UNIVERSIDADE FEDERAL DO CEARÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
CURSO DE MESTRADO

LUCIANA CARNEIRO DE OLIVEIRA

DEMOCRACIA HACKEADA: O USO DE DADOS PESSOAIS EM CAMPANHAS ELEITORAIS E AS GARANTIAS PREVISTAS NOS REGULAMENTOS GERAIS DE PROTEÇÃO DE DADOS PESSOAIS

FORTALEZA
2023

LUCIANA CARNEIRO DE OLIVEIRA

DEMOCRACIA HACKEADA: O USO DE DADOS PESSOAIS EM CAMPANHAS ELEITORAIS E AS GARANTIAS PREVISTAS NOS REGULAMENTOS GERAIS DE PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada à Coordenação do Programa de Pós-Graduação em Direito da Universidade Federaldo Ceará, como requisito parcial para obtenção do título de Mestre em Direito. Área de concentração: Ordem jurídica constitucional.

Orientadora: Prof. Dra. Raquel Cavalcanti Ramos Machado.

FORTALEZA

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

O48d Oliveira, Luciana Carneiro de.
Democracia hackeada : o uso de dados pessoais em campanhas eleitorais e as garantias previstas nos regulamentos gerais de proteção de dados pessoais / Luciana Carneiro de Oliveira. – 2023.
105 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Faculdade de Direito, Programa de Pós-Graduação em Direito, Fortaleza, 2023.
Orientação: Profa. Dra. Raquel Cavalcanti Ramos Machado.

1. Privacidade. 2. Proteção de dados. 3. Microssegmentação. 4. Política. 5. Campanhas eleitorais. I. Título.

CDD 340

LUCIANA CARNEIRO DE OLIVEIRA

DEMOCRACIA HACKEADA: O USO DE DADOS PESSOAIS EM CAMPANHAS ELEITORAIS E AS GARANTIAS PREVISTAS NOS REGULAMENTOS GERAIS DE PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada à Coordenação do Programa de Pós-Graduação em Direito da Universidade Federal do Ceará, como requisito parcial para obtenção do título de Mestre em Direito. Área de concentração: Ordem jurídica constitucional.

Aprovada em: 27/11/2023.

BANCA EXAMINADORA

_____

Profa. Dra. Raquel Cavalcanti Ramos Machado (Orientadora)
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. William Paiva Marques Júnior
Universidade Federal do Ceará (UFC)

_____

Profa. Dra. Marilda de Paula Silveira
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)

Em memória à minha tia Sula, cuja sabedoria iluminou meu caminho e me inspirou em cada etapa da vida.

AGRADECIMENTOS

Primeiramente, agradeço a Deus, cuja misericórdia infinita me permitiu trilhar o caminho do Mestrado em Direito Constitucional na Universidade Federal do Ceará. Estendo minha gratidão à Nossa Senhora, minha guia e protetora, que sempre me amparou.

A minha mãe, Lúcia, e minha tia-mãe, Celene, por serem apoios constantes em todos os meus projetos. Vocês são minha força, meus exemplos e minhas maiores incentivadoras. Tudo o que alcancei até aqui, devo em grande parte a vocês.

Ao meu querido amigo, Carlos Alberto Aragão, que desempenha um papel paternal em minha vida e é uma fonte inestimável de incentivo, minha sincera gratidão por tudo o que fez por mim ao longo dos anos. Seu apoio foi fundamental em minha jornada acadêmica e pessoal.

Aos meus irmãos, Felipe, Fernando e Larissa, e aos meus sobrinhos, Davi, Bento, Cecília e Martin, essências da minha vida. Cada sucesso que alcanço é também dedicado a vocês. Peço desculpas pelas vezes em que estive ausente devido aos meus compromissos profissionais e acadêmicos.

Aos meus amigos, David Sobreira e Samuel Martins, quero expressar minha profunda gratidão por terem sido fontes constantes de inspiração e apoio. Essa vitória também é de vocês.

Às minhas amigas do Mestrado, Lilian Order e Amanda Simões, por estarem ao meu lado e tornarem este sonho possível. Obrigada por tudo.

Quero agradecer à minha valiosa rede de apoio, composta por amigos e familiares, que cuidaram e apoiaram-me em todos os aspectos da minha vida. Sem vocês, esta conquista não teria sido possível.

Por fim, minha sincera gratidão à minha orientadora, Profa. Dra. Raquel Cavalcanti Ramos Machado, por sua dedicação incansável e valiosas contribuições ao meu trabalho. Agradeço também aos Professores da Banca, Prof. Dr. William Paiva Marques Júnior e Profa. Dra. Marilda de Paula Silveira, por aceitarem o convite e por serem inspirações na docência. Essa jornada acadêmica foi enriquecida pela sabedoria de todos vocês.

RESUMO

Com a evolução tecnológica e o advento da era digital, o fluxo de informações tem crescido exponencialmente, fazendo com que os dados pessoais se tornem uma valiosa *commodity*. Nesse contexto, tanto empresas como governos buscam maneiras de explorar essas informações, seja para fins comerciais, seja para orientações estratégicas. Por outro lado, o indivíduo, detentor primário desses dados, frequentemente se vê inserido em uma complexa rede onde sua privacidade e identidade podem estar em risco. Assim, a crescente digitalização mundial transformou os dados pessoais na nova moeda de troca, possibilitando a criação de perfis altamente detalhados para direcionamento de conteúdo. Essa realidade tem impactos significativos não apenas no campo do marketing e da publicidade, mas também levanta preocupações quanto à disseminação de desinformação, manipulação de opiniões e potenciais ameaças à democracia, especialmente em contextos eleitorais. Paralelamente, surge a questão da Internet das Coisas (IoT), que, ao ampliar a coleta de informações, reacende debates sobre privacidade e segurança de dados. Apesar da existência da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, muitos ainda desconhecem os riscos associados ao uso de suas informações. Este estudo visa entender como as garantias de proteção de dados influenciam o Estado Democrático de Direito e como se relacionam com o Direito Eleitoral. Busca-se realçar a importância dessas garantias para a consolidação democrática e ponderar sobre seus impactos em futuros contextos eleitorais. São propostas recomendações de boas práticas para campanhas eleitorais baseadas nas leis de proteção de dados do Brasil e da União Europeia. Essas recomendações são apresentadas não como soluções definitivas, mas como alicerces para o desenvolvimento de marcos regulatórios que harmonizem as complexidades do ambiente digital.

Palavras-chave: Privacidade. Proteção de Dados. LGPD. Microssegmentação Política. Campanhas eleitorais.

ABSTRACT

With technological evolution and the advent of the digital era, the flow of information has grown exponentially, making personal data a valuable *commodity*. In this context, both companies and governments are looking for ways to exploit this information, whether for commercial purposes or for strategic guidance. On the other hand, the individual, the primary holder of this data, often finds themselves inserted into a complex network where their privacy and identity may be at risk. Thus, increasing global digitalization has transformed personal data into the new currency of exchange, enabling the creation of highly detailed profiles for content targeting. This reality has significant impacts not only in the field of marketing and advertising, but also raises concerns about the spread of misinformation, manipulation of opinions and potential threats to democracy, especially in electoral contexts. At the same time, the issue of the Internet of Things (IoT) arises, which, by expanding the collection of information, reignites debates about privacy and data security. Despite the existence of the General Personal Data Protection Law (LGPD) in Brazil, many are still unaware of the risks associated with the use of their information. This study aims to understand how data protection guarantees influence the Democratic Rule of Law and how they relate to Electoral Law. The aim is to highlight the importance of these guarantees for democratic consolidation and consider their impacts in future electoral contexts. Recommendations of good practices for electoral campaigns based on data protection laws in Brazil and the European Union are proposed. These recommendations are presented not as definitive solutions, but as foundations for the development of regulatory frameworks that harmonize the complexities of the digital environment.

Keywords: Privacy. Data Protection. LGPD. Political Microtargeting. Election campaigns.

SUMÁRIO

1 INTRODUÇÃO

Em um mundo cada vez mais digitalizado, os dados pessoais se tornaram a nova moeda de troca. Estes, quando manipulados por algoritmos sofisticados, são capazes de criar perfis detalhados, direcionando conteúdos sob medida para cada indivíduo. Ao mesmo tempo em que essa estratégia revoluciona a publicidade e o marketing, também abre espaço para a disseminação de desinformação e manipulação de opiniões, ameaçando o cerne da democracia. Esse cenário se acentua ainda mais em contextos eleitorais, onde a influência sobre os eleitores pode determinar os rumos de uma nação.

A constante evolução digital e a utilização estratégica de dados na criação de perfis de consumidores são evidências da forma como a tecnologia está remodelando nosso mundo. Nessa linha de pensamento, a Internet das Coisas (IoT) apresenta-se como um avanço que estende ainda mais essa capacidade de coleta e análise de informações, trazendo à tona novos debates e desafios. Por um lado, tem-se a possibilidade de um ecossistema mais integrado e funcional, onde objetos comunicam-se entre si e facilitam a vida cotidiana. Por outro, esse cenário amplia as questões sobre privacidade e segurança de dados, visto que a disseminação de sensores e dispositivos amplifica a gama de informações que pode ser coletada e potencialmente mal utilizada. Este ponto de inflexão nos faz questionar até onde estamos dispostos a ir em nome da conveniência, e se as legislações atuais estão preparadas para proteger os direitos dos cidadãos nesse ambiente hiperconectado.

Neste cenário tecnológico transformador, é imperativo reconhecer que as informações individuais detêm uma dualidade. Por um lado, exibem uma dimensão existencial, manifestada principalmente na preservação da privacidade e identidade do ser humano, oriunda da proteção da sua dignidade. Paralelamente, esses dados detêm uma faceta patrimonial, reconhecida pela capacidade de utilizar essas informações como matéria-prima para iniciativas comerciais em diversos setores. Esta dimensão é identificada como a monetização de dados, traduzindo-se na transformação de informação em capital. Assim, além da necessidade de salvaguardar direitos extrapatrimoniais, como privacidade e identidade, torna-se relevante observar a perspectiva patrimonial dessas informações, pilar central dos modelos de negócio adotados por protagonistas no âmbito eleitoral.

A Lei Geral de Proteção de Dados Pessoais (LGPD) surgiu como uma resposta jurídica à crescente preocupação com a privacidade e o uso de dados. Entretanto, mesmo com tal regulamentação, muitos indivíduos ainda carecem de conhecimento sobre os potenciais riscos e implicações associados à coleta e uso de suas informações.

O presente estudo se justifica pela imperativa análise do impacto do novo paradigma de marketing eleitoral, fundamentado nas novas plataformas e mídias sociais, sobre a democracia tal como a conhecemos. A pertinência desse questionamento é evidenciada por episódios emblemáticos como o Brexit, a eleição de Donald Trump e a ascensão de líderes de extrema-direita ao redor do mundo.

O trabalho em tela, inserido na intersecção entre tecnologia, direito, sociologia, marketing e política, propõe uma reflexão sobre a efetividade das garantias presentes nos regulamentos de proteção de dados no contexto eleitoral. Assim, investiga-se o potencial impacto dessas regulações na salvaguarda do Estado Democrático de Direito e a necessidade de um diálogo construtivo com o Direito Eleitoral.

Sua relevância não se limita ao âmbito acadêmico, mas se estende à esfera político-social, especialmente quando consideramos a proteção de dados como pilar para uma participação política autêntica no Estado Democrático de Direito.

Ademais, faz-se necessário que a comunidade acadêmica se debruce sobre as reverberações dessas transformações sociais e busque maneiras de regulamentar os mecanismos emergentes. Sem essa reflexão, corremos o risco de ver a essência da democracia ser subvertida por uma manipulação tecnológica que desvirtua o conceito de representação política.

Neste contexto, a questão problema que norteará este estudo é a seguinte: como as garantias estabelecidas nos regulamentos gerais de proteção de dados pessoais impactam o fortalecimento do Estado Democrático de Direito, e de que forma elas podem estabelecer um diálogo construtivo com as premissas do Direito Eleitoral?

Nesse sentido, o objetivo geral é investigar como as garantias oferecidas pelos regulamentos de proteção de dados pessoais influenciam a consolidação do Estado Democrático de Direito e estabelecer uma inter-relação construtiva com os fundamentos do Direito Eleitoral.

Já como objetivos específicos, busca-se avaliar a evolução do direito à privacidade e a legislação brasileira sobre proteção de dados pessoais; examinar a interação entre a proteção de dados pessoais e a legislação eleitoral, destacando os principais agentes envolvidos; e analisar os desafios da proteção de dados no cenário político-eleitoral, com uma atenção especial voltada para a técnica de microssegmentação política online.

O trabalho está estruturado em três capítulos. O primeiro aborda o tema da privacidade e proteção de dados pessoais, iniciando com uma discussão sobre o direito fundamental à privacidade. Em seguida, discute-se o direito fundamental à proteção de dados pessoais, e, por fim, examina-se a legislação brasileira específica sobre dados pessoais.

O segundo capítulo estabelece uma conexão entre a proteção de dados pessoais e o direito eleitoral. Primeiramente, analisa-se o uso de dados pessoais dentro da legislação eleitoral. A partir disso, é apresentada uma visão eleitoral dos princípios que regem a proteção de dados pessoais. O texto identifica, então, as principais bases legais para o tratamento de dados pessoais em campanhas eleitorais e conclui discutindo o papel dos agentes de tratamento de dados pessoais, do encarregado e da Autoridade Nacional de Proteção de Dados Pessoais no ambiente eleitoral.

Por fim, no terceiro capítulo, o foco se volta para a salvaguarda da democracia em face dos riscos digitais. Os desafios relacionados à proteção de dados pessoais no cenário político-eleitoral são inicialmente explorados, seguidos por uma discussão sobre a microssegmentação política eleitoral, uma técnica avançada que usa dados para segmentar e direcionar mensagens a eleitores específicos. Na conclusão do capítulo são apresentadas recomendações de boas práticas para campanhas eleitorais, considerando os regulamentos de proteção de dados, a fim de contribuir para um ambiente eleitoral mais seguro e transparente.

Nesta dissertação, adota-se uma abordagem exploratória, descritiva e interpretativa, de cunho qualitativo, fundamentada na análise de fontes bibliográficas e documentos. Utiliza-se o método dedutivo como uma ferramenta analítica central.

A presente pesquisa almeja evidenciar a relevância das garantias estabelecidas nos regulamentos de proteção de dados pessoais para a consolidação do Estado Democrático de Direito. Ademais, sob um prisma político-eleitoral, busca-se analisar de que maneira a aplicação destas normativas poderá impactar futuros pleitos eleitorais. Não se pretende, contudo, oferecer uma solução abrangente para todos os desafios relacionados à temática, mas, sim, aprofundar-se em sua importância e implicações.

2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Como uma das bases da democracia e da representatividade popular, o processo eleitoral brasileiro tem envidado esforços para garantir a privacidade e a proteção de dados pessoais, como forma de primar pela autodeterminação informativa e pela lisura das eleições. Por outro lado, embora estejam positivados em nosso ordenamento constitucional como direitos fundamentais, esses direitos vêm sendo objeto de constantes abusos por parte de candidatos, partidos e seus respectivos militantes, demandando uma atuação cada vez mais ativa do legislador e do Poder Judiciário.

Nessa esteira, compreender as bases do sistema jurídico europeu e brasileiro, bem como as questões constitucionais e legais atinentes ao tema em estudo, revela-se como primeiro passo para identificar os gargalos na efetivação dessas garantias, bem como para se pensar e discutir as melhores soluções para corrigir as distorções evidenciadas.

2.1 O direito fundamental à privacidade

Ao longo da história, em diferentes sociedades, o conceito de privacidade foi objeto de múltiplas interpretações. Contudo, foi apenas no final do século XIX que a privacidade começou a ser moldada de forma mais tangível pelo sistema jurídico, ganhando destaque e reconhecimento (Doneda, 2020).

Na Inglaterra, o emblemático caso entre Alexander Pope e Jonathan Swift evidenciou a essencialidade da proteção à correspondência privada. Naquela época, a troca de cartas era uma das principais formas de comunicação, e muitas dessas cartas continham pensamentos íntimos, opiniões políticas e informações pessoais. A divulgação não autorizada de suas cartas desencadeou um processo judicial, culminando em uma decisão favorável a Pope. Este marco jurídico solidificou o entendimento sobre a sacralidade das correspondências privadas e a imperatividade de sua proteção contra exposições indevidas (Blackstone, 1765).

Em terras francesas, o episódio envolvendo a atriz Elisa Rachel Félix destacou a necessidade de salvaguardar a privacidade em momentos íntimos, como o leito de morte. A exposição de imagens da atriz nesse contexto vulnerável motivou sua irmã a buscar amparo legal para interromper tal exposição, alegando o profundo sofrimento da família. A decisão judicial foi favorável, sublinhando a primazia do respeito à privacidade e à dignidade humana, mesmo em circunstâncias extremas (Lindon, 1974).

Na Itália, os debates em torno da exposição de aspectos íntimos da relação entre Clara Petacci e Benito Mussolini ressaltaram a importância do direito à privacidade. A revelação desses detalhes íntimos suscitou debates e embates judiciais, reiterando que a privacidade deve ser assegurada a todos, inclusive àqueles em posições de destaque público (Auletta, 1978).

Com o avanço social e tecnológico, novas facetas do direito à privacidade emergiram, acompanhadas de novos desafios e dilemas. Discussões sobre biografias não autorizadas e o complexo enquadramento da privacidade no mundo contemporâneo de dados, exemplificado pela "Internet das Coisas" *(Internet of things* - IoT*)*, tornaram-se questões predominantes na área. Esses avanços requerem uma constante reflexão sobre como proteger e equilibrar o direito à privacidade em uma sociedade em constante mudança.

Historicamente, a noção de privacidade tem sido esculpida com base no contraste entre o público e o privado (Lafer, 1988). Essa dualidade destaca a distinção entre aspectos da vida que pertencem ao domínio íntimo, protegidos de olhares externos, e aqueles que se situam no âmbito público, estando assim mais expostos e regulamentados.

É dentro do recinto privado que os indivíduos encontram um espaço seguro para introspecção, reflexão crítica e autoconhecimento. Nesse refúgio, as pessoas têm a liberdade de construir pensamentos, formar opiniões e expressar sentimentos sem o peso do escrutínio alheio. Essa introspecção prepara os indivíduos para se engajarem de forma mais ponderada e informada no espaço público, enriquecendo o diálogo democrático.

Por outro lado, o espaço público é onde as ideias são trocadas, debatidas e, muitas vezes, postas à prova. A capacidade de um indivíduo de se retirar para o espaço privado, refletir e depois retornar ao debate público com perspectivas renovadas é um pilar fundamental para a sustentação de uma democracia saudável. Como Bioni (2020) destaca, a privacidade está intrinsecamente ligada ao desenvolvimento da identidade individual e, por extensão, ao fortalecimento do tecido democrático da sociedade.

Para compreender o conceito de privacidade, é imperioso entender o surgimento dessa expressão. Assim, verifica-se a necessidade de analisar, sucintamente, o texto *"The Right to Privacy"*, dos então advogados norte-americanos Warren e Brandeis, que surgiu, à época, como resposta às invasões perpetradas pela imprensa na vida privada das pessoas. O texto continua relevante na atualidade, sendo uma das grandes referências sobre o tema (Warren, Brandeis, 1890).

A partir desse texto, a ideia de que os indivíduos possuem o direito de controlar as suas próprias informações começou a ganhar força. Os autores introduziram no léxico legal o conceito do "direito de ser deixado em paz" (*right to be let alone*). Ao analisarem vários casos

judiciais relacionados à propriedade, aos direitos autorais e à difamação, Warren e Brandeis reconheceram a necessidade de um direito geral à privacidade (Warren, Brandeis, 1890).

Os autores chamaram a atenção também para os riscos que a privacidade enfrentava devido aos avanços tecnológicos do final do século XIX (Warren, Brandeis, 1890). Embora a tecnologia da informação traga muitos benefícios, a exemplo dos ganhos de produtividade, é importante estar ciente das ameaças que podem dela decorrer, especialmente no que diz respeito à proteção da privacidade.

Além disso, Warren e Brandeis (1890) defenderam uma abordagem dinâmica e adaptável ao direito à privacidade. Eles acreditavam que referido direito não era estático, mas, sim, um direito que evoluía juntamente com as mudanças sociais e tecnológicas. Por fim, postularam que, embora a privacidade pudesse ser violada de muitas maneiras, a proteção legal deveria se concentrar em proibir interferências indesejadas e danosas.

Dessa forma, essas reflexões iniciais sobre o direito à privacidade foram fundamentais ao desenvolvimento posterior desse direito, fornecendo uma base conceitual e ética para sua compreensão e aplicação. Os estudos subsequentes ampliaram o campo de abrangência da privacidade, abordando questões emergentes e refletindo sobre as transformações sociais e tecnológicas que afetam a privacidade individual.

A Constituição Federal de 1988 consagra e protege o direito à privacidade, à intimidade e à inviolabilidade de dados, escolha que reflete a importância intrínseca desses elementos para a dignidade e personalidade humanas. Há situações, contudo, em que a privacidade deve ser ponderada com outros direitos e interesses coletivos, sendo essa ponderação um exercício delicado e fundamental no Estado Democrático de Direito (Barroso, 2012).

Em questões de segurança pública, por exemplo, a proteção da privacidade individual pode precisar ser ponderada em relação à necessidade de investigações criminais ou proteção da sociedade como um todo. Nesses casos, é necessário encontrar um equilíbrio entre a necessidade de coletar informações pessoais para fins de segurança e o respeito aos direitos à privacidade e à presunção de inocência.

A consagração de um direito como fundamental em uma constituição, a exemplo do direito à privacidade, atribui-lhe uma posição de destaque no sistema jurídico. Direitos fundamentais são vistos como direitos humanos com elevado grau de proteção, sendo primordiais para a dignidade, liberdade e autodeterminação dos cidadãos.

Nessa esteira, Norberto Bobbio (1992) explica que os direitos humanos, por mais fundamentais que sejam, são direitos históricos. Isso significa que surgiram em momentos específicos e são marcados por confrontos em defesa de novas liberdades contra os poderes

preexistentes, tendo sua consolidação ocorrido de formal gradual, isto é, nem de uma vez por todas e nem todos de uma vez.

De acordo com a visão de Robert Alexy, é necessário proteger não apenas a saúde e a vida como direitos fundamentais, mas também outros direitos, como liberdade, dignidade, propriedade e família. Essa proteção pode assumir diversas formas, incluindo normas do direito penal, responsabilidade civil, direito processual, atos administrativos e medidas práticas. A diversidade dessas formas de proteção está ligada ao fato de que os direitos a serem protegidos são prerrogativas constitucionais e medidas positivas fáticas ou normativas em relação ao Estado. O propósito é delimitar as esferas dos sujeitos de direito que estão em posição hierárquica igual, garantindo a efetividade e exigibilidade dessa demarcação (Alexy, 2008).

Tomando por base a análise da lei ordinária, verifica-se que o direito à privacidade também é um direito da personalidade. O artigo 21 do Código Civil de 2002, que faz parte do capítulo intitulado “Dos Direitos da Personalidade”, estabelece a inviolabilidade da vida privada (Brasil, 2002).

Os direitos da personalidade desempenham um papel fundamental na proteção dos atributos mais íntimos e inerentes do ser humano, abrangendo aspectos como a honra, a imagem, a integridade física e moral e, é claro, a privacidade.

Segundo William Marques Júnior (2018), nota-se uma interdependência entre os direitos da personalidade e os direitos fundamentais, já que muitos deles possuem dupla caracterização: são tanto da personalidade quanto fundamentais (como é o caso da privacidade, honra e imagem). Contudo, é importante não confundir os conceitos, visto que os direitos da personalidade se referem às relações entre indivíduos, enquanto os direitos fundamentais estabelecem diretrizes no âmbito do direito público.

Para Maria Helena Diniz (2007), esses direitos são considerados inalienáveis e inerentes à própria existência e dignidade humanas. Isso significa que tais direitos não podem ser vendidos ou transferidos ou renunciados, pois são fundamentais e acompanham o indivíduo desde o nascimento até o fim da vida. Eles emanam da própria natureza humana e são essenciais para garantir o respeito e a justiça em qualquer sociedade. Tais direitos têm caráter universal, sendo reconhecidos e exigíveis perante todos, garantindo, assim, a proteção da dignidade humana em qualquer contexto.

Através dessas reflexões, é possível constatar que os direitos da personalidade e, em particular, o direito à privacidade, são pilares no sistema jurídico brasileiro, atuando como defensores e promotores da dignidade humana. Levando-se em consideração as informações apresentadas até este ponto do trabalho, pode-se inferir que o direito à privacidade é um direito

fundamental e um direito da personalidade.

