas em relação à realidade contemporânea (Farias; Melo Neto, 2022).

Outra frente importante é investir em educação, capacitação e cooperação. A fiscalização eficaz envolve múltiplos atores: autoridades, plataformas, partidos, mídia e os próprios eleitores (International Idea, 2020). Deve-se promover capacitação técnica contínua dos servidores da Justiça e do Ministério Público eleitorais para acompanharem as inovações do marketing digital e entenderem as ferramentas de segmentação disponíveis. As plataformas de redes sociais, por sua vez, podem ser chamadas a colaborar de forma mais sistemática - por exemplo, entregando relatórios frequentes às autoridades com resumo de como foi feita a segmentação dos anúncios políticos em seus serviços (TSE, 2024). Já os eleitores e a imprensa podem atuar como fiscalizadores difusos, se municiados de informação e conscientização. Campanhas de esclarecimento público podem explicar ao cidadão como funciona o *microtargeting* e orientá-lo a consultar as bibliotecas de anúncios para verificar que tipos de mensagem cada candidato está veiculando (Farias; Melo Neto, 2022). Essa transparência ativa facilita que inconsistências venham à tona por meio do controle social. Em última análise, o esforço de responsabilização não recai apenas sobre punir *ex post*, mas também em prevenir: criar um clima normativo e cultural em que certas práticas abusivas sejam desencorajadas e consideradas ilegítimas (Bayer, 2020).

Em suma, a efetividade de quaisquer regras sobre *microtargeting* depende de uma fiscalização bem estruturada e de mecanismos de responsabilização proporcionais e dissuasórios (Privacy International, 2021). A experiência do escândalo *Cambridge Analytica* evidenciou que somente graças à atuação firme de autoridades e denunciantes foi possível revelar e coibir aquele esquema - que provavelmente teria continuado nas sombras de outro modo (ICO, 2018). Logo, para que as propostas regulatórias discutidas anteriormente (transparência e limites ao *microtargeting*) produzam os resultados desejados, é imprescindível dotar o sistema eleitoral brasileiro de meios para auditar, detectar e punir abusos no uso de dados e técnicas de segmentação durante as campanhas (Farias; Melo Neto, 2022).

5 CONCLUSÃO

A análise empreendida neste artigo evidenciou que o *microtargeting* em campanhas eleitorais coloca um dos dilemas regulatórios mais desafiadores da atualidade. De um lado, representa uma inovação nas estratégias de comunicação política, com potencial para tornar as campanhas mais eficientes e adequadas a diferentes segmentos do eleitorado; de outro, envolve riscos concretos de manipulação do debate público, violação da privacidade dos cidadãos e comprometimento da igualdade de condições nas disputas eleitorais. Os estudos de caso comparados mostraram abordagens bastante distintas: enquanto os Estados Unidos adotam uma postura permissiva, amparada em sua interpretação ampla da liberdade de expressão, a União Europeia avança no sentido de uma regulação estrita, fundamentada na proteção de dados e na transparência integral da propaganda personalizada. O Brasil, por sua vez, encontra-se em posição intermediária - com algumas normas gerais potencialmente aplicáveis, mas sem um arcabouço específico consolidado - o que torna particularmente relevante o debate sobre eventuais reformas legais e regulamentares.

Frente a esse panorama, defende-se a adoção de uma combinação de medidas que aumentem a transparência das campanhas digitais, imponham limites razoáveis à segmentação de eleitores e reforcem a fiscalização do uso de dados nas eleições. Regulamentar o *microtargeting* não equivale a tolher o debate político, mas sim a estabelecer garantias de que o uso das tecnologias de informação não subverta a integridade do processo eleitoral nem a autonomia do voto. Como bem colocam Borgesius *et al.* (2018), é necessário aprofundar a pesquisa e o debate sobre essas práticas emergentes, buscando soluções que equilibrem a inovação tecnológica com a preservação dos princípios democráticos.

Conclui-se, portanto, que uma regulamentação cuidadosa do *microtargeting* em campanhas eleitorais é não apenas desejável, mas indispensável para resguardar a legitimidade das eleições na era digital. Ao adotar algumas das propostas delineadas - maior transparência (com registros públicos de anúncios e identificação do *targeting*), restrições ao uso de dados sensíveis e à hiperpersonalização de mensagens, e mecanismos eficazes de responsabilização e fiscalização - o legislador e as autoridades eleitorais poderão inibir os abusos sem inviabilizar o uso responsável de ferramentas digitais pelas forças políticas. O desafio central reside em calibrar essas medidas de forma a proteger a democracia dos perigos da manipulação algorítmica, garantindo simultaneamente um ambiente propício ao livre debate e à participação política informada. Em última instância, enfrentar o *microtargeting* exige atualizar as regras do jogo eleitoral para que a concorrência pelo voto permaneça leal, transparente e assentada em ideias acessíveis a todos - e não em táticas invisíveis reservadas a poucos.