Conforme pontuado anteriormente, a Constituição de 1988 declara a inviolabilidade da intimidade e da vida privada nos termos do artigo 5º, inciso X. Quanto a este ponto, vale destacar um princípio básico da hermenêutica jurídica, segundo o qual "a lei não contém palavras inúteis" – a despeito da realidade, por vezes, mostrar-se diferente. Dessa forma, como o próprio texto constitucional faz distinção entre essas duas expressões, é possível concluir que as duas, vida íntima e vida privada, possuem objetos distintos (Brasil, 1988).

José Afonso da Silva (2020) distingue o direito à privacidade e à intimidade defendendo uma relação de continência, estando a intimidade incluída no conceito de privacidade. Dessa forma, a intimidade seria uma subcategoria da privacidade, sendo uma de suas facetas mais sensíveis e protegidas.

Ainda de acordo com José Afonso da Silva (2020), a existência humana se manifesta em duas dimensões: uma externa, relacionada às interações sociais e atividades públicas, que por serem públicas, podem ser acessadas e divulgadas por outros; e outra interna, que se refere ao âmbito pessoal, envolvendo a pessoa, sua família e amigos. Esta última representa a essência da vida privada, que, conforme os preceitos constitucionais, deve permanecer resguardada e inviolada.

A diferenciação entre as expressões também pode apresentar semelhanças com a teoria das esferas proposta por Robert Alexy (2008). A teoria é fundamentada na ideia de três esferas de diferentes tamanhos, em que a menor está contida dentro da esfera intermediária e esta, por sua vez, dentro da esfera maior.

Essas três esferas representam áreas distintas de atuação e interesse. A esfera menor representa o campo da intimidade, caracterizado pela máxima proteção. Nesse espaço, encontram-se as questões mais reservadas e secretas do indivíduo, estando fora do alcance das observações de terceiros. Essa esfera é considerada como absolutamente protegida, preservando a privacidade e a liberdade do sujeito em relação a aspectos íntimos e pessoais (Alexy, 2008).

Já a esfera mediana está associada ao plano privado, no qual o indivíduo compartilha certos assuntos com terceiros, baseado no fator confiança. Nessa esfera, há uma maior abertura para o compartilhamento de informações e vivências pessoais, porém ainda delimitada pela vontade e escolha do próprio sujeito (Alexy, 2008).

Por fim, a esfera maior relaciona-se ao campo social, abrangendo os assuntos que não são abarcados pelas esferas menores. Essa esfera envolve os aspectos mais públicos da vida do indivíduo, como suas interações sociais, participação em atividades coletivas e engajamento na esfera pública (Alexy, 2008).

Dessa forma, a teoria de Alexy estabeleceu uma divisão hierárquica entre as esferas, reconhecendo que certas áreas têm uma abrangência maior do que outras. Cada esfera abarca diferentes aspectos da vida humana, com suas próprias normas e limites. Essa diferenciação permitiu uma compreensão mais precisa das diferentes dimensões da vida pessoal, social e pública (Alexy, 2008).

Outra teoria das esferas pode ser descrita por António Menezes Cordeiro, que a definiu da seguinte forma:

> Assim, teríamos, sucessivamente: a) uma esfera pública: própria de políticos, atores, desportistas ou outras celebridades, ela implicaria uma área de condutas propositadamente acessível ao público, independentemente de concretas autorizações; b) uma esfera individual-social: reporta-se ao relacionamento social normal que as diversas pessoas estabelecem com amigos, colegas e conhecidos; c) uma esfera privada: tem a ver com a vida privada comum da pessoa: apenas acessível ao círculo da família ou dos amigos mais estreitos, equiparáveis a familiares; d) uma esfera secreta: abrange o âmbito que o próprio tenha decidido não revelar a ninguém; desde que o momento em que ele observe a discrição compatível com tal decisão, esta esfera tem absoluta tutela; e) uma esfera íntima: reporta-se à vida sentimental ou familiar no sentido mais estrito (cônjuge e filhos); tem uma tutela absoluta, independentemente de quaisquer prévias decisões, nesse sentido, do titular considerado; elas são dispensáveis (Cordeiro, 2007, p. 240-1).

Por meio dessas teorias, entende-se que privacidade e intimidade possuem diferentes cargas de valor. Embora a Constituição Federal de 1988 não forneça uma definição objetiva e não mencione a teoria das esferas, é importante reconhecer uma certa semelhança que auxilia na compreensão das diferenças de conteúdo entre essas expressões.

Dessa forma, a privacidade possui uma conceituação complexa e de difícil delimitação. Nesse estudo, não se busca reformular a definição de privacidade, mas, sim, recuperar exclusivamente sua essência, que trata de um direito cercado pela dicotomia entre o privado e o público e consubstanciado como uma liberdade negativa. Tem-se, portanto, um direito estático, aguardando que o seu titular estabeleça quais fatos da sua vida devem ficar fora do domínio público.

Por seu turno, o "progresso" do direito à privacidade, que abarcaria o direito à proteção de dados pessoais, residiria em uma tutela eivada de dinamismo e em uma liberdade positiva do controle sobre as informações pessoais. O domínio privado não seria algo já à espera de ser violado, mas sim um espaço construído e moldado dinamicamente por meio do controle das informações pessoais.

Portanto, ocorre uma mudança qualitativa. O foco, que anteriormente estava centrado no trinômio "pessoa-informação-sigilo", agora se expande para incorporar uma quarta

dimensão, resultando no quadro “pessoa-informação-circulação-controle”, conforme lição de Bioni (2020).

Essa nova abordagem reconhece que a privacidade não se limita apenas à proteção do sigilo das informações pessoais, mas também à regulação da circulação dessas informações e ao controle exercido sobre elas. Isso reflete a crescente importância das questões relacionadas à coleta, uso e compartilhamento de dados pessoais em um contexto de avanços tecnológicos e sociedade da informação.

Assim, a ideia clássica de privacidade deve coexistir com essa nova concepção, o que não significa que os direitos de proteção de dados pessoais devam ser reduzidos a uma mera evolução dos direitos de privacidade, conforme será explicado adiante (Bioni, 2020).

De fato, as discussões a respeito da privacidade giram, cada vez mais, em torno de questões relacionadas a dados pessoais. O papel da informação como paradigma para uma multiplicidade de situações jurídicas é flagrante, e sua notoriedade e relevância para as sociedades pós-industriais são igualmente evidentes.

2.2 O direito fundamental à proteção de dados pessoais

O caso do *National Data Center* é um exemplo que destaca a reação profunda de segmentos da sociedade à crescente capacidade e manejo da tecnologia da informação para processar dados pessoais em larga escala. Mais do que apenas um incidente isolado, esse caso simboliza uma transição na maneira como a informação é percebida e utilizada na estrutura sociopolítica. Representa as primeiras tentativas de estabelecer limites e controles sobre o uso da informação, destacando a necessidade emergente de equilibrar os benefícios da tecnologia com os direitos fundamentais à privacidade e proteção de dados pessoais.

Em meados de 1965, o Escritório do Orçamento dos Estados Unidos apresentou uma proposta que buscava aprimorar a estrutura administrativa. Essa iniciativa se tornou possível com o uso da informática e poderia ser considerada um avanço para a época, pois visava elaborar uma central de armazenamento única para as informações pessoais dos cidadãos norte-americanos, denominada *National Data Center*. Tal estrutura reuniria os dados provenientes de várias instituições da administração federal, como os do Censo, os provenientes dos registros trabalhistas, da Receita Federal e da previdência social, em um único banco de dados. O projeto tinha como objetivo unificar todos esses cadastros, que estavam fragmentados em diversos bancos de dados governamentais, dificultando a obtenção da eficácia da administração pública (Doneda, 2020).

Os criadores do *National Data Center*, embora tenham focado na eficiência por meio de um planejamento, não sopesaram as implicações do projeto para a privacidade dos cidadãos. Tal atitude provocou uma reação nos mais diversos setores da sociedade, que já manifestavam certo medo quanto à introdução de tecnologias computacionais em suas vidas (Doneda, 2020).

Na época em que tal questão foi discutida, os problemas decorrentes da concentração de dados pessoais em um único local eram muitos. Havia a preocupação de que uma quantidade desproporcional de poder pudesse ser concentrada nas mãos daqueles que controlavam esses sistemas computacionais. É inegável, no entanto, a praticidade de centralizar as informações dos cidadãos em um único banco de dados. A dispersão dessas informações em múltiplos locais tornava a pesquisa mais lenta e onerosa. Além disso, duplicar a mesma informação em diferentes bancos de dados resultava em esforço e gastos redundantes (Doneda, 2020).

Outras razões também podem ser citadas para explicar por que a unificação do centro de processamento de dados se tornou uma prioridade para o governo, tais como a racionalização das ações do Estado, a antecipação do desenvolvimento socioeconômico e a melhoria dos serviços prestados à população. Assim, sob uma certa ótica tecnocrata, unificar esse centro de processamento de dados era o caminho almejado (Doneda, 2020).

Apesar do insucesso do estabelecimento do *National Data Center*, diversos tópicos acerca de sua viabilidade ainda continuaram sendo discutidos. É fato que muitos outros bancos de dados pessoais, mesmo que em menores escalas, foram sendo estruturados (Doneda, 2020).

Em contraste, na Alemanha, mesmo antes da existência de uma lei federal que regulamentasse a proteção de dados pessoais, que só viria a existir em 1977, o país já mantinha uma cultura de preservação e garantia da privacidade em relação às informações pessoais (Doneda, 2020).

A realização de um censo na República Federal Alemã, em 1983, desencadeou uma série de preocupações em diversos setores da sociedade, principalmente no que se refere ao método de coleta e destinação dos dados. Essa situação motivou o julgamento, pelo Tribunal Constitucional Federal alemão *(Bundesverfassungsrichter)*, de um caso que até hoje é considerado um ponto de referência na história dos direitos de proteção dos dados pessoais (Doneda, 2020).

A Lei do Censo, aprovada em 1982, foi a base para a sentença proferida. Ela estabelecia que os cidadãos deveriam responder a 160 perguntas, as quais seriam posteriormente processadas por meio de computadores. A lei gerou grande discussão, visto que alguns pontos suscitaram controvérsias. Dentre eles, estava a possibilidade de os dados obtidos pelo censo serem confrontados com os do registro civil para uma eventual retificação, além da

possibilidade de transmissão desses dados, desde que não identificados, às autoridades federais e aos estados federados. Outras questões eram a existência de uma multa pecuniária alta para aqueles que não respondessem ao questionário e a criação de um mecanismo incentivador para denunciar essas pessoas (Doneda, 2020).

Tais fatores geraram um desconforto generalizado na sociedade, levando-a a acreditar que o governo poderia usar seus dados – inicialmente coletados para fins estatísticos – para exercer controle sobre ela. Essa situação desencadeou um litígio que culminou com a suspensão temporária do censo. O Tribunal Constitucional, então, ancorado nos artigos 1.1 e 2.1 de sua Lei Fundamental,[1] proferiu uma sentença declarando a inconstitucionalidade da lei que estabelecia o recenseamento (Doneda, 2020).

Após uma análise das razões que levaram a Corte a reconhecer a inconstitucionalidade da Lei do Censo, verificou-se que a principal delas foi a possível utilização simultânea dos dados recolhidos para fins administrativos e estatísticos. Uma vez que isso ocorresse, estaria configurada a diversidade de finalidades, o que impedia que o cidadão conhecesse o uso real dos dados por ele fornecidos (Doneda, 2020).

A sentença também destacou a importância de não subestimar o tratamento de certos tipos de dados quando se trata de garantir a privacidade. É preciso ter em mente que a coleta de dados vai além da simples natureza das informações. A utilidade e a necessidade dos dados são fundamentais e dependem tanto da finalidade para a qual serão processados quanto da capacidade de conexão e desenvolvimento da tecnologia da informação (Doneda, 2020).

O tratamento de dados pessoais, uma realidade cada vez mais presente em nosso cotidiano, tem transformado a maneira como compreendemos e utilizamos as informações disponíveis. Nesse contexto, salienta-se que o valor e o significado dos dados não precisam ser evidentes de imediato. Essa mudança de perspectiva indica que não existe mais um dado considerado irrelevante, uma vez que este pode adquirir valor em novos contextos ou em combinação com outras informações.

Referido julgamento também revelou a influência da tecnologia nos danos à personalidade causados pela formação de perfis individuais com base nos dados coletados no censo (Doneda, 2020). Devido aos avanços na área da informática, tornaram-se possíveis violações de direitos fundamentais básicos. Atualmente, a ampla capacidade tecnológica de armazenar e cruzar informações pessoais é amplamente reconhecida. Quando esses dados são

[1] Em tradução livre: “Artigo 1.1 A dignidade da pessoa humana é intangível. Respeitá-la e protegê-la é obrigação de todo o poder público. [...] Artigo 2.1 Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral”.

combinados e analisados, podem resultar em perfis pessoais altamente personalizados, muitas vezes sem que os titulares dos dados tenham controle sobre essa situação.

Por fim, a sentença enfatizou o direito à autodeterminação informativa, que representa uma referência significativa para o sistema jurídico alemão e tem influenciado diversos países do sistema romano-germânico. Além disso, esse conceito é um dos pilares fundamentais da Lei Geral de Proteção de Dados Pessoais brasileira (Doneda, 2020).

Esse direito consiste na capacidade de o indivíduo controlar ativamente o tratamento de seus dados pessoais, permitindo-lhe tomar decisões sobre como suas informações serão coletadas, usadas, armazenadas e compartilhadas. Portanto, ter controle sobre esses dados é equivalente a ter controle sobre aspectos significativos da própria vida.

Na tradição democrática alemã, a autodeterminação informativa se enraíza na afirmação do personalismo, mas também na participação social de cada cidadão (Doneda, 2020). Em um regime democrático, a participação ativa dos indivíduos é de suma importância para a tomada de decisões coletivas e o bem-estar de todos. Quando as pessoas têm o poder de decidir como suas informações são tratadas, elas podem se sentir mais seguras e confiantes em compartilhar seus pontos de vista e se envolver em debates e processos políticos. Essa é uma questão muitas vezes subestimada, mas necessária para garantir a liberdade e a autonomia de todos.

Além disso, é importante notar que o Tribunal Constitucional alemão não tomou como base a distinção entre o que é público e privado para estabelecer o direito à autodeterminação informativa. Ao invés disso, superando tal dicotomia, sustentou que a utilização dos dados pessoais não deve afetar o livre desenvolvimento da personalidade dos indivíduos. Para isso, era necessário garantir aos cidadãos um maior controle sobre seus dados, bem como prevenir-los de práticas de discriminação social (Bioni, 2020). Essa abordagem vai ao encontro dos princípios democráticos, uma vez que a participação ativa dos cidadãos é necessária para o funcionamento saudável de uma democracia.

A partir de discussões como essa, foi possível avançar na construção de um direito autônomo da personalidade relativo à proteção dos dados pessoais. Assim, esse julgado foi fundamental para se entender que a dinâmica envolvendo esses dados ultrapassa os limites entre o domínio público e privado (Bioni, 2020).

Em 1981, bem antes do caso do censo, os Estados Membros do Conselho da Europa já haviam firmado a Convenção nº 108 para expandir a proteção das liberdades e dos direitos fundamentais dos indivíduos, com ênfase no direito à vida privada. Essa iniciativa ocorreu em resposta ao crescente fluxo transfronteiriço de dados pessoais sujeitos ao tratamento automatizado (Council of Europe, 1981).

A Convenção nº 108 se propôs a reafirmar a liberdade de informação sem limites de fronteiras, reconhecendo a importância de harmonizar os valores fundamentais do respeito à privacidade com o direito à livre circulação de informações entre os povos. Em seu artigo 1º, a Convenção estabeleceu o respeito aos direitos e liberdades fundamentais dos indivíduos, com destaque para o direito à vida privada, no contexto do tratamento automatizado de dados pessoais, o que ficou conhecido como "proteção de dados" (Council of Europe, 1981).

Em 24 de outubro de 1995, o Parlamento Europeu e o Conselho da União Europeia publicaram a Diretiva 95/46/CE, relativa à proteção das pessoas naturais quanto ao tratamento de dados pessoais e à livre circulação desses dados. No entanto, essa Diretiva não se aplicaria ao tratamento de dados relacionados à segurança pública, à defesa ou à segurança do Estado (incluindo questões econômicas ligadas à segurança estatal), às atividades do Estado no domínio do Direito Penal, ou ao tratamento de dados realizado por uma pessoa para fins exclusivamente individuais ou domésticos (União Europeia, 1995).

A Diretiva 95/46/CE estipulou ainda que a proteção das pessoas deveria ser aplicada tanto ao tratamento automatizado de dados como ao tratamento manual, e que o âmbito dessa proteção não poderia depender das técnicas utilizadas, pois, caso contrário, haveria o risco de a proteção não ser efetivada. Apesar de conter pouco mais de 30 artigos, a Diretiva é precedida por 72 considerandos, o que indica a grande complexidade das situações abrangidas (União Europeia, 1995).

Em contrapartida, a Carta de Direitos Fundamentais da Europa, de 7 de dezembro de 2000, submeteu o direito à proteção de dados pessoais ao título dedicado às "Liberdades", onde está tutelado o respeito pela vida privada e familiar, demonstrando como esse direito evoluiu e passou a ser entendido como conexo à liberdade. Nesse sentido, foram as palavras de Stefano Rodotà:

> Na Carta dos Direitos Fundamentais da União Europeia, de fato, o direito à proteção de dados posiciona-se justamente na parte que se refere à liberdade. Aqui também se reflete uma importante evolução destes anos, que transformou o antigo direito a ser deixado só em pré-condição para o exercício de outros direitos e liberdades fundamentais. [...] No momento atual europeu, a associação entre privacidade e liberdade torna-se cada vez mais forte (Rodotà, 2008, p. 236).

Em maio de 2018, entrou em vigor o *General Data Protection Regulation* (GDPR), acordado pelo Parlamento Europeu e pelo Conselho da União Europeia. Trata-se de um documento relativo à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, tendo substituído a supracitada Diretiva 95/46/CE

(GDPR, 2018).

Embora tenha estabelecido objetivos e princípios de proteção de dados, a Diretiva 95/46/CE não conseguiu evitar a fragmentação de sua aplicação na União Europeia. O novo Regulamento buscou corrigir esse problema e garantir maior segurança jurídica às pessoas.

No Brasil, a cultura de proteção de dados ainda é relativamente recente, tendo sido consolidada com a criação da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD). Com a referida lei, passou-se a contar com um modelo *ex ante* e mais amplamente estruturado para o tratamento de dados (Brasil, 2018).

Até a promulgação da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, não existia, na Constituição brasileira, uma tutela específica para os dados pessoais, sendo necessária, para salvaguardá-los, uma interpretação conjunta com outros direitos fundamentais, como o direito à privacidade, ao sigilo das comunicações, à inviolabilidade do domicílio e ao *habeas data* (Brasil, 2022).

Foi nesse cenário que o Supremo Tribunal Federal (STF) foi instado a se manifestar sobre a constitucionalidade da Medida Provisória nº 954, de 17 de abril de 2020, que previa o compartilhamento de dados pessoais de milhões de consumidores de empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística - IBGE (Brasil, 2020).

Tais dados permitiriam que o IBGE obtivesse informações, como nomes, números de telefone e endereços residenciais dos usuários de serviços de telefonia (sejam pessoas físicas ou jurídicas), em substituição à coleta presencial – haja vista a situação pandêmica ocasionada pelo Coronavírus (COVID-19) –, os quais serviriam para direcionar políticas públicas e processos decisórios.

Segundo o Governo Federal, a urgência de aludida providência se justificava, em primeiro lugar, pela necessidade da rápida coleta de dados para o monitoramento da pandemia de COVID-19; em segundo, para garantir a continuidade da Pesquisa Nacional por Amostras de Domicílio (PNAD); e, em terceiro, pela tempestividade necessária para a aquisição dos dados requeridos junto às empresas de telecomunicações, pressupondo-se ser a medida provisória o instrumento mais eficaz na solicitação de referidas informações (Brasil, 2020).

O nível de insegurança quanto à finalidade e necessidade do uso desses dados pessoais foi tamanho que motivou a proposição de diversas Ações Diretas de Inconstitucionalidade (ADIs), tais como a ADI nº 6.387, do Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), a ADI nº 6.389, do Partido Socialista Brasileiro (PSB), a ADI nº 6.390, do Partido Socialismo e Liberdade (PSOL), a ADI nº 6.388, do Partido da Social Democracia Brasileira (PSDB), e a ADI nº 6.393, do Partido Comunista do Brasil (PCdoB).

A ADI nº 6.387, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), argumentou que a Medida Provisória ora analisada era formalmente inconstitucional, não obedecendo aos requisitos relativos à urgência e relevância, como também era materialmente inconstitucional, sendo possível constatar violações aos direitos assegurados pela Constituição Federal de 1988, especificamente no tocante à dignidade da pessoa humana (art. 1º, inciso III), à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas (art. 5º, inciso X), ao direito ao sigilo de dados (art. 5º, inciso XII) e à autodeterminação informativa (STF, 2020).

No julgamento que referendou as medidas cautelares deferidas pela Ministra Rosa Weber nas cinco Ações Diretas de Inconstitucionalidade (ADIs), merecem destaque os votos dos Ministros Luiz Fux e Gilmar Mendes, os quais defenderam a existência de um direito autônomo e fundamental à proteção de dados. De acordo com o Ministro Gilmar Mendes, a "afirmação de um novo direito fundamental não resulta de um criacionismo jurisprudencial", pois "há mais de duas décadas, já se ensaia a evolução do conceito de privacidade" (STF, 2020, p. 111).

Ele ressaltou que, apesar de não terem ocorrido alterações no texto da Constituição, legislações setoriais, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet e a Lei Geral de Proteção de Dados, já asseguravam, materialmente, o direito à proteção de dados pessoais (STF, 2020).

O Ministro Gilmar Mendes justificou a reconceitualização dos direitos na força normativa da Constituição, visando preservar garantias individuais que constituem os alicerces da democracia e que estão sendo ameaçados devido ao desequilíbrio entre a vigilância e a proteção da intimidade. Assim, para ele, a força normativa da Constituição não deve obstruir, mas sim dar suporte à proteção jurídica da intimidade enquanto garantia básica da ordem democrática (STF, 2020).

Segundo Mendes, a base para o reconhecimento de um direito autônomo e fundamental à proteção de dados pessoais advém da compreensão integrada do texto constitucional, amparada no direito fundamental à dignidade da pessoa humana, na concretização do compromisso de renovação da força normativa de proteção ao direito constitucional à intimidade diante dos riscos decorrentes dos avanços tecnológicos e no *habeas data* como meio de tutela material do direito à autodeterminação informativa (STF, 2020).

Nesse sentido, foi o voto do Ministro Luiz Fux, para quem a proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos resultantes da interpretação conjunta da garantia da inviolabilidade da intimidade e da vida privada, do

princípio da dignidade da pessoa humana e da garantia processual do habeas data (STF, 2020).

Por fim, o Ministro Gilmar Mendes afirmou que a Medida Provisória nº 954/2020 é extremamente deficitária no quesito relacionado à proteção da privacidade dos usuários brasileiros de serviços de telefonia, ficando evidente a necessidade de se estabelecer salvaguardas mínimas para assegurar tal direito (STF, 2020).

Já o Ministro Fux evidenciou que, assim como a Lei do Censo de 1983 na Alemanha, aludida medida provisória "também padece de vagueza e amplitude injustificadas, não atendendo a princípios básicos de privacidade, como a definição da finalidade específica e a necessidade para a transferência das informações" (STF, 2020, p. 68).

Em maio de 2020, o Supremo referendou, por maioria (10 votos contra 1), a medida cautelar deferida para suspender a eficácia da Medida Provisória em questão. Posteriormente, as ADIs que atacavam a MP foram extintas sem julgamento do mérito devido ao término do prazo estabelecido para conversão da Medida em lei. Observa-se que os votos dos Ministros Gilmar Mendes e Luiz Fux foram de extrema importância para o reconhecimento do direito autônomo e fundamental à proteção de dados pessoais, acompanhando, assim, a evolução da jurisprudência alemã referente ao direito à autodeterminação informativa.

À vista de tal decisão, surgiram diversos questionamentos sobre a necessidade e conveniência da aprovação e promulgação da Proposta de Emenda à Constituição (PEC) nº 17/2019, que tornava a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental previsto na Constituição Federal, bem como remetia privativamente à União a função de legislar sobre o tema (Brasil, 2019).

Após ser aprovada na Câmara dos Deputados e no Senado Federal e promulgada, em 10 de fevereiro de 2022, pelo Congresso Nacional, a PEC nº 17/2019 deu origem à Emenda Constitucional (EC) nº 115/2022, elevando, assim, a proteção de dados ao patamar de direito fundamental explícito (Brasil, 2022).

Apesar de o Supremo Tribunal Federal já ter reconhecido a proteção de dados como um direito fundamental implícito, a sua positivação formal na Constituição assegurava maior proteção jurídica e dissipava qualquer debate a respeito do seu reconhecimento ou não como direito fundamental. Nos dizeres do Ministro do Superior Tribunal de Justiça, Ricardo Villas Bôas Cueva:

> Trata-se de um marco civilizatório, que coloca o Brasil no mesmo patamar de proteção de direitos fundamentais que a Europa. Agora se completa a arquitetura legislativa da proteção de dados no Brasil. A positivação do direito fundamental à proteção de dados é fundamental para aprofundar a tutela da autodeterminação informativa no país, pois a LGPD tem caráter marcadamente instrumental (Rodas, 2022).

É evidente, portanto, que o direito à proteção de dados pessoais vem ganhando reconhecimento e importância crescentes, tanto no cenário nacional quanto internacional. Esse reconhecimento reflete o compromisso com a preservação da liberdade individual e da dignidade humana. Afinal, o manuseio inadequado de informações pode resultar em discriminação, perda de oportunidades e até manipulação em contextos político-eleitorais, temas que serão abordados ao longo desta dissertação.

2.3 A legislação brasileira sobre dados pessoais

Após uma sucinta análise da proteção de dados pessoais como um direito fundamental e autônomo, é relevante destacar, sob a perspectiva da legislação ordinária, algumas leis que abordam os dados pessoais não como o foco principal de sua regulamentação, mas de maneira secundária.

Dentre elas, destaca-se a Lei nº 8.078/1990, conhecida como Código de Defesa do Consumidor (CDC). Seu artigo 43 estabeleceu diretrizes referentes aos bancos de dados que armazenam informações sobre os consumidores (Brasil, 1990). Ele visa garantir que o consumidor tenha o direito de acessar suas informações pessoais armazenadas, bem como corrigi-las, caso estejam incorretas.

É importante ressaltar a ampla abrangência desse dispositivo legal, que engloba todos os dados pessoais do titular, indo além dos bancos de informações negativas utilizados para análise de crédito. A intenção do legislador foi regular todos os bancos de dados que possam impactar o pleno desenvolvimento da personalidade do consumidor (Bioni, 2020).

Dentro dessa perspectiva, a legislação consumerista optou por garantir ao cidadão o controle sobre suas informações pessoais. Na verdade, o espírito dessa regulamentação é empoderar o consumidor para que ele possa gerir seus próprios dados. Isso se inicia com a exigência de informá-lo sobre a criação de um banco de dados pessoais que não tenha sido de sua solicitação (art. 43, § 2º, do CDC). Tal requisito de aviso prévio possibilita que o titular dos dados esteja ciente e possa supervisionar a utilização de suas informações, garantindo maior transparência (Bioni, 2020).

Essa transparência deve-se ao fato de que o responsável pelos bancos de dados possui obrigações que correspondem aos direitos do consumidor, que são: i) garantir o acesso do titular dos dados às suas informações (art. 43, caput); ii) assegurar a precisão dessas informações; iii) restringir o uso do banco de dados a propósitos claros e legítimos; e iv) respeitar o prazo

máximo de cinco anos para o armazenamento de informações negativas (art. 43, § 1º, do CDC) (Bioni, 2020).

Desse modo, ao garantir o acesso às informações pessoais, o consumidor tem a possibilidade de verificar sua veracidade e corrigir eventuais imprecisões. Além disso, restringir o uso do banco de dados a propósitos claros e legítimos evita que as informações pessoais sejam utilizadas de forma indevida ou abusiva. Já o estabelecimento de um prazo máximo de armazenamento de informações negativas impede que tais informações sejam mantidas indefinidamente, permitindo que o consumidor tenha a oportunidade de superar situações passadas e reconstruir sua reputação.

Sob essa ótica, o consumidor pode exigir a imediata retificação ou cancelamento de uma informação imprecisa ou que tenha excedido o prazo de retenção, com fulcro no art. 43, § 3º, do CDC (Brasil, 1990). Esses direitos, juntamente com os princípios da transparência, precisão e limitação temporal, são primordiais para garantir que o consumidor, na qualidade de titular dos dados pessoais, tenha controle sobre suas informações (Bioni, 2020).

Por seu turno, a Lei nº 12.414/2011, conhecida como Lei do Cadastro Positivo, determinou a estrutura necessária para a consolidação desses bancos de dados, que contêm informações sobre as operações financeiras e o cumprimento das obrigações dos consumidores, com o objetivo de auxiliar na concessão de crédito (Brasil, 2011).

Essa evolução legislativa mudou o panorama anterior, permitindo que a análise da viabilidade financeira de um solicitante de crédito não dependesse exclusivamente de informações sobre débitos pendentes, mas também considerasse outros dados que revelassem aspectos positivos de sua situação financeira e histórico de pagamento. Em virtude disso, a lei adquiriu esse nome de “Cadastro Positivo”, refletindo a extensão da avaliação de crédito para além da mera investigação de inadimplementos.

Cumpre esclarecer que antes da promulgação da Lei Complementar nº 166/2019, responsável por alterar a Lei nº 12.414/2011, a inclusão de consumidores em tais bancos de dados somente era possível mediante consentimento explícito (Brasil, 2019). No entanto, essa nova legislação mudou esse panorama, tornando a inclusão no banco de dados um procedimento automático, dando aos titulares de dados pessoais a oportunidade de solicitar a remoção de seus nomes desse registro. Essa mudança representou uma transição de um sistema de adesão voluntária para um sistema de exclusão voluntária, colocando nas mãos dos indivíduos o controle sobre a sua participação nesses bancos de dados.

A Lei Complementar nº 166/2019 trouxe ainda outras importantes modificações à Lei do Cadastro Positivo. No que diz respeito ao compartilhamento de informações cadastrais e de

adimplemento com terceiros, a nova legislação passou a permitir que o gestor do banco de dados realizasse o compartilhamento dessas informações com outros bancos de dados. Com essa permissão, as obrigações e responsabilidades relacionadas ao tratamento desses dados passaram a ser também do terceiro agente envolvido (Brasil, 2019).

Já no tocante ao uso de informações para fins não relacionados ao crédito, bem como quanto a certas categorias sensíveis de dados, a Lei Complementar supracitada estabeleceu restrições claras. Essas restrições possuem o objetivo de limitar a coleta e os propósitos do tratamento de dados pessoais pelo gestor do banco, garantindo a proteção da privacidade e empoderando o consumidor no controle de suas informações pessoais.

Além disso, outras leis relacionadas à proteção de dados foram implementadas nesse período, como a Lei de Acesso à Informação (Lei nº 12.527/2011) (Brasil, 2011). Essa lei foi criada com o propósito de regulamentar o princípio constitucional da transparência e determinar diretrizes para o acesso a informações públicas. Ela definiu o conceito de "informação pessoal" de forma semelhante àquela posteriormente delineada pela Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018).

Com efeito, a Lei de Acesso à Informação, em seu artigo 31, determinou uma regra específica para a proteção de dados pessoais mantidos pelo poder público. Esse artigo determina que as informações pessoais dos cidadãos, que são coletadas pelo poder público, devem ser protegidas, assegurando a privacidade e a segurança desses dados (Brasil, 2011).

Essa disposição é significativa, pois reconhece a importância de salvaguardar as informações pessoais, mesmo dentro de uma legislação que tem como objetivo principal regular o princípio da transparência governamental. Ao proteger os dados pessoais, a Lei de Acesso à Informação busca assegurar que a transparência seja alcançada de forma compatível com a privacidade dos cidadãos.

Por fim, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, instituiu princípios, garantias, direitos e obrigações para a utilização da internet no Brasil. Essa legislação, de natureza principiológica, desempenhou um importante papel na regulação do ambiente digital no país (Brasil, 2014).

Por meio de seu artigo 7º, o Marco Civil da Internet assegurou uma série de direitos aos usuários da internet e incluiu disposições específicas para tutelar a privacidade em seus diferentes aspectos. Além disso, o direito à privacidade e à liberdade de expressão foram reconhecidos como condições essenciais para o pleno exercício do direito de acesso à rede mundial de computadores, conforme estabelecido em seu artigo 8º (Brasil, 2014).

No que diz respeito à proteção dos dados pessoais, o Marco Civil da Internet reconheceu

o direito dos usuários de não fornecer seus dados pessoais a terceiros, incluindo registros de conexão e acesso a aplicações de internet, exceto quando houver consentimento livre, expresso e informado ou nas hipóteses previstas em lei (art. 7º, inciso VII). Estabeleceu ainda o direito dos usuários de receber informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados, bem como sobre as finalidades dessas atividades (art. 7º, inciso VIII). Também foi garantido o direito dos usuários de consentir ou não com a coleta e uso de seus dados (art. 7º, inciso IX) (Brasil, 2014).

Na Seção II do Capítulo III da Lei, intitulada "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas", foram estipuladas diretrizes e salvaguardas para garantir a privacidade e a segurança das informações no ambiente digital (Brasil, 2014).

O artigo 10 da Lei supracitada instituiu que a guarda e a disponibilização dos registros de conexão, dados pessoais e conteúdo de comunicações privadas devem respeitar a preservação da intimidade, vida privada, honra e imagem das partes envolvidas. O provedor responsável pela guarda dos registros só fica obrigado a disponibilizá-los mediante ordem judicial, respeitando o que está estabelecido no artigo 7º (Brasil, 2014).

O artigo 11, por sua vez, determinou que as operações de coleta, armazenamento, guarda e tratamento de registros, dados pessoais e comunicações por provedores de conexão e aplicações de internet devem cumprir a legislação brasileira e respeitar os direitos à privacidade, proteção de dados pessoais e sigilo das comunicações. Isso se aplica mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que ofereçam serviços ao público brasileiro ou haja uma integrante do mesmo grupo econômico com estabelecimento no Brasil (Brasil, 2014).

Já o artigo 12 previu sanções para as infrações às normas dos artigos 10 e 11, como advertência, multa, suspensão temporária das atividades ou proibição de exercício das atividades relacionadas. No caso de empresa estrangeira, sua filial, sucursal, escritório ou estabelecimento situado no Brasil fica solidariamente responsável pelo pagamento da multa (Brasil, 2014).

Embora o Marco Civil da Internet tenha sido um marco importante na regulação da internet, é válido destacar que ele não abordou, de forma detalhada, as definições conceituais essenciais para restringir a coleta e o tratamento de dados pessoais. O texto legal deixou lacunas em termos como "dado pessoal" e "dados sensíveis", que foram posteriormente definidos no Decreto nº 8.771/2016, responsável por regulamentar essa legislação (Brasil, 2016).

Ademais, o Marco Civil da Internet, em seu art. 3º, inciso III, estabeleceu que as normas para a utilização da internet devem abranger a proteção de dados pessoais "nos termos da lei",

ou seja, apontou para a necessidade de uma legislação própria para disciplinar esse tema de forma adequada. Essa disposição reconhece a importância de tratar a proteção de dados pessoais de maneira específica e detalhada, considerando as particularidades e os desafios inerentes ao ambiente online (Brasil, 2014).

Diante da acirrada situação de intensa inovação tecnológica nacional e internacional e do impacto sobre os direitos da privacidade, o governo brasileiro, aos poucos, começou a perceber que o arcabouço legal vigente precisava ser revisto. Assim, em 2010, o Ministério da Justiça, em colaboração com a sociedade, deu início à elaboração de um texto-base do Anteprojeto de Lei de Proteção de Dados Pessoais. Este seria o começo de uma longa discussão popular sobre o tema que culminou na criação da LGPD (Magrani, 2019).

Vale ressaltar que a divulgação, por Edward Snowden, das atividades de espionagem do governo dos Estados Unidos, teve um impacto significativo no debate sobre a proteção da privacidade no ambiente digital. Os líderes de Estado, como a então presidente Dilma Rousseff, do Brasil, e a então chanceler da Alemanha Angela Merkel, foram alvos diretos dessas práticas de vigilância global, o que despertou preocupações sobre a segurança e confidencialidade dos indivíduos e a necessidade de medidas para proteger seus dados pessoais. Em resposta a essas revelações, os países afetados e outros atores internacionais se mobilizaram para buscar soluções e propor medidas de proteção da privacidade na era digital (Magrani, 2019).

A construção da Lei Geral de Proteção de Dados (LGPD) envolveu um processo democrático de ampla discussão e participação da sociedade. Desde o início, foi reconhecida a importância de envolver diversos setores e dar voz aos diferentes atores envolvidos no tratamento de dados pessoais.

Para garantir a participação da sociedade, foram realizadas consultas públicas, nas quais pessoas e organizações puderam contribuir com sugestões e comentários sobre o projeto de lei. Esse processo foi fundamental para que fossem trazidas à discussão diferentes perspectivas, conhecimentos e preocupações dos cidadãos e especialistas (Bioni, 2020).

Além das consultas públicas, ocorreram debates em audiências públicas, seminários, eventos e rodas de conversa, nos quais foram discutidos os aspectos técnicos, éticos, jurídicos e práticos da proteção de dados pessoais. Esses fóruns propiciaram a troca de opiniões, a introdução de novas propostas e a reflexão sobre as consequências da nova regulamentação (Bioni, 2020).

Após passar por várias etapas legislativas, a Lei Geral de Proteção de Dados Pessoais (LGPD) foi promulgada em 14 de agosto de 2018. Sua entrada em vigor ocorreu de forma escalonada, com algumas disposições imediatamente aplicáveis e outras com prazos para que

as organizações se adequassem a ela. Somente em setembro de 2020, a lei entrou completamente em vigor, estabelecendo que todas as empresas, órgãos públicos e demais organizações que tratem dados pessoais devem estar em conformidade com seus princípios e normas.

Com isso, a LGPD tornou-se o primeiro diploma legal no Brasil a regulamentar, de forma específica, o tratamento de dados pessoais. Anteriormente, conforme já mencionado, esse tema era abordado de maneira não sistematizada, o que causava incertezas e lacunas no tratamento dessas informações (Brasil, 2018).

A referência para a criação da LGPD é notavelmente proveniente de um modelo já estabelecido e reconhecido internacionalmente: o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Diversos elementos, conceitos e diretrizes presentes no GDPR podem ser encontrados na LGPD, refletindo uma busca pelo equilíbrio na proteção dos dados pessoais.

Ao se espelhar no exemplo europeu durante a elaboração da LGPD, o Brasil demonstrou não apenas o compromisso em fortalecer os direitos individuais em relação aos dados pessoais, mas também adotou uma consonância com as práticas e normas internacionais. Isso é particularmente relevante em uma era digital caracterizada por transações e interações transfronteiriças, onde a harmonização das regras de proteção de dados se tornou essencial.

A LGPD possui como propósito proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, inclusive nos meios digitais, quando houver o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado (art. 1º, *caput*). Aludida lei é composta por 65 artigos e estabelece fundamentos, princípios, direitos dos titulares dos dados e deveres às organizações que realizam o tratamento desses dados. Dessa forma, busca-se garantir uma proteção efetiva das informações pessoais, promovendo a privacidade e a segurança dos indivíduos (Brasil, 2018).

Nesse contexto, é primordial definir, primeiramente, o objeto de tutela: os dados pessoais. De acordo com o art. 5º, inciso I, da LGPD, dados pessoais são informações relacionadas à pessoa natural identificada ou identificável. Isso abrange qualquer informação que possa ser usada para reconhecer um indivíduo, como nome, endereço, número de identificação, dados de localização, ou até mesmo um identificador online. Observa-se que a LGPD tem como escopo salvaguardar os dados pessoais de pessoas físicas, isto é, o escopo de aplicação da lei não abrange os dados de pessoas jurídicas (Brasil, 2018).

Tal definição é integrada com a de dado pessoal sensível, uma espécie de dado pessoal que exprime a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação

sindical, o estado de saúde, a orientação sexual, além de dados genéticos ou biométricos (art. 5º, inciso II). Devido à capacidade de revelar informações mais intrusivas à privacidade do cidadão, com alto potencial discriminatório e riscos aos direitos e garantias individuais, a LGPD dedicou um regime jurídico mais protetivo para essa categoria especial de dados (Brasil, 2018).

Bioni (2020) destaca que um simples dado pessoal pode transformar-se em um dado sensível, especialmente quando se utiliza tecnologias avançadas, como análise de grandes volumes de dados, que possibilitam correlacionar sequências de informações para antecipar comportamentos e tendências.

O autor ilustra essa transformação de dados com um estudo realizado pela Universidade de Cambridge, que utilizou o Facebook como plataforma de pesquisa. Baseando-se na análise de "curtidas" em determinadas publicações, o trabalho conseguiu identificar com precisão aspectos profundos e sensíveis dos usuários, como inclinações políticas, orientação sexual e etnia (Bioni, 2020). Em outras palavras, informações aparentemente inofensivas, como "curtidas", foram processadas de modo a desvendar detalhes íntimos e altamente pessoais, com potencial para uso discriminatório.

No tocante a dados anonimizados, o art. 5º, inciso III, da LGPD, define que são considerados dados relativos a um titular que não possa ser identificado, levando em consideração a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento (Brasil, 2018). Portanto, os dados anonimizados são considerados o oposto dos dados pessoais. Ao passar por um processo de anonimização, os dados do titular são transformados de tal forma que torna impossível sua associação com uma pessoa em particular.

O artigo 2º da LGPD apresenta os fundamentos que promovem a estrutura da proteção dos dados pessoais, englobando não apenas aspectos de natureza existencial, mas também de âmbito patrimonial e mercadológico. Entre os fundamentos elencados pela nova legislação estão: a reverência à privacidade; o princípio da autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; a defesa do consumidor e os direitos humanos. Salienta-se também a consideração pelo livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. No mesmo escopo, a lei ainda menciona a proteção do desenvolvimento econômico e tecnológico, a inovação, a liberdade de iniciativa e a livre concorrência (Brasil, 2018).

Já os princípios estabelecidos no artigo 6º da LGPD desempenham um papel de suma importância ao nortear as atividades relacionadas ao tratamento de dados pessoais. Eles fornecem diretrizes que devem ser seguidas para garantir uma abordagem adequada e

responsável no manejo dessas informações (Brasil, 2018).

Esses princípios incluem: (i) a boa-fé, que orienta ações e intenções honestas no tratamento dos dados; (ii) a finalidade, que determina que os dados devem ser utilizados para propósitos específicos e legítimos; (iii) a adequação, que requer que o tratamento seja compatível com a finalidade declarada; (iv) a necessidade, que estabelece que apenas os dados necessários devem ser coletados; (v) o livre acesso, que garante que o titular dos dados tenha acesso fácil e gratuito às informações sobre o tratamento; (vi) a qualidade dos dados, que busca assegurar que os dados sejam corretos e atualizados; (vii) a transparência, que exige que o titular seja informado de forma clara e acessível sobre o tratamento de seus dados; (viii) a segurança, que visa proteger os dados contra acessos não autorizados e incidentes; (ix) a prevenção, que busca evitar danos aos titulares dos dados; (x) a não discriminação, que veda o tratamento discriminatório dos dados; (xi) a responsabilização, que impõe às organizações a responsabilidade pelo cumprimento da LGPD, (xii) e a prestação de contas, que requer que as organizações sejam capazes de demonstrar a conformidade com a lei (Brasil, 2018).

No próximo capítulo, estes princípios serão analisados de forma mais detalhada. Eles são fundamentais à construção de um ambiente mais seguro para a comunicação das campanhas políticas com os eleitores. O objetivo é fornecer uma referência principiológica que oriente as questões jurídico-regulatórias e auxilie na tomada de decisões.

Enquanto os princípios fornecem uma orientação segura para o tratamento de dados pessoais, garantindo que sejam manuseados com integridade e respeito, as bases legais estabelecem o alicerce jurídico que legitima e permite esse tratamento. Juntos, esses elementos formam a estrutura de um sistema de proteção de dados sólido e confiável, equilibrando as demandas organizacionais com os direitos inerentes aos titulares dos dados. Durante qualquer atividade de tratamento de dados, faz-se necessário identificar e se respaldar na base legal apropriada que justifica e valida tal procedimento.

A LGPD, em seu artigo 7º, estabelece as bases legais para o tratamento de dados pessoais. Essas bases legais são as seguintes: (i) consentimento do titular dos dados, (ii) cumprimento de obrigação legal ou regulatória pelo controlador, (iii) interesse público, (iv) realização de estudos por órgão de pesquisa, (v) execução de contrato, (vi) exercício regular de direitos em processos judiciais, (vii) proteção da vida e da incolumidade física, (viii) tutela da saúde, (ix) legítimo interesse do controlador ou de terceiros, e (x) proteção do crédito (Brasil, 2018).

Por outro lado, para os dados categorizados como sensíveis, o artigo 11 da LGPD traz fundamentos mais específicos para seu tratamento. Estes compreendem: (i) consentimento

destacado do titular para propósitos claros, (ii) cumprimento de obrigações legais, (iii) tratamento compartilhado para políticas públicas, (iv) estudos por entidades de pesquisa, (v) exercício de direitos em processos, (vi) proteção da vida ou da incolumidade física, (vii) tutela da saúde por profissionais da área, e (viii) prevenção à fraude e segurança do titular em sistemas eletrônicos (Brasil, 2018).

Cada uma dessas bases legais possui requisitos próprios que devem ser cumpridos para garantir que o tratamento de dados seja realizado de forma legal e legítima. A observância desses requisitos é essencial para evitar infrações e garantir a proteção dos direitos dos titulares dos dados. Dentre as bases retromencionadas, algumas são especialmente relevantes em contextos eleitorais.

A respeito dos direitos dos titulares dos dados, o artigo 18 da LGPD elenca diversas garantias, incluindo o direito de acesso às informações, a retificação de dados imprecisos, a exclusão de informações que não se fazem mais necessárias, a portabilidade de dados, a possibilidade de revogar o consentimento previamente dado, dentre outras (Brasil, 2018). Estas prerrogativas asseguram aos titulares maior clareza e autonomia sobre como suas informações pessoais são tratadas.

Além dos direitos conferidos aos titulares dos dados, a LGPD também impõe deveres às organizações que realizam o tratamento dessas informações. Esses deveres visam garantir a segurança, a privacidade e a integridade dos dados pessoais, bem como promover uma cultura de responsabilidade no uso desses dados. O não cumprimento desses deveres pode resultar em sanções administrativas, como advertências, multas e até mesmo a proibição total ou parcial do exercício das atividades relacionadas ao tratamento de dados (art. 52). Portanto, as entidades precisam estar cientes de suas obrigações e adotar as medidas necessárias para garantir a conformidade com a legislação (Brasil, 2018).

Sem dúvidas, o efetivo cumprimento da Lei Geral de Proteção de Dados é uma tarefa desafiadora, dada a complexidade e a abrangência das questões que envolvem os dados pessoais. Esta norma não apenas estabelece um novo patamar de proteção de dados no país, mas também destaca a importância de uma mentalidade focada na valorização do titular da informação.

No âmbito das campanhas eleitorais, a LGPD atua como guardiã dos dados pessoais de eleitores, candidatos e demais envolvidos no processo eleitoral. Ela fornece parâmetros e medidas de segurança para assegurar que as informações coletadas sejam tratadas de forma adequada, respeitando os princípios anteriormente citados.

A questão central é como equilibrar a proteção dos dados pessoais e a necessidade

legítima de coletar, processar e compartilhar tais informações. Além disso, a implementação da LGPD exige uma mudança de cultura nas organizações, com a adoção de práticas e políticas de proteção de dados desde o início de seu ciclo de vida. Isso implica conscientizar sobre a importância da privacidade e da segurança dos dados, além de estabelecer mecanismos de governança e responsabilidade internos.

Além disso, há o desafio relacionado à educação da população em geral sobre seus direitos e como exercê-los. Muitas pessoas ainda não compreendem totalmente as garantias associadas aos seus dados pessoais, o que pode resultar em uma menor atuação ativa na defesa de seus interesses. Esse cenário ressalta a importância de campanhas educativas e de conscientização para que os cidadãos estejam aptos a proteger seus dados e exercer seus direitos de forma plena.

Por fim, é importante mencionar a necessidade de cooperação entre diferentes atores, como órgãos governamentais, empresas, sociedade civil e especialistas em proteção de dados. O efetivo cumprimento da LGPD, especialmente em campanhas eleitorais, requer a colaboração de todos esses segmentos, bem como a troca de experiências e boas práticas para lidar com os desafios e encontrar soluções adequadas. A jornada pode ser complexa, mas extremamente necessária para assegurar a proteção dos direitos inalienáveis dos cidadãos na era digital.

3 CONEXÃO ENTRE PROTEÇÃO DE DADOS E DIREITO ELEITORAL

O liame entre a proteção de dados pessoais e o Direito Eleitoral é importante para garantir o acesso à informação e à participação política. Enquanto a proteção de dados pessoais assegura que os indivíduos tenham autonomia sobre a utilização e divulgação de suas informações, o direito eleitoral garante que os cidadãos tenham voz ativa nas decisões que afetam diretamente suas vidas. Quando combinados, esses conceitos podem ajudar a garantir um processo democrático justo e transparente. A conexão entre ambos reforça a importância da privacidade na democracia. Em um sistema democrático, as pessoas devem ter o direito de decidir quais informações pessoais podem ser coletadas e usadas para fins políticos.