REFERÊNCIAS

ASCENSÃO, Rafael. Parlamento europeu dá luz verde a regulamento para tornar a propaganda política mais transparente. ECO, 27 fev. 2024. Disponível em: https://eco.sapo.pt/2024/02/27/parlamento-europeu-da-luz-verdade-a-regulamento-para-tornar-a-propaganda-politica-mais-transparente/. Acesso em: 29 mai. 2025.

BAYER, Judit. Double harm to voters: data-driven micro-targeting and democratic public discourse. Internet Policy Review, v. 9, n. 1, 2020. DOI: 10.14763/2020.1.1460.

BENNETT, Colin J. Voter databases, microtargeting, and data protection law: can political parties campaign in Europe as they do in North America? International Data Privacy Law, v. 6, n. 4, p. 261–275, 2016.

BERGHEL, Hal. Malice domestic: The Cambridge Analytica dystopia. 2018.

BLASI CASAGRAN, Carles; VERMEULEN, Mathias. Reflections on the murky legal practices of political micro-targeting from a GDPR perspective. International Data Privacy Law, v. 11, n. 4, 2021. Disponível em: https://www.researchgate.net/publication/354045670_Reflections_on_the_murky_legal_practices_of_political_micro-targeting_from_a_GDPR_perspective. Acesso em: 29 mai. 2025.

BORGESIUS, Frederik J. Zuiderveen; MÖLLER, Judith; KRUIKEMEIER, Sanne; Ó FATHAIGH, Ronan; IRION, Kristina; DOBBER, Tom; BODÓ, Balázs; DE VREESE, Claes. Online Political Microtargeting: Promises and Threats for Democracy. Utrecht Law Review, v. 14, n. 1, p. 82–96, 2018. Disponível em: https://utrechtlawreview.org/articles/10.18352/ulr.420. Acesso em: 29 mai. 2025.

BRASIL. Agência Nacional de Proteção de Dados Pessoais. Guia Orientativo: Aplicação da LGPD no Contexto Eleitoral. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_lgpd_final.pdf. Acesso em 29 mai. 2025.

BRASIL. Lei nº 13.488, de 6 de outubro de 2017. Altera as Leis nº 9.504/1997 (Lei das Eleições), 9.096/1995 e 4.737/1965 (Código Eleitoral), entre outras providências. Diário Oficial da União, 2017.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais (LGPD). Diário Oficial da União, 2018.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 18 de dezembro de 2019. Dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas

ilícitas em campanha eleitoral. Brasília: TSE, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 29 mai. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 27 de fevereiro de 2024. Altera a Resolução nº 23.610/2019 para disciplinar a propaganda eleitoral em plataformas digitais. Diário da Justiça Eletrônico, Brasília, 2024. Disponível no link da referência anterior.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 29 mai. 2025.

DA EMPOLI, Giuliano. Os engenheiros do caos: como as fake news, as teorias da conspiração e os algoritmos estão sendo utilizados para disseminar ódio, medo e influenciar eleições. São Paulo: Vestígio, 2019.

DOBBER, Tom; Ó FATHAIGH, Ronan; BORGESIUS, Frederik J. Zuiderveen. The regulation of online political micro-targeting in Europe. Internet Policy Review, v. 8, n. 4, 2019. Disponível em: https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe. Acesso em: 29 mai. 2025.

ERGA. Position Paper on the proposed Regulation on political advertising. Bruxelas: ERGA, 2022. Disponível em: https://erga-online.eu/wp-content/uploads/2022/09/2022-09-21_ERGA-PR_-Position-Paper-on-Political-advertising.pdf. Acesso em: 29 mai. 2025.

FARIAS, Rodrigo Nóbrega; MELO NETO, Afranio Neves de. Microtargeting eleitoral e os riscos à democracia representativa. Revista Justiça Eleitoral em Debate, Rio de Janeiro, v. 12, n. 2, p. 43–49, 2022.