Ademais, a proteção de dados pessoais também é importante para assegurar a igualdade no direito eleitoral. Se determinadas informações são coletadas e usadas de forma discriminatória, isso pode afetar a capacidade de as pessoas exercerem seu direito à participação política. Nesse sentido, as leis de proteção de dados servem como um escudo contra esse tipo de prática, garantindo que todos tenham igualdade de acesso aos processos políticos.

3.1 O uso de dados pessoais na legislação eleitoral

A legislação brasileira adotou medidas rigorosas em relação à propaganda eleitoral com o firme propósito de assegurar a equidade entre os candidatos, estabelecendo limitações claras que abrangem diversos aspectos da campanha, desde o conteúdo até a forma e o momento de sua divulgação. A responsabilidade pelo cumprimento destas regras recai sobre a Justiça Eleitoral. Contudo, o rápido avanço da comunicação apresenta desafios sem precedentes. O modelo de comunicação tradicional, representado por rádio, televisão e jornais, já não detém mais o monopólio da cena.

Na era digital, a comunicação tomou um novo rumo, permitindo que figuras notáveis, como o ex-presidente Jair Messias Bolsonaro, conquistassem audiências online de magnitude surpreendente. No mundo virtual, a linha divisória entre emissor e receptor da mensagem se torna tênue. Durante as interações, uma pessoa pode facilmente assumir ambos os papéis, e um simples comentário instantâneo desfaz essas fronteiras, possibilitando que o receptor se transforme também em emissor.

A aplicação das normas relacionadas à propaganda eleitoral sempre suscitou debates, devido à sua natureza intrincada e à necessidade de análises minuciosas de circunstâncias específicas. No entanto, é incontestável que a propaganda eleitoral desempenha um papel

essencial na disseminação das ideias e programas de candidatos, representando o cerne do mandato partidário representativo.

No cenário de comunicação atual, caracterizado pela rápida circulação de informações, surge uma questão pertinente: até que ponto a Justiça Eleitoral pode exercer controle sobre esse conteúdo? A disponibilidade das poderosas ferramentas de comunicação apresenta desafios significativos para o modelo de regulamentação da propaganda eleitoral, particularmente quando se trata do ambiente online.

A internet e as redes sociais, apesar de terem revolucionado o acesso à informação e expandido o espaço para o debate democrático, também deram origem a desafios significativos, como a disseminação de notícias falsas e discursos de ódio.

Marilda Silveira (2021) destaca que as novas tecnologias intensificaram esse cenário de desinformação. Segundo ela, uma ampla variedade de agentes cria conteúdo usando ferramentas que manipulam imagens com alta precisão e direcionam esse conteúdo para públicos específicos, alinhados com suas preferências. Além disso, Marilda Silveira (2021) enfatiza que muitas dessas informações são originadas anonimamente, ou são distorcidas e disseminadas por robôs automatizados, minando assim a capacidade crítica dos receptores em discernir e avaliar a veracidade do conteúdo com que interagem.

Quando o legislador estabeleceu as regras para a propaganda eleitoral, não antecipou a extensão e a complexidade das ferramentas digitais. Portanto, o desafio atual consiste em como regular um ambiente tão fluido e dinâmico sem restringir a liberdade de expressão. Por um lado, as redes sociais proporcionam um espaço para que candidatos com recursos limitados se destaquem, nivelando o campo de jogo. Por outro lado, esse mesmo espaço também pode ser explorado para disseminar informações incorretas.

Em 2009, com a promulgação da Lei nº 12.034, o cenário digital ganhou destaque jurídico nas campanhas eleitorais brasileiras. Esta lei introduziu os artigos 57-A ao 57-I na Lei nº 9504/1997, estabelecendo uma seção voltada especificamente para a propaganda eleitoral online (Brasil, 2009). Anteriormente, em 2008, a Justiça Eleitoral já havia tentado regulamentar a campanha eleitoral na internet por meio da Resolução nº 22.718 (Brasil, 2008). Contudo, essa tentativa mostrou-se superficial, dada a compreensão ainda emergente das potencialidades digitais daquele momento.

A reforma eleitoral de 2017, por meio da Lei nº 13.488, introduziu mudanças significativas na Lei das Eleições, permitindo que candidatos, partidos políticos e coligações pudessem impulsionar conteúdo. Essas alterações representaram mais um esforço para modernizar a legislação, tornando-a mais adequada ao ambiente dinâmico da internet e às suas

características singulares (Brasil, 2017).

Em 2021, por meio da Resolução nº 23.671, que promoveu alterações na Resolução nº 23.610/2019, o Tribunal Superior Eleitoral (TSE) avançou ainda mais na regulamentação do ambiente virtual, introduzindo regras específicas para o uso de dados pessoais. Esta iniciativa ganhou destaque em um contexto em que a privacidade e a ética na manipulação de dados se tornaram de importância considerável a nível global (Brasil, 2019).

Dentro dessas alterações, a Resolução nº 23.610/2019, ao abordar a propaganda eleitoral, passou a indicar, no art. 41, sua sintonia com a Lei Geral de Proteção de Dados, bem como passou a ressaltar, de acordo com o parágrafo 4º do artigo 31, que todas as atividades relacionadas a dados pessoais, desde doações até uso e compartilhamento, realizadas tanto por pessoas jurídicas quanto por pessoas físicas, devem estar em total conformidade com a Lei Geral de Proteção de Dados Pessoais (Brasil, 2019).

Esse enfoque reflete um compromisso sólido em garantir que as atividades relacionadas ao tratamento de dados, especialmente por parte de candidatos, partidos políticos ou coligações, estejam alinhadas com a LGPD. Tal compromisso se torna de extrema relevância, especialmente no contexto das ações vinculadas à propaganda eleitoral (Massaro et al., 2020).

O e-mail, ao longo dos anos, consolidou-se como uma ferramenta valiosa para campanhas eleitorais, permitindo que candidatos e partidos políticos se comuniquem de forma direta e adaptada com os eleitores. Por meio dele, é possível disseminar propostas, agendas, vídeos e outros materiais pertinentes de maneira eficiente. No entanto, quem faz uso dessa ferramenta deve estar vigilante em relação às normativas legais sobre o uso de dados pessoais, garantindo que a coleta e uso desses endereços eletrônicos respeitem integralmente os princípios da LGPD.

A Lei das Eleições, ao contemplar, no art. 57-B, a viabilidade da propaganda eleitoral na internet, concedeu a permissão para que candidatos, partidos, coligações ou federações divulguem mensagens eletrônicas, contanto que os endereços eletrônicos destinados a esse fim tenham sido registrados gratuitamente pelos *players* (Brasil, 1997).

A Resolução nº 23.610/2019, ao regulamentar esse dispositivo, estabeleceu regras minuciosas para a coleta desses endereços eletrônicos. Conforme estipulado no art. 28, inciso III, dessa Resolução, a veiculação de propaganda eleitoral por mensagens eletrônicas, além de exigir o cadastro gratuito do endereço eletrônico, deve estar fundamentada em uma das bases legais que permitem o tratamento de dados pessoais (Brasil, 2019). Em outras palavras, não basta apenas coletar os dados pessoais de forma gratuita, é imprescindível que exista uma base legal, que garanta o tratamento desses dados.

A divulgação dessa modalidade de propaganda, quando em desacordo com as normas retromencionadas, pode acarretar penalizações financeiras significativas. Tanto o usuário responsável pelo conteúdo quanto o beneficiário, quando comprovado seu prévio conhecimento, podem ser penalizados com multas que variam de R$ 5.000,00 a R$ 30.000,00, ou até o dobro do valor gasto, caso esse cálculo ultrapasse o limite máximo da multa, conforme estabelecido pelo artigo 57-B, § 5º da Lei nº 9.504/1997 (Brasil, 1997).

No panorama da comunicação política, houve um período em que o e-mail era o principal meio de contato digital. No entanto, com o surgimento e popularização das mensagens instantâneas, que são mais dinâmicas e frequentemente incluem elementos visuais e sonoros, a estratégia de propaganda eleitoral encontrou um novo atrativo para conquistar a atenção do eleitorado. O ambiente das mensagens instantâneas oferece uma plataforma altamente interativa e imediata, tornando-se uma ferramenta valiosa para candidatos que desejam se conectar diretamente com os eleitores.

Nesse contexto, é importante notar que a propaganda eleitoral pode ser realizada também através de aplicativos de mensagens instantâneas, desde que não envolva a contratação de disparos em massa "sem o consentimento do destinatário", como estipulado nos arts. 28, inciso IV, e 33 e 34 da Resolução nº 23.610/2019 (Brasil, 2019).

Destaca-se que a coleta de dados pessoais com o objetivo de, posteriormente, enviar mensagens publicitárias é considerada uma forma de tratamento de dados. Desse modo, o responsável pelo tratamento deve sempre respeitar a vontade da pessoa titular, obtendo um consentimento livre, informado e inequívoco, nos termos do art. 5º, inciso XII, da LGPD. Especial atenção deve ser dada quando se refere a dado sensível, exigindo um consentimento específico e destacado, como definido no art. 11, inciso I, da referida lei. É fundamental fornecer informações claras e precisas sobre o tratamento dos dados. A falta de transparência ou a apresentação de informações enganosas ou abusivas tornam o consentimento nulo, sujeitando o tratamento de dados a irregularidades e possíveis sanções pela ANPD e pela Justiça Eleitoral em suas respectivas áreas de competência (TSE, 2021).

Em todos os casos, deve ser garantida a opção de "descadastramento", conforme estabelecido no art. 57-G da Lei das Eleições e nos arts. 33 e 34 da Resolução nº 23.610/2019 (Brasil, 2019). Essas disposições asseguram aos eleitores a capacidade de revogar o consentimento concedido para receber tais mensagens, fornecendo um mecanismo de proteção à autodeterminação informativa. Assim, o consentimento pode ser retirado a qualquer momento.

Para garantir o exercício desse direito, o agente de tratamento deve oferecer um

procedimento gratuito e de fácil acesso, por meio do qual a pessoa titular possa manifestar sua vontade, nos termos do art. 8º, § 5º, da LGPD. Uma vez efetuada a solicitação de revogação, o tratamento dos dados deve ser imediatamente interrompido, e os dados da pessoa titular, excluídos, a menos que existam circunstâncias que permitam a sua retenção, de acordo com o art. 16 da LGPD (Brasil, 2018).

A enxurrada de mensagens políticas recebidas, sejam eletrônicas ou instantâneas, tornou-se uma fonte de incômodo para muitos destinatários. Diante desse problemática, o legislador eleitoral tomou a iniciativa de estabelecer regras claras para lidar com essa situação. Para fazer uso dessas ferramentas de comunicação, o remetente, não só deve oferecer meios para que o destinatário possa se descadastrar e interromper o recebimento de mensagens, como também precisa ser prontamente identificável. Se o destinatário solicitar o descadastramento e o remetente não atender dentro de 48 horas após a solicitação, o envio de mensagens após esse período pode acarretar multa no valor de R$ 100,00 por mensagem aos responsáveis, conforme estabelecido no art. 57-G da Lei das Eleições e no art. 33 da Resolução nº 23.610/2019 (Brasil, 2019).

Para cumprir tais obrigações legais, é aconselhável que, na própria mensagem enviada, sejam fornecidas instruções visíveis sobre como a pessoa titular pode revogar o consentimento e solicitar a remoção de seus dados da lista de envio de mensagens. Essa ação deve ser fácil de realizar e não deve acarretar custos para o titular, podendo ser feita, por exemplo, com um simples “clique” em um link disponibilizado na mensagem (TSE, 2021).

Importante ressaltar que essas regulamentações não se aplicam às mensagens eletrônicas e às mensagens instantâneas enviadas de forma consensual por indivíduos, seja em âmbito privado ou em grupos restritos de participantes, nos termos do art. 33, §2º, da Resolução supracitada (Brasil, 2019).

Assim, vê-se que a construção e a manutenção de bancos de dados destinados ao envio de propaganda eleitoral são práticas recorrentes durante as campanhas. No entanto, é importante mencionar que o manejo desses bancos de dados deve estar em conformidade não apenas com as restrições previamente estipuladas, mas também com as regulamentações estabelecidas no art. 57-E da Lei 9.504/1997 e no art. 31 da Resolução nº 23.610/2019 (Brasil, 2019).

Essas disposições normativas proíbem a doação, cessão e utilização de dados pessoais seja por parte da administração pública ou por empresas de direito privado, bem como a venda de cadastros eletrônicos, em benefício de candidatos, partidos políticos, coligações e federações.

Segundo Eduardo Magrani (2020), esta vedação geral impede que cadastros eletrônicos

sejam compartilhados por uma ampla gama de entidades ou governos estrangeiros, órgãos públicos, fornecedores de serviços públicos, sindicatos, ONGs financiadas publicamente, entre outros. Um acréscimo notável foi a inclusão de empresas privadas nesta lista após uma decisão do Supremo Tribunal Federal, no caso da ADI nº 4650, que declarou a inconstitucionalidade dos dispositivos legais que autorizavam as contribuições de pessoas jurídicas às campanhas eleitorais.

Caso essas regras sejam infringidas, podem resultar em penalidades aplicadas pela Justiça Eleitoral, incluindo multas que podem chegar a R$30.000,00 (Art. 57-E, § 2º, da Lei nº 9.504/1997 e art. 31, § 2º, da Res.-TSE nº 23.610/2019), bem como a cassação do registro ou diploma, se houver evidência de abuso de poder político ou econômico e uso indevido dos meios de comunicação (Brasil, 2019).

É relevante notar que o artigo 31, § 3º, da Resolução nº 23.610/2019 esclarece que a violação dessa norma eleitoral não exclui a aplicação de outras penalidades estabelecidas por lei, com destaque para a Lei Geral de Proteção de Dados (LGPD). Além disso, o § 4º do mesmo artigo estipula que o tratamento de dados pessoais, incluindo sua utilização, doação ou cessão, tanto por pessoa jurídica quanto por pessoa física, deve obedecer às disposições da Lei Geral de Proteção de Dados (Brasil, 2019).

Assim, além da fiscalização exercida pela Justiça Eleitoral, os agentes responsáveis pelo tratamento de dados devem aderir estritamente às diretrizes estabelecidas pela LGPD. Isso implica que eles estão sujeitos às regulamentações da Autoridade Nacional de Proteção de Dados (ANPD), tanto no contexto específico de comercialização, uso, doação ou transferência de dados pessoais, quanto em outras circunstâncias relacionadas ao tratamento de dados pessoais (TSE, 2021).

Essas considerações destacam a importância de as campanhas eleitorais serem cuidadosas com a procedência de seus dados e com quem pode acessá-los. Um exemplo marcante de violação desta norma é quando um órgão público compartilha dados pessoais de beneficiários de um programa social com um candidato, que utiliza esses dados para criar perfis e veicular propaganda eleitoral por meio de aplicativos de mensagens instantâneas e impulsionamento em redes sociais (TSE, 2021).

Nesse caso, a Justiça Eleitoral, como previamente elucidado, pode tomar medidas que incluem a suspensão do acesso ao conteúdo veiculado e a aplicação de multa de até R$30.000,00, nos termos dos artigos 57-I e 57-E, § 2º, da Lei 9.504/1997 (Brasil, 1997). Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) também tem o direito de investigar o ocorrido, com o objetivo de avaliar a conformidade do tratamento dos dados com a Lei Geral

de Proteção de Dados (LGPD). Durante essa investigação, a ANPD pode considerar vários aspectos, incluindo a base legal utilizada, a observância dos princípios da finalidade, necessidade e transparência, bem como o respeito aos direitos dos titulares dos dados. Dependendo da gravidade do caso, a ANPD pode emitir orientações ao controlador dos dados ou aplicar sanções administrativas, conforme previsto no artigo 52 da LGPD (TSE, 2021).

Os partidos políticos, coligações, candidatos e candidatas ainda têm a possibilidade de realizar propaganda eleitoral por meio do "impulsionamento de conteúdo" na internet, conforme estabelecido no artigo 57-C da Lei nº 9.504/1997 (Brasil, 1997).

O impulsionamento de conteúdo é definido como um mecanismo ou serviço que, por meio de contrato com provedores de aplicação de internet, amplia a divulgação da informação para alcançar usuários que normalmente não teriam acesso ao conteúdo. Isso inclui a priorização paga de conteúdos gerados por aplicativos de busca na internet (art. 37, inciso XIV, da Resolução nº 23.610/2019). Em outros dizeres, o impulsionamento de conteúdo permite que candidatos, partidos políticos e grupos promovam suas mensagens para um público mais amplo, incluindo eleitores em potencial que talvez não estivessem cientes das suas propostas (Brasil, 2019).

Uma das vantagens do impulsionamento é a capacidade de segmentar o público-alvo com base em diversos critérios, como idade, gênero, localização geográfica, interesses e comportamentos online. Isso possibilita direcionar mensagens para grupos específicos que têm mais probabilidade de se interessar pelo conteúdo. Além disso, os anúncios impulsionados podem ser personalizados para atender a diferentes grupos demográficos e interesses, permitindo criar mensagens específicas que ressoam com diferentes segmentos do eleitorado.

No entanto, é importante ressaltar que esse mecanismo ou serviço está sujeito a um conjunto de regras previstas na legislação eleitoral. Isso compreende a exigência de contratar provedores com sede e foro no país, bem como a obrigação de que sua finalidade seja exclusivamente promover ou beneficiar candidatas, candidatos ou suas agremiações, e a necessidade de identificar claramente as mensagens como propaganda eleitoral, conforme definido no art. 29 da Resolução nº 23.610/2019 (Brasil, 2019).

Ademais, a utilização de dados pessoais em estratégias de impulsionamento de conteúdo deve estar em total conformidade com as disposições legais da LGPD. Nesse sentido, deve-se identificar a base legal aplicável e garantir que a análise e a operação sejam devidamente registradas. Visto que a legislação eleitoral não estipulou uma base legal específica para o impulsionamento de conteúdo, a avaliação deve ser conduzida com base nas particularidades do caso concreto, levando em consideração as categorias de dados utilizadas, o método de coleta

e os diversos agentes envolvidos na operação, entre outros fatores relevantes. De maneira geral, o impulsionamento de conteúdo pode ser realizado de acordo com as bases legais do consentimento ou do legítimo interesse, desde que estejam alinhadas com o contexto factual e os requisitos legais aplicáveis à situação (TSE, 2021).

As campanhas ainda devem assegurar a transparência no tratamento de dados. Partidos políticos, candidatos, coligações e plataformas digitais devem disponibilizar avisos e políticas de privacidade de fácil acesso, apresentados em linguagem simples e com informações claras e precisas. Dado que o funcionamento da publicidade online e o uso de dados pessoais podem ser complexos para o cidadão comum, é recomendável incorporar recursos visuais que simplifiquem e tornem mais compreensível esse processo (TSE, 2021).

É inegável que existe uma clara relação entre o impulsionamento de conteúdo e a formação de perfis comportamentais. Frequentemente, o impulsionamento se apoia na criação desses perfis para direcionar o conteúdo ao público apropriado. Sob a ótica da Lei Geral de Proteção de Dados (LGPD), caso a criação desses perfis ocorrer unicamente por meio de decisões automatizadas, os titulares dos dados têm o direito de requerer uma revisão dessas decisões, conforme previsto no artigo 20 da lei. Além disso, a legislação impõe a necessidade de transparência na divulgação dos critérios e procedimentos utilizados para tomar essas decisões, sempre respeitando, no entanto, segredos comerciais e industriais (TSE, 2021).

A LGPD ainda habilita a Autoridade Nacional de Proteção de Dados (ANPD) a realizar auditorias caso o uso desses segredos comerciais ou industriais seja alegado como justificativa para não fornecer informações claras sobre a formação de perfis comportamentais, nos termos do art. 20, §2º (TSE, 2021). Isso reforça a importância de equilibrar a eficácia das estratégias de impulsionamento de conteúdo com a devida observância dos direitos de privacidade dos indivíduos.

Por fim, em qualquer procedimento de tratamento de dados envolvendo o impulsionamento de conteúdo, os direitos das pessoas titulares desses dados devem sempre ser respeitados. Partidos políticos, candidatas, candidatos, coligações, federações e plataformas digitais devem dar prioridade à implementação de mecanismos intuitivos e de fácil acesso. Tais mecanismos devem garantir às pessoas titulares o completo controle sobre o uso de seus dados. Nesse contexto, é altamente recomendável disponibilizar ferramentas simplificadas que facilitem a realização de diversas ações, como bloquear anúncios indesejados, solicitar o descadastramento, requerer a eliminação de dados, revogar o consentimento ou expressar oposição ao tratamento de dados, entre outras funcionalidades essenciais (TSE, 2021).

A ascensão da internet e das redes sociais reformulou os padrões de comunicação. De

acordo com Raquel Machado e Desirée Ferreira (2021), essa evolução levou muitos a enxergar o ciberespaço como um reflexo contemporâneo da ágora, evocando a antiga Atenas, berço da democracia direta. Com uma plataforma global ao alcance de um clique, a capacidade de influenciar e ser influenciado tomou proporções inéditas, reforçando a necessidade de uma comunicação consciente.

Nesta era digital, os comunicadores políticos precisam buscar originalidade e probidade. Isso vai além da mera prevenção de multas ou sanções. Trata-se de construir uma relação de confiança com o eleitorado. Afinal, o respeito mútuo entre candidatos e eleitores é a base de qualquer democracia saudável. Há uma tendência crescente de humanização na comunicação política. As mensagens, mais do que nunca, precisam ressoar em um nível pessoal e emocional. Além disso, os candidatos devem estar plenamente cientes dos canais que utilizam e do impacto que suas mensagens exercem sobre o público.

Dessa forma, a comunicação política é, no final das contas, uma forma de arte. Uma arte que requer equilíbrio entre legalidade, ética e engajamento. À medida que o cenário digital continua a evoluir, os comunicadores devem se adaptar, assegurando que suas mensagens não apenas estejam em conformidade com as leis, mas também ressoem eticamente com o seu público-alvo.

3.2 Uma visão eleitoral dos princípios de proteção de dados pessoais

A Lei Geral de Proteção de Dados (LGPD) surgiu como uma resposta à necessidade de diretrizes robustas para o manejo de dados pessoais no Brasil. Mais do que meras diretrizes, os princípios contidos nessa legislação constituem o coração e a estrutura da proteção de dados em nosso país. Eles delineiam e influenciam como entidades e indivíduos devem interagir com informações pessoais.

Ao considerar os princípios da LGPD como o alicerce inicial, evidencia-se a sua importância no processo de tomada de decisão. Eles atuam como bússolas, garantindo que as operações de tratamento sejam realizadas de forma ética, transparente e, acima de tudo, respeitosa aos direitos dos titulares dos dados.

Passa-se, então, à exploração de cada um dos princípios mencionados no artigo 6º da LGPD: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Serão eles que fornecerão parâmetros para abordagens relacionadas ao uso de dados pessoais em cenários eleitorais, pavimentando um caminho seguro para a comunicação das

campanhas com os eleitores.

O primeiro deles é o princípio da boa-fé. Destacado no *caput* do artigo 6º da referida legislação, ele enfatiza a necessidade de um tratamento transparente, íntegro e honesto dos dados pessoais. No contexto eleitoral, isso se traduz em uma obrigação para candidatos, partidos e equipes de campanha de serem abertos sobre suas práticas de coleta, uso e compartilhamento de informações dos eleitores. Eles devem esclarecer o motivo da coleta de dados, a maneira como serão empregados e quem terá acesso a eles. A integridade e a ética são fundamentais nesse processo, exigindo que as campanhas evitem atitudes enganosas, como propagar notícias falsas ou usar dados pessoais de forma inadequada para influenciar votos (Brasil, 2018).

Já o princípio da finalidade, conforme definido no artigo 6º, inciso I, da LGPD, está relacionado com os objetivos para os quais os dados pessoais são tratados. Em sua essência, ele estabelece que os dados pessoais só podem ser coletados com propósitos legítimos, específicos e claros, devendo previamente ser comunicados ao titular dos dados. Ressalta-se que qualquer tratamento posterior desses dados deve estar em conformidade com as finalidades originalmente informadas (Brasil, 2018).

Ao afirmar que os propósitos devem ser legítimos e específicos, significa que a finalidade não pode ir contra a lei (como as proibições da legislação eleitoral referentes à doação de bancos de dados) e não pode ser vaga ou abrangente. Coletar informações de eleitores sob a justificativa de "objetivos político-eleitorais", amplos e indefinidos, por exemplo, não está alinhado ao princípio da finalidade (Massaro et al., 2020).

Além disso, essa finalidade precisa ser explícita e comunicada ao detentor dos dados. Ou seja, é imperativo esclarecer ao titular qual será o uso específico de suas informações. Por exemplo, se uma campanha estiver coletando endereços de e-mail de eleitores para enviar *newsletters* informativas sobre as propostas do candidato, é fundamental informar de forma explícita ao eleitor que seus dados serão usados especificamente para esse envio de informações.

O princípio da finalidade também assegura que os dados não sejam posteriormente utilizados para propósitos que não estejam alinhados com a finalidade originalmente estabelecida. Dentro do cenário eleitoral, se um eleitor compartilhou seu endereço de e-mail para ser informado sobre as datas e locais de comícios de um determinado candidato, esse endereço não deve ser posteriormente utilizado para enviar pesquisas de opinião sobre temas não relacionados ao propósito autorizado ou para promover outros candidatos sem o consentimento do eleitor. Ou, ainda, se um eleitor forneceu informações demográficas para uma pesquisa eleitoral específica, esses dados não devem ser reutilizados para campanhas

publicitárias de empresas parceiras ou para outros fins que não foram claramente comunicados ao titular dos dados.

Ressalta-se que, ao final do tratamento, os dados pessoais devem ser eliminados ou tornados anônimos. Isso acontece quando o objetivo é atingido ou quando os dados já não são mais necessários ou pertinentes para alcançar a finalidade específica, conforme estabelecido no art. 15, inciso I, da LGPD. Contudo, em certas circunstâncias previstas no art. 16 da lei, os dados podem ser conservados mesmo após o término de seu tratamento (Brasil, 2018).

Em situações envolvendo dados de acesso público, faz-se necessário observar atentamente o princípio da finalidade. Registros de eleitores disponíveis em cartórios eleitorais, listagens de membros afiliados a partidos e informações divulgadas por usuários em seus perfis nas redes sociais exemplificam dados de acesso público. No caso das redes sociais, trata-se de informações que o próprio titular optou por tornar visivelmente públicas. A natureza pública de uma informação não implica sua livre utilização. As informações foram fornecidas ou divulgadas pelos usuários com propósitos específicos. Em qualquer situação, é fundamental garantir que exista uma base legal para o tratamento desses dados pessoais (Massaro et al., 2020).

Portanto, o tratamento de dados pessoais deve ser coerente com a finalidade apresentada ao titular no ato da coleta. Toda ação, desde a coleta até o processamento, deve ser pautada na transparência e na integridade, assegurando que o propósito inicialmente estabelecido seja honrado em todas as etapas.

O princípio da adequação, descrito no artigo 6º, inciso II, da LGPD, estabelece que o tratamento de dados pessoais deve ser coerente com as finalidades comunicadas ao titular dos dados, bem como em conformidade com o contexto do tratamento (Brasil, 2018).

Esse princípio está relacionado ao princípio da finalidade e envolve avaliar se as diferentes etapas de tratamento de dados são compatíveis com a finalidade original. Isso ocorre porque as operações de tratamento geralmente não são isoladas, incluindo coleta, armazenamento, compartilhamento e eliminação. Se as etapas subsequentes não forem compatíveis, uma nova finalidade deve ser identificada, garantindo a informação adequada ao titular dos dados (TSE, 2021).

No contexto eleitoral, ao coletar endereços de e-mail dos eleitores para enviar informações sobre suas propostas, um partido político deve evitar compartilhar esses dados com terceiros para fins não relacionados à política. O princípio da adequação assegura que o uso dos dados permaneça em conformidade com a intenção original e respeite os direitos dos titulares.

O princípio da necessidade, presente no artigo 6º, inciso III, da LGPD, determina o dever

de limitar o tratamento aos dados mínimos necessários para alcançar as finalidades desejadas, garantindo que os dados sejam pertinentes, proporcionais e não excessivos em relação aos objetivos do tratamento de dados. Sendo assim, nota-se um limite quantitativo e uma economicidade impostos por tal princípio no trato de dados, isto é, evitar o manuseio de informações em excesso em relação aos objetivos pretendidos (Brasil, 2018).

O agente responsável pelo tratamento de dados deve realizar uma análise cuidadosa das categorias de dados pessoais necessárias para alcançar uma finalidade específica. Isso envolve identificar os tipos de informações que são relevantes para atingir o propósito desejado. Ao fazer isso, ele deve evitar a coleta ou manipulação de dados além do que é estritamente necessário para alcançar os objetivos estabelecidos (TSE, 2021).

Essa abordagem ressalta a significância de restringir o tratamento aos dados essenciais, com o intuito de evitar os excessos informacionais, reduzindo os riscos de exposição e possíveis violações de privacidade. Além disso, demonstra o compromisso do agente de tratamento em respeitar os direitos dos titulares dos dados, garantindo que suas informações pessoais sejam tratadas de maneira responsável e conforme as finalidades comunicadas.

No âmbito eleitoral, a aplicação desse princípio ganha complexidade adicional, visto que está intrinsecamente ligado ao processo democrático em si. Dentro desse contexto, emerge um desafio intricado e ainda não completamente solucionado: estabelecer os parâmetros das informações que partidos políticos e candidatos devem considerar para garantir uma comunicação eficaz com os eleitores (Massaro et al., 2020).

Em países com sistema de voto obrigatório, como o Brasil, essa equação se torna ainda mais complexa, levando em conta que esse diálogo é primordial para o exercício pleno da cidadania. No entanto, a busca por uma comunicação efetiva com os eleitores não deve servir de justificativa para qualquer forma de tratamento de dados pessoais que desrespeite o princípio da necessidade (Massaro et al., 2020).

Esse dilema fica mais evidente em situações como a coleta de dados para criar perfis psicométricos detalhados de eleitores, visando ao microdirecionamento de mensagens, como foi o caso da Cambridge Analytica. Esse tipo de abordagem tende a ser uma clara violação do princípio da necessidade, pois envolve o tratamento excessivo de dados que ultrapassa os limites estabelecidos. Assim, é fundamental encontrar um equilíbrio entre a obtenção da informação necessária para uma comunicação eficaz e a preservação dos princípios de proteção de dados (Massaro et al., 2020).

No tocante ao princípio do livre acesso, este encontra-se presente no artigo 6º, inciso IV, da LGPD e positiva a garantia de consulta simplificada e gratuita sobre a forma e a duração

do tratamento, assim como sobre a integralidade dos dados pessoais dos titulares (BRASIL, 2018).

Ele é uma importante salvaguarda que reforça a transparência e a participação dos titulares no processo de tratamento de dados pessoais, garantindo aos indivíduos o direito de obter informações claras e acessíveis sobre como seus dados estão sendo utilizados, o propósito desse tratamento e por quanto tempo serão retidos. Isso possibilita que os titulares tenham um maior controle sobre suas informações pessoais e tomem decisões informadas em relação ao compartilhamento e uso de seus dados.

Em uma campanha eleitoral, o princípio do livre acesso é fudamental para fortalecer a transparência e a *accountability*. Ele permite que os eleitores tenham visibilidade sobre como os partidos políticos e candidatos estão coletando, armazenando e utilizando suas informações pessoais, auxiliando na construção de um ambiente de confiança entre eles e os agentes de tratamento de dados. Vale ressaltar que os titulares têm o direito de solicitar detalhes sobre o tratamento de seus dados, possibilitando que detectem eventuais irregularidades e tomem medidas para proteger sua privacidade.

Já o princípio da qualidade dos dados, previsto no artigo 6º, inciso V, da LGPD, estabelece a importância de garantir a precisão e a atualização das informações pessoais coletadas e tratadas. Esse princípio ressalta a necessidade de assegurar que os dados sejam corretos, completos e estejam atualizados, de modo a garantir a sua adequação e confiabilidade para os fins propostos (Brasil, 2018).

Para cumprir esse princípio, os agentes de tratamento de dados devem adotar medidas adequadas para garantir a veracidade das informações coletadas. Isso envolve a implementação de processos de validação, atualização e correção de dados, bem como a revisão periódica das informações armazenadas. A precisão dos dados é indispensável para garantir que as decisões tomadas com base nessas informações sejam confiáveis e não prejudiquem os direitos dos titulares.

No contexto eleitoral, o princípio da qualidade dos dados assume uma importância peculiar. Informações incorretas, desatualizadas ou incompletas podem impactar negativamente o processo democrático, levando a decisões equivocadas ou desinformadas por parte dos eleitores, partidos políticos e candidatos. Assegurar a qualidade dos dados utilizados em campanhas políticas contribui para a integridade do processo eleitoral e para a confiabilidade das informações divulgadas ao público.

Por sua vez, o princípio da transparência, mencionado no artigo 6º, inciso VI, da LGPD, ressalta a necessidade de garantir a clareza e a acessibilidade das informações relacionadas ao

tratamento de dados pessoais. Tal princípio visa promover a comunicação transparente entre os agentes de tratamento e os titulares, permitindo que os detentores das informações compreendam como seus dados estão sendo coletados, utilizados, compartilhados e protegidos (Brasil, 2018).

Em processos eleitorais, a abordagem racional no uso de dados pessoais exige a transparência por parte de partidos políticos e campanhas. Isso implica fornecer informações claras aos eleitores titulares dos dados, por meio de políticas de privacidade acessíveis e precisas. Essas políticas devem abordar a finalidade do tratamento, armazenamento, compartilhamento e medidas de segurança. Além disso, a convergência entre a LGPD e a legislação eleitoral pode ampliar a transparência, permitindo a fiscalização da integridade eleitoral. Isso pode incluir programas de governança no plano de campanha e registros detalhados de atividades de tratamento de dados para evitar abusos e garantir uma comunicação política ética e responsável (Massaro et al., 2020).

Em cada situação específica de coleta e tratamento de dados, é fundamental avaliar a melhor abordagem para garantir a transparência adequada. Um exemplo emblemático ocorreu durante a campanha eleitoral de 2022, no Rio de Janeiro, envolvendo o pastor Silas Malafaia. Nessa ocasião, o pastor enviou correspondência contendo informações políticas a um eleitor, sem obter o consentimento prévio deste indivíduo. Em resposta a essa ação, o eleitor decidiu tomar medidas legais e ingressou com uma ação no Tribunal de Justiça do Estado, buscando uma indenização no valor de R$ 10.000,00 (dez mil reais) (Lima Neto, 2022).

O eleitor alegou que teve sua privacidade comprometida pelo pastor, que acessou dados pessoais não autorizados, como seu nome completo e endereço residencial. Nessa situação, a transparência teria sido alcançada se o eleitor tivesse sido previamente informado sobre a coleta e utilização de seus dados, além de ter concedido seu consentimento de forma clara e específica para essa finalidade.

Outro caso notório de falta de transparência ocorreu no Estado do Ceará também durante as eleições de 2022. A cúpula do Partido Liberal utilizou indevidamente a documentação de três ex-candidatas a vereadora de Fortaleza, que haviam concorrido nas eleições de 2020, sem obter o consentimento delas. O partido reproduziu a documentação e efetivou o pedido de registro de candidatura dessas três ex-candidatas, com o intuito de fraudar a cota de gênero e atingir o número mínimo de mulheres na disputa eleitoral (Fraude…, 2023).

Esses exemplos realçam a necessidade urgente de uma abordagem mais rigorosa e ética no tratamento de dados pessoais, especialmente em campanhas eleitorais, garantindo que todas as ações sejam realizadas com total transparência e com o consentimento explícito daqueles

cujas informações estão sendo utilizadas.

Em meio aos desafios da era digital, o Tribunal Superior Eleitoral (TSE) tem trabalhado diligentemente para harmonizar a transparência democrática com a proteção de dados pessoais. Em 2020, uma decisão marcante do Tribunal determinou que as informações pessoais e patrimoniais de candidatos não eleitos não seriam mais divulgadas publicamente no Sistema de Divulgação de Candidaturas e Contas Eleitorais (DivulgaCandContas). O ministro Og Fernandes, ao defender a decisão, enfatizou que, embora os candidatos sejam vistos como figuras públicas durante o período eleitoral, após seu encerramento, os dados de candidatos não eleitos não necessitariam de exposição pública, dando destaque ao direito à privacidade (Brasil, s.d.)

O sistema DivulgaCandContas, por sua vez, foi ressaltado como um instrumento vital para a transparência, proporcionando aos cidadãos informações detalhadas sobre todos os candidatos. No entanto, o debate também evidenciou a importância de balancear essa transparência com a privacidade individual. Assim, enquanto a transparência é primordial durante as eleições, o direito à privacidade pode se tornar preponderante após esse período, sobretudo para candidatos não eleitos. Esta visão é corroborada pela jurisprudência do TSE, que reconhece a necessidade de equilibrar a transparência com outros direitos fundamentais após o término do processo eleitoral (Brasil, s.d.).

Em um mundo cada vez mais digitalizado, onde os dados são considerados o “novo petróleo”, garantir sua segurança torna-se imprescindível para proteger não apenas a privacidade dos indivíduos, mas também para assegurar a confiança nas relações digitais. O princípio da segurança, estabelecido no artigo 6º, inciso VII, da Lei Geral de Proteção de Dados (LGPD), enfatiza este ponto. Ele sublinha a importância de implementar medidas técnicas e administrativas para salvaguardar os dados pessoais contra acessos indevidos e situações que possam comprometê-los, seja por acidentes, ilegalidades ou tratamentos impróprios (Brasil, 2018).

No ambiente eleitoral, a ênfase na segurança da informação assume uma importância duplamente significativa. Enquanto protege o eleitor de potenciais ameaças à sua privacidade, especialmente em tempos onde informações podem ser usadas para influenciar decisões, ela também protege a integridade da campanha, sua teia de apoiadores e táticas de comunicação. Além disso, essa proteção reforça a relação de confiança entre o eleitor e o candidato ou partido em questão (Massaro et al., 2020).

Em relação às estratégias de segurança da informação no ambiente eleitoral, a Autoridade Nacional de Proteção de Dados (ANPD) enfatiza a importância de instituir uma

política de segurança, ainda que inicial, abrangendo aspectos relacionados ao tratamento de dados pessoais. A formação contínua e a conscientização dos colaboradores são componentes primordiais, visto que o elemento humano é determinante para a efetividade das estratégias de segurança. Contratos estabelecidos devem ser meticulosamente geridos, incorporando cláusulas de confidencialidade e assegurando um controle de acesso rigoroso, pautado no princípio da restrição de acesso (TSE, 2021).

É imperativo que os agentes responsáveis pelo tratamento de dados assegurem a proteção das informações armazenadas, empregando métodos como a pseudonimização e a criptografia. Além da atualização contínua dos sistemas e da vigilância constante contra potenciais vulnerabilidades, dispositivos móveis e infraestruturas em nuvem devem aderir a padrões de segurança elevados. Diante de incidentes de segurança, a resposta deve ser imediata e eficiente, com comunicação célere à ANPD e às partes interessadas (TSE, 2021).

Nesta ótica, é relevante mencionar o princípio da prevenção, articulado no artigo 6º, inciso VIII, da LGPD, que orienta a implementação de ações preventivas contra potenciais danos decorrentes do tratamento de dados pessoais (Brasil, 2018). Ele ressalta a necessidade de, antes de iniciar o tratamento de dados, as campanhas avaliarem meticulosamente os riscos e potenciais danos associados. Se identificados riscos significativos, medidas protetivas devem ser implementadas ou o tratamento pode ser pausado. Esta abordagem visa resguardar tanto o eleitor quanto a integridade da campanha (Massaro et al., 2020).

Em um exemplo prático, durante uma eleição municipal, um partido, que estava prestes a lançar um aplicativo para mobilizar eleitores, ao adotar o princípio da prevenção, descobriu vulnerabilidades durante testes de segurança. Decidiu, então, postergar o lançamento até que todas as questões fossem adequadamente solucionadas. A adoção desse princípio não apenas protege os eleitores de possíveis danos, mas também demonstra o compromisso e a responsabilidade do partido ou candidato em relação à proteção de dados.

Em outro giro, o princípio da não discriminação, previsto no art. 6º, inciso IX, da LGPD, visa garantir que o tratamento de dados pessoais não seja utilizado para fins discriminatórios ou abusivos (Brasil).

No âmbito eleitoral, o princípio da não discriminação ganha uma importância particular. Os dados dos eleitores não devem ser usados para segmentar, excluir ou favorecer certos grupos de forma injusta. É inaceitável que informações pessoais sejam utilizadas para enviar mensagens enganosas a um grupo particular de eleitores com o propósito de influenciar suas decisões de voto de maneira manipulativa. Da mesma forma, disseminar informações falsas ou criar obstáculos que dificultem o voto de certos segmentos da população vai contra os valores

fundamentais de uma democracia justa e equitativa.

Portanto, o princípio da não discriminação assegura a equidade no uso dos dados, protegendo a integridade democrática. Ele garante que todas as vozes sejam ouvidas e respeitadas, evitando manipulações que prejudiquem as escolhas dos eleitores ou erodam a confiança política.

Por fim, o artigo 6º, inciso X, da LGPD enfatiza o princípio da responsabilidade e prestação de contas, assegurando que os agentes encarregados do tratamento de dados sejam responsabilizados por suas ações e tenham o dever de prestar contas sobre suas práticas (Brasil, 2018).

A LGPD, de forma acertada, fornece uma gama de ferramentas para auxiliar nesse processo. Dentre elas, destaca-se a criação de um Programa de Governança em Privacidade (PGP), mencionado no art. 50, § 2º, inciso I. O PGP serve para demonstrar o comprometimento do agente de tratamento, estabelecendo diretrizes e procedimentos internos que assegurem a total conformidade com as normas e as melhores práticas de proteção de dados. Isso engloba ações como o mapeamento e inventário de dados pessoais, detalhando todos os procedimentos, como suas finalidades, bases legais, compartilhamentos e estratégias de segurança (TSE, 2021).

Uma outra ferramenta é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), empregado especialmente em contextos de alto risco, visando avaliar possíveis ameaças às liberdades pessoais. Segundo o art. 5º, inciso XVII, da LGPD, este relatório detalha os procedimentos de tratamento de dados que podem representar ameaças às liberdades civis e direitos fundamentais, apresentando também estratégias, salvaguardas e mecanismos para redução desses riscos. Dado que, no âmbito eleitoral, pode haver manipulação de uma vasta quantidade de dados sensíveis, como opiniões e filiações partidárias, o RIPD é uma importante ferramenta para garantir transparência e responsabilidade (TSE, 2021).

Com essas ferramentas em mãos, partidos, candidatos e demais agentes envolvidos no processo eleitoral têm a capacidade de conduzir suas atividades de maneira mais segura e alinhada às expectativas da sociedade. Além de cumprir com as obrigações legais, a implementação desses instrumentos pode servir como um diferencial, demonstrando proatividade e um compromisso genuíno com a privacidade e os direitos dos eleitores.

Em um mundo onde a proteção dos dados é cada vez mais valorizada, respeitar todos os princípios mencionados solidifica a confiança entre eleitores e agremiações políticas. Esta confiança é a pedra angular da democracia. Portanto, ao abraçá-los, as campanhas não só evitam contratempos legais, mas também reforçam seu compromisso com a integridade e a ética, fortalecendo, assim, o tecido da democracia.

3.3 Principais leis para o tratamento de dados pessoais em campanhas eleitorais

Após explorar os princípios de proteção de dados no cenário eleitoral, faz-se necessário destacar os principais alicerces jurídicos que autorizam o tratamento de dados pessoais: as bases legais.

Estas bases são estipuladas por lei e definem as circunstâncias sob as quais entidades, públicas ou privadas, podem manipular informações pessoais. Elas estabelecem as condições para coleta, armazenamento, compartilhamento e processamento de tais informações. A correta identificação e aplicação da base legal apropriada assegura a conformidade com as normas vigentes, minimizando os riscos de penalidades e respeitando os direitos dos titulares de dados.

Conforme abordado no capítulo anterior, o artigo 7º da LGPD lista os dez requisitos que autorizam o tratamento de dados pessoais não sensíveis, enquanto o artigo 11 define as bases legais para para lidar com dados de caráter sensível, que demandam uma maior proteção (Brasil, 2018).

Inicialmente, a atenção será voltada para as bases legais arroladas no art. 7º supracitado. Dessas dez bases legais, quatro se destacam no ambiente eleitoral: consentimento, obrigação legal ou regulatória, execução de contrato e legítimo interesse. Vale ressaltar que nenhuma base legal é inerentemente superior ou mais importante do que outra. Em vez disso, cada base legal é adequada para circunstâncias específicas (Brasil, 2018).

O consentimento, como a primeira base a ser destacada, representa uma manifestação livre, informada e inequívoca pela qual a pessoa titular de dados concorda com o tratamento de suas informações pessoais para uma finalidade específica, conforme estabelecido no art. 5º, inciso XII, da LGPD. Esse mecanismo garante que os titulares de dados tenham controle e autonomia sobre suas informações, permitindo-lhes decidir conscientemente como e quando seus dados podem ser utilizados (Brasil, 2018).

A ênfase no consentimento posiciona o titular dos dados no epicentro do processo de tratamento de informações, sublinhando a premissa de que as informações são de propriedade do indivíduo, e não da organização que as coleta ou gerencia. Dada essa perspectiva, em diversos contextos, notadamente no cenário político-eleitoral, o consentimento emerge como a justificativa legal mais adequada para o tratamento de dados.

O consentimento é tido como livre quando o titular dos dados tem a autonomia de aceitar ou rejeitar o tratamento proposto sem enfrentar consequências adversas ou interferências do controlador de dados que possam comprometer ou distorcer sua decisão (TSE, 2021). Por

exemplo, se um candidato solicita o e-mail de um eleitor para enviar materiais de campanha e informa que, caso o eleitor não forneça seu e-mail, não terá acesso a determinados benefícios ou informações, esse consentimento não é verdadeiramente livre. O eleitor está sendo indiretamente coagido a fornecer seus dados sob a ameaça de perder algo em troca.

O consentimento é reconhecido como informado quando o agente de tratamento fornece todas as informações necessárias para que o titular dos dados possa tomar uma decisão consciente. Isso significa que, antes de dar seu consentimento, o titular deve estar ciente de como, por quanto tempo e para quais finalidades seus dados serão tratados pelo controlador. Qualquer alteração nas condições iniciais acordadas invalida o consentimento anteriormente dado. Assim, um novo consentimento deve ser obtido ou uma diferente base legal deve ser aplicada, sempre mantendo o titular informado sobre as mudanças (TSE, 2021). Para ilustrar, se uma campanha eleitoral recebe permissão para enviar atualizações via WhatsApp, ela não pode, posteriormente, usar esses contatos para fins comerciais sem um novo consentimento. Tal ação iria contra o conceito de consentimento informado da LGPD.

Por último, o consentimento é visto como inequívoco quando o responsável pelo tratamento obtém uma manifestação explícita da vontade do titular dos dados. Não se pode presumir ou inferir o consentimento a partir de ações tácitas ou ausência de ação por parte do titular. Vale destacar que é dever do controlador dos dados comprovar que o consentimento foi adquirido em conformidade com as diretrizes da LGPD. Assim, é recomendável manter um registro detalhado e documentar todos os passos tomados para assegurar que o consentimento concedido esteja livre de irregularidades e tenha sido fornecido com todas as informações pertinentes (TSE, 2021).

Ressalta-se que é fundamental assegurar o direito de revogação do consentimento, conforme delineado no art. 8º, §5º, da LGPD. O controlador dos dados tem a responsabilidade de disponibilizar um meio simples e sem custos para que o titular possa revogar seu consentimento, interrompendo o tratamento de seus dados. Esse meio pode ser um simples formulário eletrônico ou um e-mail solicitando o descadastramento. A decisão de revogar é de direito exclusivo do titular e deve ser prontamente atendida a cada solicitação (TSE, 2021).

A segunda base relevante para campanhas políticas está relacionada ao cumprimento de obrigações legais ou regulatórias. Ela autoriza o controlador a tratar dados pessoais para atender a determinações previstas em leis ou regulamentos, conforme delineado no art. 7º, inciso II, da LGPD. Em outras palavras, em situações específicas, o tratamento de dados não é uma opção, mas sim uma imposição legal. No entanto, o controlador deve sempre respeitar os parâmetros e finalidades estipulados pela legislação ou norma pertinente (Brasil, 2018).

Ademais, mesmo que o consentimento não seja requisitado nesses casos, o titular dos dados deve ser informado sobre tal tratamento. A clareza e transparência precisam ser mantidas para preservar a confiança e assegurar que os direitos dos titulares dos dados sejam observados, inclusive quando o tratamento é determinado por preceitos legais.

Por exemplo, todos os candidatos e partidos políticos são obrigados a prestar contas de suas campanhas à Justiça Eleitoral. Isso inclui detalhes sobre doadores, valores doados e despesas realizadas. A coleta e tratamento desses dados são mandatados por lei.

Da mesma forma, quando um indivíduo decide se candidatar a um cargo eletivo, ele deve fornecer uma série de informações pessoais à Justiça Eleitoral, como declarações de bens, antecedentes criminais e comprovantes de filiação partidária. Essa coleta de dados é uma exigência legal para garantir a elegibilidade do candidato.

Além disso, todo cidadão que se registra para votar fornece dados pessoais à Justiça Eleitoral. Esses dados são usados para criar o título de eleitor, determinar a zona eleitoral e garantir que a pessoa vote apenas uma vez. A coleta desses dados também é uma obrigação legal.

Ademais, quando um cidadão decide se filiar a um partido político, seus dados são registrados e, posteriormente, enviados à Justiça Eleitoral. Isso é feito para cumprir as normas que regulam as filiações partidárias e garantir que um cidadão não seja membro de mais de um partido ao mesmo tempo.