GAUMOND, E. Is Canadian Law Better Equipped to Handle Disinformation? Lawfare, 11 dez. 2020. Disponível em: https://www.lawfaremedia.org/article/canadian-law-disinformation. Acesso em: 29 mai. 2025.

INFORMATION COMMISSIONER'S OFFICE. Investigation into the use of data analytics in political campaigns. London: ICO, 2018. Disponível em: https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf. Acesso em: 29 mai. 2025.

INTERNATIONAL IDEA. Webinar Series: Online Political Advertising and Microtargeting.

Stockholm: International IDEA, 2020. Disponível em: https://www.idea.int/sites/default/files/reference_docs/report-%20webinar-%20series-on-political-advertising-June-2020.pdf. Acesso em: 29 mai. 2025.

INTERNETLAB. Dados pessoais em campanhas políticas: recomendações para o Brasil. São Paulo: InternetLab, 2022. Disponível em: https://internetlab.org.br/pt/biblioteca/relatorio-protecao-de-dados-pessoais-e- eleicoes/. Acesso 29 mai. 2025.

KING, Jack. Microtargeted Political Ads: An Intractable Problem. Boston University Law Review, v. 102. Disponível em: https://www.bu.edu/bulawreview/files/2022/04/KING.pdf. Acesso em: 29 mai. 2025.

KROTOSZYNSKI, Ronald J. Big Data and the electoral process in the United States. Constitutional constraint and limited data privacy regulations. *In:* WITZLEB, Norman; PETERSON, Moira; RICHARDSON, Janice (org.). Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting. New York: Routledge, 2020.

McDONAGH, Maeve. Freedom of processing of personal data for the purpose of electoral activities after the GDPR. *In:* WITZLEB, Norman; PETERSON, Moira; RICHARDSON, Janice (org.). Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting. New York: Routledge, 2020.

MEIO & MENSAGEM. Google proíbe anúncios de conteúdo político no Brasil. Meio & Mensagem, 24 abr. 2024. Disponível em: https://www.meioemensagem.com.br/midia/google-proibe-anuncios-de-conteu do-politico-no-brasil. Acesso em: 29 mai. 2025.

MONTELLARO, Zach. Google to limit targeted political ads as Silicon Valley grapples with 2020. Politico, 20 nov. 2019. Disponível em: https: //www.politico.com/news/2019/11/20/google-political-ads-targeting-072352. Acesso em: 29 mai. 2025.

PARISIER, Eli. The Filter Bubble: How the New Personalized Web is Changing What we Read and How We Think. Londres: Penguin, 2011.

PRIVACY INTERNATIONAL. Micro-targeting in political campaigns: A comparative analysis of legal frameworks. London: Privacy International, 2021. Disponível em: https://privacyinternational.org/sites/default/files/2021-01/UoE_PI%20Micro-targeting%20in%20policital%20campaigns%20comparative%20analysis%202021.p df. Acesso em: 29 mai. 2025.

RAUCH, Daniel. Customized Speech and the First Amendment. Harvard Journal of Law & Technology. v. 35, 2022. Disponível em: http://dx.doi.org/10.2139/ssrn.3937435. Acesso em: 29 mai. 2025.

SAURA GARCÍA, Carlos Saura. Microtargeting político y vigilancia social masiva: impactos negativos en las democracias occidentales. Daimon. Revista Internacional de Filosofía, n. 93, p. 73-89, 2024. DOI: 10.6018/daimon.609851.

UNIÃO EUROPEIA. Conselho da União Europeia. EU introduces new rules on transparency and targeting of political advertising. Press release: Bruxelas, 11 mar. 2024. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2024/03/11/eu-introdu ces-new-rules-on-transparency-and-targeting-of-political-advertising/. Acesso em: 29 mai. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho, de 13 de março de 2024, sobre a transparência e o direcionamento da propaganda política. Jornal Oficial da União Europeia, L 900, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 29 mai. 2025.

UNITED KINGDOM. Information Commissioner's Office (ICO). Democracy disrupted? Personal information and political influence. Report, 11 jul. 2018. Disponível em: https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf. Acesso em: 29 mai. 2025.

UNITED KINGDOM PARLIAMENT. DCMS COMMITTEE. Disinformation and 'fake news': Final Report. Londres: UK Parliament, fev. 2019. Disponível em: https://committees.parliament.uk/work/6330/disinformation-and-fake-news/. Acesso em: 29 mai. 2025.

WITZLEB, Norman; PETERSON, Moira e RICHARDSON, Janice (org.). Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting. New York: Routledge, 2020.