Outra situação é quando a legislação eleitoral estabelece regras claras sobre quando, onde e como a propaganda eleitoral pode ser realizada. Para garantir o cumprimento dessas regras, os candidatos e partidos podem ser obrigados a fornecer informações sobre suas atividades de propaganda, incluindo dados sobre gastos, fornecedores e locais de eventos.

Em casos de suspeitas de irregularidades eleitorais, como compra de votos ou financiamento ilegal de campanha, a Justiça Eleitoral pode exigir que candidatos e partidos forneçam informações adicionais. A coleta e análise desses dados são feitas com base em obrigações legais para garantir a integridade do processo eleitoral.

Todos esses exemplos destacam situações em que o tratamento de dados pessoais no contexto político-eleitoral é realizado não por escolha, mas por uma exigência legal ou regulatória.

A terceira base legal, aplicável no contexto político-eleitoral, refere-se à execução de contrato. De acordo com o art. 7°, inciso V, da LGPD, essa base autoriza o tratamento de dados pessoais quando necessário para cumprir um contrato do qual o titular é parte ou em procedimentos preliminares a pedido do titular. O tratamento dos dados deve estar alinhado

com a finalidade do contrato, coletando-se somente os dados que são primordiais para tal propósito (Brasil, 2018).

Há controvérsias sobre o alcance dessa base legal, especialmente em relação ao que é considerado tratamento “necessário” para a execução de um contrato e se o titular precisa ser sempre uma das partes envolvidas. Diante dessas reflexões, no ambiente eleitoral, torna-se fundamental identificar relações contratuais que demandem tratamento de dados e discernir se esse tratamento é indispensável para o contrato ou se atende a uma mera conveniência do controlador. Se for o último caso, outra base legal, como o legítimo interesse, pode ser mais apropriada (Santos et al., 2021).

Se a relação entre os filiados e os partidos for interpretada como um contrato, então o uso de seus dados pessoais para informá-los sobre uma convenção ou eleição de chapas pode ser visto como intrínseco ao propósito principal desse contrato. É importante destacar que essa base legal deve ser aplicada quando a questão em foco for uma obrigação principal, e não um aspecto secundário ou adicional, do acordo estabelecido entre o titular dos dados e o responsável pelo seu tratamento (Massaro et al., 2020).

A quarta base legal está atrelada ao legítimo interesse. Conforme o art. 7º, inciso IX, da LGPD, essa base permite o tratamento de dados pessoais quando for necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (Brasil, 2018).

Aludida base, válida somente para dados pessoais não sensíveis, destaca-se por sua flexibilidade, podendo ser adaptada a uma ampla gama de finalidades. Devido a essa característica, o art. 10 da LGPD estabeleceu diretrizes para a aplicação do legítimo interesse. Uma delas enfatiza que o tratamento de dados pessoais, além de estar em conformidade com a lei, deve ser rigorosamente vinculado ao objetivo almejado, garantindo-se sempre a máxima transparência nesse processo (Brasil, 2018).

A título de exemplo, candidatas, candidatos, partidos políticos, coligações e federações não podem alegar legítimo interesse em acessar dados sob custódia da administração pública ou de entidades privadas, considerando que essa ação é proibida pela legislação eleitoral, nos termos do art. 57-E da Lei nº 9.504/1997 e do art. 31 da Resolução-TSE nº 23.610/2019. Igualmente, a comercialização de cadastros eletrônicos por pessoas físicas e jurídicas é proibida, eliminando, assim, a chance de alegar legítimo interesse nessas situações (art. 57-E, § 1º, da Lei nº 9.504/1997 e o art. 31, § 1º, da Resolução-TSE nº 23.610/2019). Além disso, o envio de propaganda eleitoral por telemarketing não pode ser justificado pelo legítimo interesse, pois é uma prática proibida tanto pela Resolução-TSE nº 23.610/2019 quanto pelo Supremo

Tribunal Federal (STF), conforme a ADI nº 5.122 (TSE, 2021).

Além disso, o art. 10, inciso II, da LGPD determina que o controlador, antes de adotar essa base legal, deve levar em conta os direitos e liberdades fundamentais do titular dos dados, bem como avaliar se é razoável supor que ele possui alguma expectativa quanto ao uso de seus dados pessoais, o que se alinha ao conceito de legítima expectativa (Brasil, 2018).

Assim, se um partido político, candidata ou candidato optar por essa base legal, deve-se seguir as diretrizes do art. 10 da LGPD, incluindo os princípios da necessidade, finalidade e transparência. A ANPD, conforme o § 3º desse artigo, pode requerer um relatório de impacto na proteção de dados pessoais, através do qual o controlador deve evidenciar o cumprimento dos critérios definidos pela LGPD para o tratamento dos dados (TSE, 2021).

Imagine um candidato que, durante uma campanha eleitoral anterior, organizou encontros comunitários para debater propostas locais. Os participantes, interessados nas discussões, forneceram seus e-mails para receber informações sobre futuras atividades. Agora, em uma nova eleição, o candidato planeja enviar um boletim informativo a esses eleitores, atualizando-os sobre suas novas propostas. Dada a interação anterior, o candidato pode alegar legítimo interesse para essa comunicação, pois os eleitores já demonstraram interesse em suas iniciativas e é razoável supor que gostariam de ser informados sobre novidades. O objetivo da comunicação é claro: manter os eleitores informados. No entanto, para garantir a transparência, o boletim deve explicar o motivo do contato e oferecer uma opção para que os eleitores possam optar por não receber mais essas atualizações. O candidato, ao enviar o boletim, utiliza apenas os e-mails, sem tratar outros dados pessoais desnecessários. Contudo, faz-se necessário que o candidato siga as diretrizes da LGPD e da legislação eleitoral, assegurando que o uso do legítimo interesse esteja em conformidade com as normas e respeite os direitos dos titulares dos dados.

Quando se trata de dados pessoais sensíveis, a LGPD, reconhecendo o potencial discriminatório e abusivo desses dados, estabeleceu critérios mais rígidos para o seu tratamento. O artigo 11 da supracitada lei listou oito hipóteses que autorizam o tratamento de dados pessoais. No entanto, no âmbito das campanhas eleitorais, apenas três são particularmente relevantes: o consentimento do titular, o cumprimento de uma obrigação legal ou regulatória pelo controlador e o exercício regular de direitos (Brasil, 2018).

Para dados pessoais sensíveis, o consentimento, conforme estipulado no art. 11, inciso I, da LGPD, além de ser informado, livre e inequívoco, deve ser específico e claramente destacado. Um desafio reside em entender a amplitude e o significado exato de um consentimento classificado como específico e destacado (Brasil, 2018).

Segundo Mario Viola e Chiara Teffé (2023), o consentimento é considerado específico quando é expresso para finalidades precisas e claramente definidas pelo controlador antes do tratamento dos dados. Para esses autores, o consentimento é considerado “destacado” quando o titular possui acesso integral ao documento que detalha todas as informações pertinentes sobre o tratamento dos dados. Essas informações, por sua vez, devem ser ressaltadas para que o próprio consentimento também se destaque. Além de se referir a dados específicos e estar atrelado a um propósito definido, essa manifestação de vontade deve ser claramente evidenciada no documento que permite o tratamento dos dados.

Assim, em campanhas eleitorais, é aconselhável que a solicitação de consentimento para o tratamento de dados pessoais sensíveis seja distinta do corpo principal do texto ou que se usem recursos para realçá-la, esclarecendo de forma explícita quais dados serão coletados e a maneira como o controlador pretende utilizá-los. A finalidade do consentimento deve ser específica, limitada e direcionada exclusivamente à atividade para a qual foi concedido. Uma abordagem eficaz seria usar um formulário que obtenha de forma separada o consentimento para a coleta e tratamento desses dados para uma finalidade específica (TSE, 2021).

A base referente ao cumprimento de obrigação legal ou regulatória pelo controlador, disposta no art. 11, inciso II, alínea a, da LGPD, também pode ser aplicada em campanhas eleitorais. Isso significa que, em determinadas situações, o controlador pode tratar dados pessoais sensíveis, mesmo sem o consentimento do titular, se estiver cumprindo uma determinação legal ou regulamentar (TSE, 2021).

Já quando se trata da base legal para “exercício regular de direitos, inclusive em contrato”, encontrada no art. 11, inciso II, alínea d, há discussões sobre sua proximidade com a base legal de “execução de contrato” e quais são as reais diferenças entre elas (Brasil, 2018).

Em face disso, ainda se estuda a viabilidade de usar essa base legal em situações contratuais que envolvam o tratamento de dados pessoais, desde que tal tratamento seja direcionado ao exercício de um direito específico (Santos et al., 2021).

Dessa forma, nota-se que as hipóteses para o tratamento de dados pessoais sensíveis em campanhas eleitorais limita consideravelmente a autonomia dos controladores. É de suma importância ter uma atenção redobrada, visto que dados como opiniões políticas, origem racial ou étnica e convicções religiosas são comumente empregados na segmentação de eleitores e no direcionamento de campanhas publicitárias.

Ademais, vale destacar que esse regramento mais rigoroso não se aplica somente ao tratamento de dados sensíveis em si, mas também a qualquer tratamento que possa revelar tais dados, como interações e informações em redes sociais que possam indicar as inclinações

políticas de um indivíduo (Santos et al., 2021).

Exatamente porque as bases legais podem ser distintas para cada situação e demandarem um entendimento das particularidades das atividades de tratamento em um campo específico, este estudo não busca, e realmente não poderia, sugerir uma única solução para todos os cenários. Em vez disso, visa destacar algumas considerações a serem ponderadas nesse processo.

Cabe à Justiça Eleitoral, com sua estrutura robusta de monitoramento do processo eleitoral e em colaboração contínua com a Autoridade Nacional de Proteção de Dados (ANPD), garantir a correta aplicação das bases legais no contexto eleitoral. A complexidade e especificidade das atividades de tratamento de dados nesse campo exigem uma abordagem conjunta e bem informada. Através dessa cooperação, é possível assegurar que os direitos dos cidadãos sejam protegidos, enquanto se mantém a integridade e transparência do processo eleitoral.

3.4 O papel dos Agentes de tratamento, do Encarregado e da Autoridade Nacional de Proteção de Dados Pessoais

A governança de dados no contexto eleitoral assume uma importância inegável, devendo ser pautada pela ética, legalidade e transparência. O correto tratamento de dados pessoais, alinhado aos princípios e às bases legais previamente discutidos, emerge como uma ferramenta poderosa para moldar estratégias políticas e campanhas eleitorais, facilitando uma interação mais precisa e efetiva com os eleitores. No entanto, faz-se necessário que todos os envolvidos no tratamento estejam cientes e cumpram as obrigações e responsabilidades estabelecidas pela legislação, assegurando que as atividades relacionadas aos dados respeitem os direitos dos indivíduos e os padrões de proteção.

Em meio a esse cenário, é de suma importância entender o papel dos diversos atores existentes. Desde partidos políticos e candidatos até a Autoridade Nacional de Proteção de Dados (ANPD), cada um tem uma função na preservação da privacidade e dos direitos dos eleitores.

De acordo com a LGPD, constituem agentes de tratamento o controlador e o operador de dados pessoais. Nos moldes do art. 5º, inciso VI, da lei mencionada, o controlador é o agente responsável por tomar as principais decisões concernentes ao tratamento de dados pessoais e por estabelecer os objetivos desse tratamento. Por sua vez, o operador, consoante previsão do art. 5º, inciso VII, é definido como o agente responsável pela realização do tratamento de dados

em nome do controlador e de acordo com o propósito por este estabelecido. Em outras palavras, o operador apenas pode tratar os dados para o intuito previamente traçado pelo controlador (Brasil, 2018).

Controladores e operadores podem ser pessoas naturais ou jurídicas, de direito público ou privado, delineados a partir de seu viés institucional. Na hipótese de uma pessoa jurídica, a organização assume a responsabilidade como controladora dos dados pessoais. Ela é a entidade responsável por determinar as normas para o tratamento desses dados, e seus representantes ou agentes designados têm a incumbência de aplicar as orientações previamente estabelecidas.

Por outro lado, quando uma pessoa física é a responsável pelas decisões mais relevantes relacionadas ao tratamento de dados pessoais, ela pode atuar como controladora. Nessa posição, a pessoa física age de forma independente, em nome próprio, sem estar sujeita à subordinação de uma pessoa jurídica ou atuando como membro de um órgão desta. Essa autonomia permite que ela determine as finalidades e os meios do tratamento dos dados pessoais, além de tomar as decisões relacionadas à proteção dessas informações.

Em suma, o poder de decisão é um elemento central na diferenciação entre controlador e operador. Mesmo que a LGPD não estabeleça expressamente que o controlador e o operador devam celebrar contrato a respeito do tratamento de dados, tal ajuste se revela uma boa prática, visto que as cláusulas contratuais prescrevem limites à atuação do operador, estabelecem claros parâmetros para a alocação de responsabilidade entre as partes e minimizam as incertezas e os riscos oriundos da operação. Os aspectos que podem ser fixados em contrato são o objeto, a duração, a natureza e o objetivo do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos, as obrigações e as responsabilidades vinculadas ao cumprimento da LGPD (ANPD, 2021).

Na esfera político-eleitoral, candidatos, partidos, coligações e federações podem ser considerados agentes de tratamento. Esses atores estão engajados na condução de campanhas eleitorais, as quais demandam o uso de dados pessoais, incluindo dados de eleitores, apoiadores e doadores.

Sob a ótica da Lei dos Partidos Políticos (Lei nº 9.096/1995) e da Lei Geral de Proteção de Dados Pessoais, fica evidente que o sistema de proteção de dados também se aplica aos partidos, coligações e federações. Isso porque os partidos políticos são considerados pessoas jurídicas de direito privado, e a LGPD, como mencionado anteriormente, abrange o tratamento de dados pessoais tanto por pessoas naturais quanto por pessoas jurídicas de direito público ou privado. Portanto, assim como os órgãos estatais e as empresas, os partidos políticos também são obrigados a cumprir as disposições da legislação nacional de proteção de dados.

Os partidos políticos desempenham um papel central no processo eleitoral e podem atuar como controladores de dados pessoais. Eles estabelecem as finalidades para o tratamento dos dados, bem como determinam as estratégias de campanha. As coligações, que são alianças estabelecidas entre diversos partidos durante as eleições, também possuem a capacidade de atuar como controladoras no tratamento de dados.

Da mesma forma, as federações partidárias, que são organizações constituídas por diferentes partidos políticos, podem desempenhar o papel de controladoras de dados, estabelecendo as diretrizes para o tratamento das informações pessoais. Elas podem coletar, armazenar e utilizar dados pessoais de membros dos partidos que as compõem ou de indivíduos interessados na política.

Em uma campanha eleitoral, é fundamental que o controlador tenha uma visão abrangente dos fluxos de dados, preferencialmente por meio de um painel de conformidade utilizado por todos os responsáveis pelo tratamento e pelos operadores envolvidos. Esse sistema centralizado de gerenciamento de informações deve incluir informações de contato e identificar o encarregado dentro da estrutura organizacional. Ademais, é necessário ter um mapeamento completo e controle dos dados que estão sendo tratados e transferidos, juntamente com seu propósito legal associado (Magrani, 2020).

De acordo com as normativas de proteção de dados, o controlador deve cumprir com as obrigações de informação, o que engloba a disponibilização da identidade e de detalhes de contato do responsável pelo tratamento e do encarregado da proteção de dados, da finalidade do tratamento, da base jurídica para sua realização, da duração do tratamento, bem como dos direitos conferidos ao titular dos dados, dentre outras informações relevantes. É igualmente importante que o controlador seja capaz de processar de forma ágil e eficiente as solicitações de acesso do titular dos dados (Magrani, 2020).

Além disso, o controlador deve implementar mecanismos para manter um registro que acompanhe a linha do tempo do consentimento dado ou retirado pelo indivíduo em relação ao tratamento de seus dados. Também é necessário estabelecer permissões e controles de acesso granulares, garantindo que apenas os principais agentes na estrutura da campanha tenham autorização aos grupos de dados pertinentes. Todos esses aspectos do relacionamento entre o operador e o titular dos dados devem ser traduzidos em interfaces de fácil utilização, como aplicativos e formulários, a fim de garantir que o titular compreenda claramente seus direitos e que o responsável pelo tratamento possa demonstrar conformidade com as leis vigentes (Magrani, 2020).

Desse modo, o diálogo claro e inequívoco entre os agentes de tratamento – nessa

hipótese, o candidato, o partido político, a coligação ou a federação partidária – e o titular dos dados (o eleitor) é elementar. Notadamente, o titular deve compreender como seus dados estão sendo tratados. Sem essa clareza, as demais garantias estabelecidas pela legislação de proteção de dados ficam comprometidas.

Conforme a situação específica, as plataformas online e as empresas de análise de dados podem ser consideradas controladoras ou operadoras. Isso dependerá do papel desempenhado por elas no tratamento dos dados pessoais. Se tiverem autonomia e tomarem decisões sobre o propósito e os meios de processamento dos dados, serão consideradas controladoras. Já se atuarem apenas em nome e sob instruções de outras entidades responsáveis pelo tratamento, serão consideradas operadoras. É importante analisar o caso e os acordos estabelecidos entre as partes para determinar corretamente o papel de cada uma no contexto do tratamento de dados (Comissão Europeia, 2018a).

Outro importante protagonista para a eficácia das boas práticas em proteção de dados pessoais é o encarregado (art. 5º, inciso VIII, da LGPD). Tal figura serve como elo de comunicação entre os agentes de tratamento, as pessoas titulares e a Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Além de sua função de comunicação, o encarregado pode exercer um papel ativo na formulação e implementação de políticas de privacidade, bem como nas ações de conscientização interna e externa (TSE, 2021).

Para que o encarregado desempenhe efetivamente suas atribuições, é essencial que suas informações estejam prontamente acessíveis, conforme disposto no § 1º do artigo 41 da LGPD. Isso garante que os titulares dos dados e a ANPD possam estabelecer contato com o encarregado de forma rápida e eficiente, promovendo a transparência e facilitando a resolução de questões relacionadas à proteção de dados. Durante uma campanha eleitoral, o encarregado assume várias responsabilidades. Uma das principais é acompanhar de perto a conformidade com a legislação de proteção de dados e outras regulamentações aplicáveis (Brasil, 2018).

Além disso, o encarregado deve fornecer orientações e recomendações ao candidato, partido político, coligação ou federação com base em suas observações. Ele busca identificar áreas em que a conformidade pode ser aprimorada e oferecer diretrizes sobre práticas de segurança, revisão de políticas de privacidade e termos de uso, além de treinamento para a equipe envolvida no tratamento de dados (Magrani, 2020).

Ainda, em um contexto de eleições, é o encarregado que facilita a interlocução entre os titulares dos dados, a autoridade de proteção de dados e outras partes interessadas, respondendo a perguntas, solicitações ou reclamações relacionadas ao tratamento de dados. É importante destacar que, para desempenhar essas funções de forma eficaz, o encarregado deve ser

independente. Isso pode ser um desafio quando contratado internamente, pois é necessário garantir sua imparcialidade e autonomia na supervisão do tratamento de dados (Magrani, 2020).

Além das partes previamente citadas, existe outro ator de destaque que desempenha um papel importante na garantia efetiva da proteção de dados: a Autoridade Nacional de Proteção de Dados (ANPD).

A instituição dessa entidade como autarquia especial e suas incumbências foi, inicialmente, alvo de veto presidencial motivado por questões de inconstitucionalidade formal do projeto, como o vício de iniciativa. No entanto, diante da pressão de diversos grupos que ressaltaram a necessidade de preencher a lacuna deixada pela ausência da ANPD, a matéria foi regulamentada por meio da Medida Provisória nº 869/2018, a qual, posteriormente, foi convertida na Lei nº 13.853/2019 (Bariani Jr.; Martins, 2021).

A Lei nº 13.853/2019 optou por instituir a ANPD como um órgão vinculado à estrutura orgânica da Presidência da República, o que suscitou preocupações quanto à sua capacidade operacional e autonomia gerencial e administrativa. A vinculação direta a um órgão superior com funções predominantemente políticas poderia comprometer a independência e a atuação técnica da organização, gerando desafios para o pleno exercício de suas funções (Brasil, 2019).

Tendo em vista essas preocupações, em 14 de junho de 2022, uma nova Medida Provisória, a MP nº 1.124, foi promulgada e publicada no Diário Oficial da União, a qual foi convertida na Lei nº 14.460, de 25 de outubro de 2022, reestruturando a ANPD e transformando-a, conforme previsto originalmente, em uma autarquia especial. Com a nova legislação, a ANPD passou a ter independência técnica e decisória, não estando mais hierarquicamente subordinada à Presidência da República (Brasil, 2022).

Essa autarquia detém uma série de atribuições essenciais, que incluem a orientação, fiscalização, aplicação de sanções, estabelecimento de normas e diretrizes, bem como a função de elo com outras autoridades de proteção de dados internacionais. Sua atuação é fundamental para garantir o cumprimento da legislação de proteção de dados em todo o território nacional (Brasil, 2019).

Vale ressaltar ainda outras competências conferidas a ela, tais como (i) promover, na população, o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (ii) dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (iii) ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (iv) celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito

de processos administrativos, dentre outras (Brasil, 2019).

No tocante às sanções, a ANPD possui competência exclusiva para aplicar as penalidades administrativas estabelecidas pela LGPD, conforme previsto no caput do artigo 55-K. No entanto, é importante notar que um único evento pode acarretar consequências em diferentes esferas jurídicas (Brasil, 2018).

A título ilustrativo, o art. 18, § 8º, da LGPD assegura que as pessoas cujas informações são objeto de tratamento possuem o direito de formalizar reclamações tanto perante a ANPD quanto perante órgãos de defesa do consumidor. Além disso, o art. 52, § 2º, enfatiza que as sanções aplicadas conforme a LGPD não excluem aquelas previstas no Código de Defesa do Consumidor (CDC) e em outras legislações específicas. De modo semelhante, o art. 22 reforça a viabilidade de proteção dos interesses e direitos dos titulares de dados por intermédio do Poder Judiciário (Brasil, 2018).

Na esfera eleitoral, o cenário não deve ser diferente. Assim, um mesmo evento poderá potencialmente estar sujeito à fiscalização e imposição de penalidades tanto por parte da ANPD quanto pela Justiça Eleitoral, levando em consideração o cenário factual e as disposições legais relevantes para a situação (TSE, 2021).

Bruno Cezar Andrade de Souza (2022, p. 162) também endossa essa atuação concomitante das duas entidades, ressaltando as competências específicas de cada uma delas. Nas palavras do autor:

> Compreendo que, cada um tendo uma expertise peculiar, é possível que haja atuação entre as instâncias, na medida em que a ANPD poderia aplicar as sanções administrativas decorrentes do tratamento indevido de dados. À Justiça Eleitoral ficaria a atribuição de fiscalizar e punir, no âmbito jurisdicional, os institutos próprios previstos na legislação eleitoral, ainda que decorrentes de utilização indevida de dados pessoais.

Isso não impede, entretanto, que a ANPD atue de forma conjunta e coordenada com outros órgãos e entidades públicas. O parágrafo 3º do artigo 55-J da LGPD prevê essa coordenação, com o intuito de assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados (Brasil, 2018).

O Tribunal Superior Eleitoral (TSE) e a Autoridade Nacional de Proteção de Dados (ANPD) têm demonstrado compreender a importância dessa colaboração, como atestado pela assinatura, em 23 de novembro de 2021, do Acordo de Cooperação Técnica nº 4/2021. A finalidade primordial desse acordo é a harmonização das diretrizes da LGPD com as disposições das leis eleitorais, através da formulação conjunta de materiais educativos e da

integração da proteção de dados pessoais no cenário eleitoral (Brasil, 2021).

Fruto desse Acordo de Cooperação Técnica foi a publicação, no início do ano de 2022, do Guia Orientativo – Aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral. Esse guia foi desenvolvido pelas duas entidades e tem como objetivo destacar os elementos fundamentais a serem observados por candidatos, coligações, federações e partidos políticos em relação ao gerenciamento de informações pessoais dos eleitores. O documento estabelece uma conexão entre a avaliação das normas vigentes e situações práticas, o que confere maior aplicabilidade e orientação aos assuntos abordados (Brasil, 2022).

Por fim, cumpre destacar que a primeira multa aplicada pela Autoridade Nacional de Proteção de Dados brasileira ocorreu em 6 de julho de 2023 e foi direcionada a uma empresa de telemarketing. A empresa foi penalizada no valor de R$ 14.400,00 (catorze mil e quatrocentos reais) devido à oferta de envio de mensagens em massa, via celular e WhatsApp, para até 130 (cento e trinta) milhões de pessoas (Convergência Digital, 2023).

A ANPD baseou sua decisão em um relatório que demonstrava que a empresa Telekall estava oferecendo segmentação geográfica e grandes volumes de mensagens para fins eleitorais. A empresa alegou que, embora houvesse contato com possíveis candidatos, não houve venda real de serviços e que suspendeu temporariamente as atividades de disparo em massa para se adequar à Lei Geral de Proteção de Dados (Convergência Digital, 2023).

A fiscalização começou a partir de uma denúncia do Ministério Público de São Paulo sobre a oferta de listas de contatos de WhatsApp para campanhas eleitorais. A ANPD considerou que as atividades da empresa não se enquadravam nas hipóteses da LGPD para o tratamento de dados. Ademais, a empresa não possuía um encarregado de dados, e a ANPD enfatizou que o uso de dados públicos deve cumprir o princípio da finalidade da coleta de informações (Convergência Digital, 2023).

Vale ressaltar ainda que, caso o Ministério Público dispusesse de evidências relacionadas aos candidatos ou partidos políticos beneficiados por essas circunstâncias, teria a opção de acionar a Justiça Eleitoral, que tem a responsabilidade de garantir a integridade do processo eleitoral. Sob essa perspectiva, a Justiça Eleitoral examinaria as provas obtidas e tomaria as medidas para impor as penalidades específicas relacionadas às questões eleitorais. Essas penalidades podem variar desde multas até ações de abuso de poder econômico e abuso de poder nos meios de comunicação social, dependendo das particularidades do caso concreto.

Assim, assegurar a conformidade com as normas de proteção de dados, especialmente em atividades político-eleitorais, é fundamental para preservar a democracia. Os agentes

responsáveis pelo tratamento de dados pessoais, bem como o encarregado e a Autoridade Nacional de Proteção de Dados possuem a responsabilidade de aplicar as bases legais e os princípios de proteção de dados, além de garantir o pleno exercício dos direitos dos titulares dos dados.

Portanto, a luta para estabelecer práticas de proteção de dados efetivas, equilibradas e transparentes é imprescindível. Em um mundo cada vez mais globalizado, a proteção de dados transcende os limites individuais e se torna uma salvaguarda da própria democracia. Cada passo na direção de um uso mais ético e responsável de informações pessoais no contexto eleitoral contribui para a preservação do sistema democrático, garantindo a igualdade, a liberdade e a justiça para todos.

4 SALVAGUARDANDO A DEMOCRACIA DOS RISCOS DIGITAIS

Com a crescente democratização do acesso às novas tecnologias, a utilização de dados pessoais tornou-se uma prática generalizada no cenário político, sendo uma ferramenta empregada por candidatos e partidos para alcançar os eleitores. No entanto, em alguns casos, essa abordagem é inadequada, colocando os cidadãos em risco de violações de seus direitos fundamentais, como a privacidade e a proteção de dados, e minando a integridade do processo democrático, com influências obscuras sobre a decisão do eleitor.

É neste contexto que surgem normas como a LGPD e outras legislações similares com o objetivo de salvaguardar a democracia e minimizar os riscos digitais que ameaçam o livre exercício democrático da população. Essas regulamentações visam equilibrar o uso legítimo de dados para fins políticos com a necessidade de proteger os interesses individuais e a integridade do sistema democrático.

4.1 Democracia Digitalizada: proteção de dados no cenário político-eleitoral

A existência substancial da democracia, conforme argumenta Robert Dahl (2001), depende do cumprimento de vários critérios. Entre eles estão a participação igual e efetiva das pessoas na esfera política, a igualdade do valor do voto, o “entendimento esclarecido” (que permite ao indivíduo aprender sobre a política que o afeta e suas consequências), o poder de influenciar o planejamento de políticas e a inclusão de todos os adultos no processo.

Complementando essa perspectiva, Norberto Bobbio (1986) enfatiza a natureza evolutiva da democracia, contrastando-a com a imutabilidade do despotismo. Ele sugere que, enquanto a democracia é caracterizada por sua adaptabilidade e dinamismo, o despotismo tende a ser rígido e inalterado. No entanto, Bobbio também destaca que, apesar das transformações que a democracia pode enfrentar, há valores e princípios centrais que devem ser consistentemente mantidos e valorizados, como as noções de transparência e visibilidade do poder, bem como a defesa da dignidade da pessoa humana.

Na esfera democrática, é essencial a garantia do exercício de alguns direitos invioláveis do cidadão, tais como o direito à liberdade de expressão, de opinião, de associação, de reunião, dentre outros. No entanto, a prática dessas liberdades na era da digitalização da sociedade trouxe consigo a questão do compartilhamento de dados pessoais com empresas e organizações estatais, o que requer uma avaliação cuidadosa dos riscos correspondentes, especialmente na esfera político-eleitoral.

Sabe-se que determinados temas não param de exigir um novo olhar do Direito, apresentando, a cada período, desafios e necessidades de adequação. O mesmo ocorre com a democracia. Diante da conjuntura vivenciada, faz-se indispensável uma observância periódica, sobretudo para reafirmar sua forma no país.

Em anos de eleições, ressurgem as disputas e emergem novos fatores diante das oposições comumente intensificadas pela maior disposição dos candidatos em expressar seus pontos de vista e conquistar a confiança do eleitorado. Essa dinâmica, intrínseca ao processo democrático, conduz a uma reflexão sobre as estratégias adotadas na arena política. Com o advento de novas tecnologias e o avanço da inteligência artificial, elevou-se o interesse pelo marketing eleitoral digital, que possui a finalidade de alcançar ou influenciar as necessidades humanas, semelhante ao marketing tradicional, porém dentro do ecossistema online.

O marketing eleitoral digital é uma estratégia de comunicação e divulgação política que utiliza as plataformas e ferramentas digitais para promover candidatos, partidos políticos e suas propostas durante campanhas eleitorais. Ele envolve a criação de conteúdo online, como anúncios em redes sociais, e-mails, mensagens de texto, vídeos, blogs e outros meios digitais, visando alcançar e engajar eleitores de maneira direcionada e eficaz. Os algoritmos desempenham um papel significativo nesse cenário, auxiliando na segmentação e na entrega do conteúdo customizado.

Contudo, a digitalização das campanhas eleitorais também trouxe desafios. A Fundação Getúlio Vargas (Ruediger, 2017) revelou a presença significativa de contas automatizadas, ou robôs, em debates online. O estudo apontou que, durante as eleições presidenciais de 2014, mais de 10% das interações no Twitter (agora chamado de X) foram geradas por essas contas. Estes robôs, frequentemente chamados de *bots*, são *softwares* criados para imitar comportamentos humanos nas redes, podendo disseminar mensagens em larga escala, moldando a opinião pública e, potencialmente, influenciando resultados eleitorais. Tal realidade levanta uma questão preocupante: como os eleitores podem diferenciar um debate genuíno de uma narrativa manipulada?

Na sociedade moderna, a informação se converte em poder a partir do momento em que a tecnologia permite a transformação de mensagens parciais e dispersas em mensagens em massa e organizadas. Como resultado, os riscos à privacidade do cidadão experimentam um crescimento exponencial. Seguindo esse raciocínio, Antonia Espíndola Longoni Klee e Guilherme Magalhães Martins (2014) destacam os perigos associados à violação da privacidade na era da informação, que incluem o uso inadequado de informações pessoais, a categorização das pessoas com base em características como hábitos de consumo, a imposição de normas

comportamentais e a discriminação dos cidadãos.

É inegável que o diálogo com os eleitores é parte integrante do processo democrático. Esse diálogo não apenas estimula a construção de agendas participativas, permitindo que os cidadãos influenciem a política e contribuam para a tomada de decisões, mas também possibilita a realização de campanhas políticas alinhadas às expectativas e necessidades da sociedade.

Tal diálogo só é possivel graças a uma multiplicidade de técnicas de comunicação. Todavia, a sutileza e a sofisticação com que muitas dessas técnicas são empregadas podem gerar desconfiança quanto ao uso de dados pessoais, colocando em xeque a solidez do processo democrático. Afinal, os indivíduos só podem tomar decisões realmente bem fundamentadas sobre quem eleger se estiverem seguros de que suas escolhas não foram indevidamente influenciadas (EDPB, 2019).

Desse modo, fornecer aos cidadãos transparência, precisão e acessibilidade quanto ao tratamento de seus dados pessoais é decisivo para que possam exercer autonomia sobre suas informações. Conforme já explanado no capítulo anterior, a transparência é um princípio fundamental da LGPD. Esse princípio reflete uma racionalidade compartilhada entre as normas de proteção de dados e as normas de direito eleitoral. Ele visa reduzir a assimetria de poder e informação, promovendo um equilíbrio mais justo e igualitário no processo democrático (Massaro et al., 2020).

Dentro do universo das plataformas digitais, a combinação de vastos conjuntos de dados com algoritmos avançados de aprendizado de máquina confere a corporações, como o Google e o Facebook, um poder de vigilância e controle ainda maior do que aquela tradicionalmente atribuída a agentes governamentais. Esse poder, no entanto, não está isento de responsabilidades e consequências. Tais empresas de tecnologia enfrentam o desafio constante de garantir a privacidade e a segurança das informações de seus usuários. Quando falham nesse dever, as repercussões podem ser significativas, tanto em termos de imagem quanto financeiramente.

Na Austrália, o Tribunal Federal aplicou uma multa de, aproximadamente, US$ 40 milhões de dólares ao *Google* por fornecer informações enganosas sobre a coleta e uso de dados em *smartphones* Android entre janeiro de 2017 e dezembro de 2018. Essa não foi a primeira vez que a empresa de tecnologia se envolveu em polêmicas relacionadas à privacidade dos usuários. A decisão do Tribunal, anunciada em julho de 2021, foi baseada nas investigações da *Australian Competition & Consumer Commission (ACCC)*, órgão similar ao Procon no Brasil (Schendes, 2022).

O órgão australiano concluiu que o *Google* coletou e manteve dados de localização dos

usuários por meio da configuração *Web & Activity*, mesmo quando o histórico de localização estava desativado. A presidente da ACCC afirmou, em um comunicado, que esses dados retidos eram usados pela plataforma para direcionar anúncios a determinados consumidores. Estima-se que cerca de 1,3 milhão de contas australianas foram afetadas por essa prática invasiva. Em resposta à decisão do Tribunal, um porta-voz do *Google* enfatizou o compromisso da plataforma em atualizações contínuas para proporcionar controle, transparência e produtos úteis aos usuários (Schendes, 2022).

Uma pesquisa recente conduzida por Douglas Leith, professor de ciência da computação do *Trinity College* em Dublin, na Irlanda, levantou acusações contra dois aplicativos do Google que vêm pré-instalados em diversos *smartphones* Android. Segundo o estudo, os aplicativos "Discador" e "Mensagens" estariam coletando e transmitindo informações sem o consentimento dos usuários, além de não oferecer a opção de recusa *(opt-out)* (Ghedin, 2022).

De acordo com o pesquisador, os dados coletados seriam enviados para o *Google Play Services Clearcut* e o *Firebase Analytics*, ambos pertencentes ao *Google*, possibilitando a identificação dos dispositivos, números de telefone e, no caso das ligações, a duração das chamadas. Douglas Leith argumentou que essa prática poderia violar a legislação europeia de proteção de dados pessoais, embora reconheça que as implicações legais vão além do escopo da pesquisa. O *Google* confirmou a veracidade das descobertas e declarou estar colaborando com o pesquisador desde novembro de 2021, quando foi abordado para resolver os problemas identificados nos dois aplicativos mencionados (Ghedin, 2022).

Outro caso envolvendo a coleta indevida de dados pessoais foi protagonizado pela empresa *Microsoft*. A gigante da tecnologia foi condenada a pagar US$ 20 milhões (aproximadamente R$ 98,4 milhões) à Comissão Federal do Comércio (FTC), agência de defesa do consumidor dos Estados Unidos, por capturar, entre 2015 e 2020, dados pessoais de crianças menores de 13 anos registradas na plataforma de jogos online da empresa sem o devido consentimento dos pais, além de reter esses dados para seu benefício próprio. Um representante da *Microsoft* afirmou que não apenas cumpriria a decisão da FTC, como também se empenharia no desenvolvimento de um novo sistema de validação de identidade e idade, com o objetivo de oferecer experiências adequadas ao público jovem (Presse, 2023).

A *Apple* também foi multada em € 8 milhões (aproximadamente R$ 46,2 milhões) pela *Commission Nationale Informatique & Libertés (CNIL)*, agência francesa de proteção de dados, por coletar dados de usuários da App Store sem o devido consentimento deles. Naquele período, era possível desativar o identificador coletado pela *Apple*, no entanto a opção estava escondida nas configurações do sistema e vinha ativada por padrão. A punição manchou a imagem pró-

privacidade que a Apple cultivava e usava como fator de diferenciação para seus produtos. A empresa afirmou que iria recorrer da decisão (Ghedin, 2023).

A utilização em larga escala de informações dos usuários por organismos privados e estatais representa um desafio relevante para o direito à proteção de dados. Um dos métodos frequentemente empregados por empresas para obter dados de plataformas de mídia social é a prática conhecida como “raspagem” de dados. Por meio desse procedimento, elas coletam informações, como nome e número de celular dos usuários, e compilam em bancos de dados, que são vendidos a candidatos e partidos políticos para o envio de mensagens em massa (Mello, 2020).

Uma investigação conduzida pelo jornal Folha de São Paulo revelou que a empresa BomBrasil.net comercializava, por meio de seu site, bancos de dados de números de telefone celular contendo informações como nome, endereço, bairro, renda e data de nascimento do titular da conta. Além disso, a empresa oferecia um *software* que permitia a coleta de dados de usuários das plataformas *Instagram* e *Facebook*, bem como disponibilizava serviços de envio automático de mensagens diretas pelo Instagram e de comentários automatizados em postagens de perfis específicos (Mello, 2020).

Esses serviços, embora lucrativos para a empresa e interessantes para as campanhas, estavam em desacordo com a Lei Geral de Proteção de Dados (LGPD), pois envolviam a coleta e venda de dados sem o devido consentimento dos usuários. Ademais, a propagação massiva de mensagens utilizando esses dados poderia comprometer a integridade do processo democrático, distorcendo o diálogo público e influenciando indevidamente as decisões dos eleitores.

Recentemente, a empresa de segurança ESET divulgou a descoberta de um caso alarmante envolvendo a venda de um suposto banco de dados contendo 487 milhões de números de usuários do *WhatsApp*, provenientes de 84 países diferentes. Essa suposta base de dados, revelada em um espaço virtual de hackers, incluía cerca de 8 milhões de números pertencentes ao Brasil, além de 45 milhões do Egito, 35 milhões da Itália, 32 milhões dos Estados Unidos, 29 milhões da Arábia Saudita, 20 milhões da França, 20 milhões da Turquia e 10 milhões da Espanha. Essa descoberta revela a magnitude e a abrangência global dessa possível exposição de dados no ambiente virtual, o que pode colocar em risco a privacidade e a segurança das informações pessoais dos usuários de diversas nações. Conforme o post publicado no fórum de hackers, os dados foram coletados por meio de raspagem de dados (Hackers [...], 2022).

Com a evolução tecnológica e a digitalização em ritmo acelerado da sociedade, os dados tornaram-se ativos preciosos, cobiçados não só por corporações, mas também por governos

globais. Um estudo conduzido pela *Surfshark* revelou um aumento expressivo nas requisições de dados pessoais de usuários de redes sociais por parte de autoridades governamentais e órgãos de segurança pública, especialmente durante o ano de 2020, marcado pela pandemia de Covid-19. No Brasil, houve um crescimento de 89% nesse tipo de solicitação em relação ao ano anterior (Hackers [...], 2022b).

Esse crescente aumento nas demandas por informações de usuários de plataformas de mídia social também gera sérias inquietações relacionadas à possibilidade de abusos de poder por parte do Estado. Essa questão ganha contornos ainda mais críticos quando consideramos o risco de uma vigilância ampla e indiscriminada desses usuários, com consequências diretas para a solidez do processo democrático.

A pesquisa também enfatizou o papel das empresas de tecnologia na divulgação de dados pessoais em resposta às requisições das autoridades. A Apple liderou em termos de índices de compartilhamento, atendendo à maioria dos pedidos, com uma taxa de cumprimento de 80%. Por sua vez, a *Microsoft*, o *Facebook* e o *Google* também mostraram respostas significativas, com taxas variando de 69% a 72% (Pedido [...], 2022).

No cenário brasileiro, o *Facebook* e o *Google* foram alvos do maior número de solicitações de dados de usuários feitas pelas autoridades, totalizando 165,9 mil e 139,4 mil contas, respectivamente. O *Facebook* divulgou informações em 64% desses casos, enquanto o *Google* cumpriu com 62% das solicitações. Esses números não só evidenciam a posição central que essas empresas de tecnologia ocupam no atual ecossistema de coleta de dados no país, mas também levantam questões pertinentes sobre a privacidade, segurança e equilíbrio entre a necessidade de informação e os direitos dos usuários (Pedido [...], 2022).

À medida que as estatísticas apontam para um aumento nas solicitações de dados tanto por plataformas quanto por autoridades, a questão da responsabilidade ganha destaque no debate sobre privacidade e proteção de dados. Assumir o compromisso de investir recursos para implementar medidas sólidas e atualizadas de segurança cibernética, além de promover a transparência e a gestão ética dos dados, é imperativo para garantir a confiança dos usuários e manter a integridade das informações, especialmente diante das ocorrências de vazamento de dados pessoais.

Infelizmente, o Brasil tem sido alvo de incidentes que impactaram consideravelmente as instituições estatais. Casos recentes, como o vazamento de informações pessoais e de saúde de mais de 16 milhões de pacientes brasileiros infectados pelo coronavírus e os ataques de *ransomware* sofridos pelo governo, que comprometeram o banco de dados de vacinação de COVID-19, evidenciam a vulnerabilidade dessas instituições frente às ameaças cibernéticas

(Vinte [...], 2022).

Segundo um estudo recente da *Surfshark*, referente ao segundo trimestre de 2022, o Brasil ocupou a 4ª posição no ranking global de violações de segurança cibernética. A pesquisa revelou que, desde 2004, mais de 244,4 milhões de contas de brasileiros foram vazadas, enfatizando a importância de medidas efetivas de cibersegurança e conscientização sobre a segurança digital (Vinte [...], 2022).

Isso tem contribuído para que os dados pessoais de cidadãos brasileiros sejam altamente acessíveis e de baixo custo para os criminosos, impulsionando um mercado global de informações que já movimentou milhões de dólares. Números de cartões de crédito e endereços de e-mail pessoais estão entre os tipos de dados mais cobiçados, sendo comercializados por valores relativamente baixos. Em média, os infratores pagam R$ 47,00 (quarenta e sete reais) por informações pessoais de brasileiros, enquanto em outras nações, como a República Tcheca, tais dados podem chegar a custar até R$ 5.800,00 (cinco mil e oitocentos reais) (Demartini, 2022).

Além disso, os cibercriminosos têm acesso a uma ampla variedade de informações pessoais, incluindo logins de contas bancárias, senhas de serviços online, números de telefone, passaportes, identidades e carteiras de criptomoedas. Os dados disponíveis para venda na *dark web* são majoritariamente documentos e informações financeiras, enquanto as credenciais de acesso a contas e combinações de e-mails e senhas representam parcelas menores do mercado (Demartini, 2022).

Dentro do cenário político-eleitoral, é de suma importância que todos os envolvidos – desde candidatos e partidos até autoridades e a população – estejam alertas e se protejam contra os perigos da exposição não autorizada de dados. O Brasil, dada sua situação atual, apresenta-se como um alvo propício a tais ameaças. Dados pessoais, quando expostos, podem ser habilmente empregados para orientar campanhas ou influenciar, de forma indevida, as decisões dos eleitores. Uma ilustração vívida dessa estratégia é a prática de microssegmentação ou microdirecionamento, cujos detalhes serão explorados a seguir.

Assim, para enfrentar os desafios das campanhas digitais, não basta apenas focar no controle de conteúdo. A linha entre a moderação e a restrição da liberdade de expressão é delicada e precisa ser navegada com cautela. É preciso adotar novos métodos que atualizem os valores e as normas do jogo democrático. Isso envolve concentrar esforços na identificação de comportamentos abusivos que simulam e distorcem o debate público, comprometem o acesso à informação política, fragilizam a autonomia de decisão dos eleitores, violam sua privacidade e prejudicam a dignidade de indivíduos e grupos sociais (Brito Cruz et al., 2019).

Nesse panorama, a observância estrita das leis de proteção de dados pessoais em campanhas eleitorais assume uma importância indiscutível. Essas legislações ajudam a reduzir o uso instrumental de dados e mitigar o impacto da desinformação e da propaganda computacional, que são frequentemente utilizadas para manipulação política. A eficácia dessas normativas, no entanto, depende da sinergia e cooperação dos diversos atores envolvidos, incluindo autoridades reguladoras, partidos políticos, plataformas digitais e sociedade civil. Esta discussão será aprofundada no tópico 4.3, onde serão apresentadas orientações de boas práticas para campanhas eleitorais alinhadas às leis de proteção de dados pessoais. Por ora, faz-se necessário entender a dinâmica da microssegmentação política no ambiente digital.

4.2 Afinando a mensagem: a arte e a ciência da microssegmentação política online

Na sociedade contemporânea, imersa na dinâmica da denominada "sociedade do espetáculo"[2], somos testemunhas de um fenômeno dominante: o culto ao "parecer ser", no qual as pessoas consomem narrativas que, na realidade, são meramente ilusórias. O sensacionalismo tornou-se uma das *commodities* mais lucrativas para uma ampla gama de plataformas de mídia social. A comercialização da informação, muitas vezes divorciada de sua veracidade, tem conquistado uma fatia crescente da atenção da sociedade. A virtualização das relações humanas e o fluxo incessante de informação nas redes são consequências inevitáveis desta evolução.

Nesse cenário de uma sociedade permanentemente interconectada, as campanhas eleitorais vêm se adaptando para adotar estratégias baseadas em dados e técnicas de comunicação política personalizada. Quanto mais informações disponíveis sobre o eleitorado, maiores são as chances de um candidato obter êxito em uma eleição e consolidar seu poder.

Dentro dessa evolução estratégica, emerge uma modalidade inovadora de publicidade política: a microssegmentação política online. Originada nos Estados Unidos, onde uma regulamentação menos rígida sobre proteção de dados pode ter favorecido seu rápido desenvolvimento e adoção, essa técnica encontrou terreno fértil na União Europeia, sendo empregada em larga escala em eleições nacionais de países como Reino Unido, Países Baixos, Alemanha e França (Dobber; Fathaigh; Borgesius, 2019).

A microssegmentação ou microdirecionamento político online envolve o envio de mensagens altamente personalizadas com o intuito de influenciar, informar ou mobilizar, mas

[2] Obra filosófica e política de Guy Debord, publicada em 1967, que faz uma crítica feroz à sociedade contemporânea, ou seja, à sociedade de consumo, à cultura da imagem e à invasão da economia em todos os setores da vida.

também, em alguns casos, de dissuadir, confundir ou desmobilizar os eleitores. Para que isso aconteça, é necessário coletar e processar dados pessoais, criando grupos-alvo específicos que se tornarão receptores dessas mensagens (Dobber; Fathaigh; Borgesius, 2019).

Esses dados podem abranger desde informações básicas, como nome e endereço, até aspectos mais complexos, como opiniões políticas e histórico sociocultural. Com o avanço tecnológico e a ascensão das redes sociais, surgiram várias organizações voltadas para coleta e análise de dados para fins políticos.

Nos Estados Unidos, empresas como Aristotle e Catalist se especializaram em reunir registros eleitorais individuais, combiná-los com outros conjuntos de dados públicos e comerciais, e disponibilizá-los para campanhas mediante o pagamento de uma taxa.

A Catalist, por exemplo, afirma possuir um extenso banco de dados contendo informações de mais de 265 milhões de pessoas. Este acervo inclui uma gama diversificada de informações, desde dados do censo até informações comerciais e geográficas relacionadas ao mercado de mídia. A empresa se dedica a manter essa base de dados constantemente atualizada, incorporando registros estaduais, atualizações comerciais, processando alterações de endereços em nível nacional e adotando outras estratégias de atualização de dados. Segundo a Catalist, esse repositório auxilia organizações e campanhas a identificar e se comunicar com membros, simpatizantes e potenciais apoiadores, considerando tanto sua localização atual quanto seus endereços anteriores (Catalist, 2023).

Já a empresa Aristotle se posiciona como um proeminente provedor de dados políticos, atendendo a grandes campanhas, organizações comunitárias e pesquisadores tanto no âmbito nacional quanto internacional. Seu portfólio inclui um Arquivo Nacional de Eleitores com registros de mais de 235 milhões de votantes, um Arquivo Nacional de Consumidores com perfis de mais de 259 milhões de consumidores, um Arquivo Nacional de Doadores documentando mais de 190 milhões de contribuições e um registro atualizado de Novos Migrantes, com mais de 1,2 milhão de atualizações de endereço mensais (Aristotle, 2023).

Uma vez coletados, os dados são submetidos a algoritmos de aprendizado de máquina, e os resultados obtidos dependem do tipo de algoritmo utilizado. Isso permite fazer previsões sobre questões específicas, como resultados políticos ou identificação de padrões nos dados. A implementação desses algoritmos permite que os atores políticos identifiquem subgrupos de eleitores com características comuns, como demografia e atitudes. Com base nesses resultados, é possível elaborar mensagens ou estratégias específicas para cada subgrupo ou até mesmo para indivíduos – uma prática denominada *nanotargeting* – com o intuito de mobilizar ou desmobilizar determinados eleitores (Papakyriakopoulos, 2018).

A comunicação da mensagem pode ser teoricamente realizada de duas maneiras distintas. A primeira envolve a formação de grupos de usuários com características comuns e, em seguida, direcioná-los diretamente por meio do serviço de publicidade da plataforma. Isso permite que os ativistas personalizem públicos-alvo sem a necessidade de associar manualmente os usuários às suas identidades no mundo real. A mensagem é simplesmente transmitida por meio da plataforma. Essa abordagem oferece a vantagem da eficiência e da facilidade de implementação (Papakyriakopoulos, 2018).

Por outro lado, a segunda maneira implica a observação manual das atividades futuras de um usuário no *Facebook* e, com base em dados sociodemográficos adicionais disponíveis, a tentativa de estabelecimento de outra forma de comunicação, como e-mail, correio ou número de telefone, entre outros. Embora essa segunda abordagem seja mais demorada, complexa e, em algumas situações, inadequada, é importante notar que, na União Europeia, a viabilidade dessa estratégia é significativamente reduzida devido às rigorosas leis de proteção de dados. Para que essa segunda abordagem seja aplicável, os atores políticos devem desenvolver plataformas, aplicativos ou serviços por meio dos quais obtenham o consentimento explícito das pessoas antes de direcioná-las com mensagens customizadas (Papakyriakopoulos, 2018).

Os dados pessoais são um recurso de imenso valor na personalização da comunicação entre candidatos e seus eleitores, permitindo ajustar essa interação com base nos hábitos, opiniões e preferências dos indivíduos. A capacidade de realizar microssegmentação com base em uma ampla gama de informações torna cada dado potencialmente valioso, abrangendo desde dados do consumidor até padrões de navegação na internet.

Tendo em vista a riqueza de detalhes oferecidos por aludida técnica, surge um questionamento: qual seria a diferença entre a microssegmentação e a segmentação tradicional? Dobber, Fathaigh e Borgesius (2019) explicam que a distinção não se baseia necessariamente no tamanho do público-alvo, mas sim no grau de uniformidade percebido pelo anunciante político. Em outras palavras, um público microalvo recebe uma mensagem adaptada a uma ou mais características específicas, consideradas essenciais pelo anunciante político para tornar esse público mais receptivo à mensagem personalizada. Por outro lado, uma mensagem direcionada de forma convencional não leva em conta as nuances de heterogeneidade existentes na população.

Para ilustrar: suponha que um candidato esteja concorrendo a um cargo público em uma cidade, onde os eleitores têm uma ampla variedade de preocupações e interesses. Na segmentação tradicional, a equipe de campanha pode agrupar os eleitores com base em categorias amplas, como idade, gênero e local de residência. Assim, eles podem direcionar

mensagens genéricas, como “Melhoraremos a educação” ou “Aumentaremos a segurança”. Contudo, essa abordagem, embora útil em algumas circunstâncias, pode não ser tão eficaz em contextos mais complexos e diversificados.

Já na microssegmentação, a equipe de campanha adota uma abordagem mais refinada. Eles coletam dados detalhados sobre os eleitores, incluindo informações sobre suas preocupações específicas. Descobrem que um grupo de eleitores está especialmente preocupado com a qualidade das escolas locais, enquanto outro grupo valoriza a segurança nas ruas. Com base nesses *insights*, o candidato envia mensagens altamente personalizadas: para o primeiro grupo, ele destaca seu plano específico para melhorar a educação, enquanto para o segundo grupo, ele enfatiza suas propostas para aumentar a segurança.

Assim, a diferença primordial entre a segmentação tradicional e a microssegmentação reside na personalização das mensagens. A microssegmentação considera as preocupações e os interesses de grupos específicos de eleitores, moldando a mensagem para atendê-los, enquanto a segmentação tradicional se baseia em categorias mais genéricas, que não abordam tais detalhes. Esse nível de personalização intensifica o impacto da mensagem, elevando significativamente a possibilidade de construir uma conexão genuína com o eleitor. Isso torna a comunicação mais eficaz e relevante, aumentando a probabilidade de conquistar seu apoio.

Outra vantagem oferecida pelo microdirecionamento político online se refere a otimização de custos e esforços para os candidatos. Enquanto métodos tradicionais, como a propaganda de porta em porta e comícios, exigem considerável investimento de tempo e recursos, o microdirecionamento possibilita que os candidatos atinjam eleitores de maneira mais ágil e econômica através de plataformas digitais. Essa estratégia resulta em uma significativa economia financeira, liberando os candidatos para focarem em outros aspectos da campanha (Dobber; Fathaigh; Borgesius, 2019).

A ascensão dessa técnica é um testemunho da crescente capacidade tecnológica que as campanhas políticas têm à sua disposição. Contudo, com tamanha capacidade, surge uma responsabilidade proporcionalmente elevada. O caso da Cambridge Analytica serve como um alerta sobre os perigos inerentes a esse poder. A referida empresa enfrentou acusações de uso indevido de dados de usuários do Facebook com o intuito de direcionar propaganda personalizada. Mediante a análise minuciosa dessas informações, a Cambridge Analytica foi capaz de categorizar eleitores em grupos específicos e elaborar perfis individuais detalhados.

Segundo Kaiser (2020), ex-executiva da *Cambridge*, a empresa possuía um *Big Data* de 2 mil a 5 mil pontos de dados individuais de cerca de 240 milhões de estadunidenses. Com o suporte de cientistas de dados e psicólogos, a empresa empregava a metodologia psicográfica

para categorizar os indivíduos. Assim, através da "modelagem de dados", que consistia na elaboração de modelos a partir das informações adquiridas, a *Cambridge Analytica* tinha a habilidade de antecipar tendências comportamentais e desenvolver mensagens altamente personalizadas.

A metodologia psicográfica envolvia a aplicação de testes de personalidade, criados pelos psicólogos da empresa, ao seu vasto banco de dados. Isso possibilitava uma análise aprofundada das nuances da personalidade dos votantes, identificando seus principais estímulos e motivações. Com essas informações, as equipes de criação desenvolviam mensagens direcionadas especificamente para esses tipos de personalidade, em uma estratégia denominada "*microtargeting* comportamental" (Kaiser, 2020).

A crescente compreensão e aplicação da psicometria em estratégias de marketing digital abriram novos horizontes para a publicidade. Apesar de existirem divergências quanto à eficácia dos métodos psicométricos, recentes estudos nas áreas de propaganda e sociologia computacional corroboraram a ideia de que é possível antecipar com precisão os perfis mentais dos indivíduos com base em suas atividades online. Pesquisas sobre a influência da microssegmentação na publicidade sugerem que o *microtargeting* comportamental pode ser empregado de maneira sigilosa para atrair até 40% mais cliques e induzir até 50% mais compras. As descobertas também reforçam que profissionais de marketing são capazes de atrair até 63% mais cliques e obter até 1.400% mais conversões em campanhas publicitárias no *Facebook*, caso combinem os produtos e as mensagens de marketing com as características de personalidade dos consumidores (Magrani, 2020).

Esta é a complexa e fascinante dinâmica que define a interação entre a psicometria, a internet e o marketing, revelando a influência da personalidade dos usuários nas estratégias de publicidade online. Essa fusão entre tecnologia e psicologia representa uma revolução no mundo do marketing, onde os anúncios não são mais generalizados, mas sim, feitos sob medida. Na proporção que mais estudos emergem neste campo, a eficácia e a aplicação dessas técnicas prometem ser ainda mais surpreendentes.

No caso da *Cambridge Analytica*, a empresa utilizou o modelo OCEAN, originário da psicologia comportamental e social, para desenvolver estratégias de microssegmentação. Com base nesse modelo, a empresa categorizava os indivíduos como "abertos a novas experiências" (O de "openness"), "metódico" (C de "conscientiousness"), "extrovertidos" (E de "extraversion"), "empático" (A de "agreeableness") ou "neuróticos" (N de "neuroticism"). Vale ressaltar que uma pessoa poderia se enquadrar em várias dessas definições. A partir dessa classificação, a empresa segmentava os indivíduos em 32 grupos principais, refinando, assim,

sua mensagem (Kaiser, 2020).

Esse avançado sistema de categorização, entretanto, só se tornou viável e mais prático no cenário digital atual. Em uma época anterior à revolução da internet e à expansão das redes sociais, a maior barreira para uma eficiente aplicação da psicometria residia na complexidade de coletar os dados necessários, dados esses que dependiam de questionários extensos e detalhados. Contudo, com o advento das plataformas online e a crescente participação dos usuários nas redes sociais, essa barreira foi superada. Na contemporaneidade, a psicometria se encontra em ampla utilização para diversos fins, incluindo campanhas eleitorais (Magrani, 2020).

Apesar da crescente popularidade do microdirecionamento, sua aplicação pode apresentar desafios e riscos para os indivíduos, o debate público e os partidos políticos. Para os indivíduos, emergem preocupações de privacidade, como a potencial exposição de dados pessoais, ilustrado pelo incidente envolvendo a *Cambridge Analytica*. Ademais, o mero conhecimento de que seus dados estão sendo coletados pode fazer com que as pessoas alterem comportamentos, temendo a constante observação. Há também o perigo de manipulação, com a propagação de desinformação e a influência deliberada na tomada de decisões por grupos específicos (Dobber; Fathaigh; Borgesius, 2019).

E quanto aos eleitores que não são alvo do microdirecionamento? Não teriam eles o mesmo direito à informação política que outros recebem? Seriam privados de mensagens específicas às quais seus concidadãos têm acesso? Isso não poderia criar um desequilíbrio informacional na sociedade? A crescente adoção dessa técnica tem gerado preocupações quanto à possível marginalização de certos grupos de eleitores. É importante destacar que, ao negligenciar determinados segmentos da população, os atores políticos podem inadvertidamente contribuir para uma sub-representação social (Dobber; Fathaigh; Borgesius, 2019).

Confrontado com esses dilemas, Bayer (2020) sugeriu medidas para remediar essa violação do direito à informação. Uma solução proposta por ele seria permitir que os cidadãos pesquisassem ativamente e coletassem anúncios direcionados em repositórios online. No entanto, essa solução pode ser limitada, uma vez que depende de atitudes e características individuais dos eleitores, deixando os mais vulneráveis em desvantagem.

No tocante ao debate público, o microdirecionamento político pode mascarar as verdadeiras intenções dos candidatos e levar a uma fragmentação do discurso, fazendo com que os indivíduos se concentrem majoritariamente em assuntos de seu interesse direto. Esse panorama pode dificultar a clareza sobre o compromisso de um representante eleito, uma vez

que diversas questões específicas ganham destaque durante as campanhas (Dobber; Fathaigh; Borgesius, 2019).

Segundo Bayer (2020), essa fragmentação do debate público restringe intencionalmente o alcance de certas informações, comprometendo a integridade do processo democrático. Isso resulta em divisões e interpretações distorcidas, tornando a discussão menos abrangente e enfraquecendo a democracia em sua essência.

No contexto dos partidos políticos, o microdirecionamento também apresenta desafios significativos, tanto em termos financeiros quanto na relação com intermediários digitais. Os custos associados a essa técnica favorecem agremiações com maiores recursos, ampliando a disparidade com as menores e restringindo a pluralidade de vozes. A crescente relação de dependência com plataformas digitais, repletas de dados e tecnologias sofisticadas, pode expor os partidos a vulnerabilidades (Dobber; Fathaigh; Borgesius, 2019).

Na corrida para se manterem relevantes no cenário atual, as agremiações partidárias veem-se cada vez mais entrelaçadas a esses gigantes da tecnologia. Essa interdependência sublinha a influência crescente desses intermediários na moldagem da opinião pública, atuando como canais de expressão, organização e diálogo político, sobretudo levando em conta o controle que possuem sobre os algoritmos que influenciam o ambiente digital.

Diante dessa realidade, ao distribuir anúncios online, as plataformas se tornaram atraentes não só para empresas, como também para campanhas eleitorais. Elas exibem propagandas com precisão, escala e velocidade sem precedentes, determinando quem as pode ver, bem como reproduzem padrões de desigualdade entre gênero, raça e idade. Além disso, definem seus próprios critérios para categorizar e classificar o conteúdo para manter os indivíduos engajados (Simons; Ghosh, 2020).

Em resposta à crescente pressão por maior transparência, plataformas digitais passaram por adaptações para atender às legislações locais, resultando em alterações em suas políticas de privacidade e normas para publicidade política. É importante destacar que grandes empresas, como Facebook, Google e Twitter (este último agora denominado X), tentaram se antever à essas regulamentações, criando seus próprios mecanismos de transparência para anúncios políticos, como é o caso do Código de Conduta sobre Desinformação na União Europeia. No entanto, essas ações foram criticadas por serem vistas como lenientes e vulneráveis a explorações por parte de atores maliciosos, conforme apontado por Crowe (2020).

No contexto pós-eleitoral europeu de 2019, a Comissão Europeia avaliou aludido Código e identificou várias insuficiências. As ações para ampliar a transparência se mostraram inconsistentes, apresentando variações entre as diferentes plataformas e Estados-Membros. A

despeito da revisão do Código em 2022, a Comissão já delineava, concomitantemente, uma proposta mais robusta e holística acerca da publicidade política: um Regulamento do Parlamento Europeu e do Conselho sobre a transparência e o direcionamento da propaganda política (European Parliament, 2023a).

Tal proposta visa abarcar a publicidade política tanto online quanto offline. O foco recai sobre a publicidade política patrocinada, excluindo anúncios de fontes oficiais sobre procedimentos eleitorais. Destaca-se que a regulamentação não se limita apenas aos períodos eleitorais, mas também se estende aos intervalos entre eles. A proposta introduz novos requisitos de transparência e proíbe técnicas invasivas de microssegmentação online. Além disso, ela complementa a Lei dos Serviços Digitais, estabelecendo requisitos específicos de clareza para publicidade política online (European Parliament, 2023a).

Há também um reforço nas normas sobre o tratamento de dados pessoais em publicidade política, especialmente proibindo técnicas de microssegmentação baseadas em dados sensíveis. A proposta define anúncios políticos de maneira abrangente, incluindo mensagens associadas a um ator político, exceto aquelas de caráter privado ou comercial. A definição de ator político é ampla, abrangendo uma variedade de entidades e indivíduos envolvidos em atividades políticas (European Parliament, 2023a).

O objetivo central da proposta é a padronização completa das regras de transparência para publicidade política, tanto online quanto offline. Caso aprovada, ela estabeleceria um padrão uniforme, impedindo que os Estados-Membros adotassem normas mais rígidas ou mais lenientes. Além disso, visa estabelecer padrões claros de transparência, incluindo identificação adequada, manutenção de registros, elaboração de relatórios e implementação de mecanismos de denúncia (European Parliament, 2023a).

Outro objetivo significativo é padronizar as regras de microssegmentação na publicidade política. A proposta considera a microssegmentação como uma ameaça à tomada de decisões políticas informadas dos cidadãos. O artigo 12 proíbe o uso dessa técnica quando envolve dados sensíveis, com algumas exceções. A Autoridade Europeia para a Proteção de Dados manifestou apoio, indicando que a proposta poderia ser ainda mais rigorosa em seus termos (European Parliament, 2023a).

A iniciativa também estabelece requisitos de transparência para as entidades que se utilizam dessas técnicas. Conforme o documento, essas entidades devem estabelecer políticas internas transparentes, conservar registros detalhados de sua aplicação e esclarecer sua metodologia. Anúncios que recorrem à microssegmentação devem incluir informações claras que permitam ao público compreender a lógica e os parâmetros utilizados (European

Parliament, 2023a).

Aprovada no Parlamento no dia 2 de fevereiro de 2023 com alterações, a proposta foi direcionada à comissão designada para as negociações subsequentes. Os negociadores do Parlamento pretendem chegar a um acordo sobre essas regras com os países da UE a tempo das eleições europeias de 2024 (European Parliament, 2023).

Para além dos desafios regulatórios, a microssegmentação política suscita preocupações relativas à representatividade, interpretação de dados e causalidade. Uma das principais inquietações é a possível desconexão entre as opiniões expressas nas redes sociais e a realidade concreta do mundo offline. Não se pode presumir que as preferências políticas expressas nas plataformas sejam espelhos fiéis das convicções do eleitorado em sua totalidade. A parcela da população que se mostra politicamente engajada nas redes não reflete, de forma automática, a diversidade e amplitude da sociedade como um todo, e a mera manifestação de uma opinião política em um ambiente virtual não equivale necessariamente a sua consolidação no mundo real (Dobber; Fathaigh; Borgesius, 2019).

As conclusões obtidas das redes sociais oferecem apenas uma perspectiva limitada das inclinações políticas de um indivíduo, e isso é válido somente quando o comportamento online de alguém corresponde às suas reais preferências políticas. É importante notar ainda que os usuários identificados online podem não ter direito de voto, o que poderia introduzir viés no processo de amostragem e potencialmente distorcer a eficácia da publicidade política (Papakyriakopoulos, 2018).

A complexidade em determinar uma conexão causal direta entre a microssegmentação e os desfechos eleitorais é amplamente debatida. Embora não existam evidências conclusivas que atestem sua eficácia, as campanhas políticas persistem em adotar essa estratégia, operando sob a presunção de que ela possa gerar resultados positivos (Dobber; Fathaigh; Borgesius, 2019).

No cerne da discussão sobre microssegmentação, está a inquietação quanto ao impacto dessas mensagens altamente personalizadas. A questão que emerge é: teria a microssegmentação, com o auxílio do aprendizado de máquina, o potencial de manipular eleitores por meio de publicidade política direcionada?

É importante salientar que a entrega de mensagens personalizadas não implica, por si só, em manipulação, uma vez que os indivíduos têm a liberdade de tomar suas próprias decisões de voto. Contudo, à medida que as pessoas voluntariamente divulgam mais sobre seus interesses e preferências na internet, os algoritmos podem aprimorar sua capacidade de interpretar esses dados pessoais (Papakyriakopoulos, 2018).

Essa realidade acende um alerta sobre o risco do microdirecionamento conduzir a uma "influência instantânea", onde o objetivo é induzir o indivíduo a agir conforme os desejos dos atores políticos. Tal preocupação se origina do fato de que, em cenários de entrega acelerada de mensagens, há uma tendência de as pessoas assimilarem as informações de forma mais impulsiva do que reflexiva. Isso pode estabelecer uma ligação direta entre a mensagem recebida e o candidato, potencializando a capacidade de moldar o comportamento do eleitor (Papakyriakopoulos, 2018).

Embora a construção bem-sucedida de um candidato dependa de múltiplos fatores – psicológicos, sociais e políticos –, é possível que a aplicação sistemática da microssegmentação possa influenciar a tomada de decisão. Uma abordagem proativa seria informar o eleitorado sobre essas técnicas, incentivando uma análise crítica das mensagens, cientes de sua natureza direcionada. A capacidade de discernir influências e manter a autonomia de pensamento é imprescindível para a integridade democrática (Papakyriakopoulos, 2018).

Para Bayer (2020), o perigo do microdirecionamento político ao processo democrático é tão significativo que, mesmo com uma probabilidade reduzida de manipulação, o risco global se torna intoleravelmente elevado. Historicamente, campanhas políticas sempre utilizaram estratégias diretas, como visitas e panfletagens. No entanto, a atual combinação de acesso a dados, análises sofisticadas e comunicação personalizada alterou o jogo. A transparência na segmentação de eleitores diminuiu, e isso tem implicações profundas para a democracia.

Portanto, ao optar pelo microdirecionamento como estratégia de campanha, os atores políticos têm a responsabilidade de aderir às normas legais vigentes, com ênfase aos regulamentos gerais de proteção de dados, adaptando-se também às dinâmicas do mercado e às diretrizes estabelecidas pelas plataformas online. Nesse cenário, harmonizar avanços tecnológicos com a preservação dos valores democráticos torna-se uma missão na política contemporânea.

Avançando na discussão, serão delineadas recomendações de boas práticas considerando as normativas de proteção de dados no Brasil e na União Europeia. Com o compromisso de manter uma conduta ética e respeitosa perante os direitos fundamentais e os princípios democráticos, estas orientações para o uso de dados pessoais em campanhas eleitorais não pretendem ser soluções finais, mas, sim, diretrizes para a elaboração de marcos regulatórios que contemplem, de forma ponderada, as nuances do universo digital.

4.3 Recomendações de boas práticas para campanhas eleitorais à luz dos Regulamentos de Proteção de Dados

A significativa adesão popular às redes sociais modificou consideravelmente as dinâmicas de comunicação e os fluxos de informação em muitos países. Notavelmente, essa nova configuração também impactou a propaganda eleitoral e a comunicação política, produzindo alguns efeitos.

Via de regra – e em primeiro lugar –, plataformas de mídia social, a exemplo do X (anteriormente conhecido como Twitter) e do Facebook, não são responsáveis pela produção do conteúdo que é "postado" em seu espaço. Em verdade, apresentam-se como intermediários digitais, proporcionando um ambiente de interação onde são os próprios usuários que desempenham o papel principal na criação e disseminação de conteúdo.

Nesse ínterim, esses usuários compartilham o que lhes interessa e distribuem informações que consideram importantes. Essas transformações, no horizonte das mídias, potencializaram o advento do que se intitula de estruturas de campanha em rede. Noutras palavras, nota-se um novo formato de campanhas políticas, sinalizado por dinâmicas abertas, descentralizadas e interativas, caso comparadas com as existentes anteriormente.

Pode-se dizer que os atores estão em rede, porquanto embora envolvidos com a campanha em níveis distintos de engajamento e de relacionamento, articulam-se em cooperação e em parceria com a candidatura e com seu entorno, atuando tanto de maneira espontânea, quanto simplesmente pelas máquinas oficiais de campanha.

Diante desse cenário, é imprescindível enfatizar o valor dos "componentes" dessa dinâmica – os dados, incluindo os pessoais. Eles não são apenas números ou informações isoladas. Eles representam as identidades, preferências e comportamentos dos eleitores. Assim, assegurar a integridade e confidencialidade desses dados não é apenas uma questão técnica, mas também ética. Além disso, proteger essas informações é um passo fundamental para preservar os direitos dos votantes, bem como para prevenir manipulações e interferências por parte de atores mal-intencionados.

Antes de examinar as melhores práticas para o tratamento de dados pessoais de eleitores no Brasil, convém mencionar as ações pioneiras da União Europeia no combate ao uso indevido de dados para fins político-eleitorais. Ao adotar orientações rigorosas nessa área, a União Europeia posicionou-se na vanguarda da proteção de dados pessoais. As iniciativas tomadas pelo bloco europeu podem, desse modo, servir como referência e oferecer *insights* valiosos para países que buscam fortalecer suas próprias normativas neste campo.

No período que antecedeu as eleições para o Parlamento Europeu em 2019, a Comissão Europeia enfatizou a importância de proteger o processo eleitoral contra interferências externas e interesses privados. A era digital emergente apresentava ameaças inéditas, incluindo desinformação em grande escala e uso inapropriado de dados pessoais. Outrossim, os recentes ataques cibernéticos à estrutura eleitoral revelaram a fragilidade das estruturas governamentais (Comissão Europeia, 2018a).

Em uma tentativa de reforçar a resiliência democrática, a Comissão propôs uma série de medidas estratégicas para proteger a integridade eleitoral. Primeiro, foi recomendada a instituição de redes nacionais de cooperação eleitoral. Essas redes, compostas por diversas autoridades estatais, teriam como principal objetivo identificar e mitigar rapidamente qualquer ameaça ao processo de votação. Em segundo lugar, enfatizou-se a necessidade de maior transparência em campanhas publicitárias online, exigindo uma clara identificação dos financiadores e dos critérios utilizados para segmentação. No domínio da cibersegurança, a Comissão delineou diretrizes para proteger sistemas de informação de potenciais ameaças cibernéticas (Comissão Europeia, 2018a).

Paralelamente, foram emitidas orientações para assegurar a aplicação correta e eficaz das leis de proteção de dados da União Europeia no contexto eleitoral, garantindo que os dados pessoais dos eleitores fossem manipulados de forma ética e segura. Além disso, sugeriu-se uma revisão legislativa que tornasse as normas de financiamento mais estritas e penalizadoras para partidos políticos e fundações que infringissem regras de proteção de dados com o objetivo de influenciar os resultados eleitorais. Finalmente, foi proposta a criação de um centro especializado de competências em cibersegurança, visando orientar e otimizar o financiamento e a pesquisa nesta área crítica, garantindo uma resposta proativa e robusta às crescentes ameaças cibernéticas (Comissão Europeia, 2018a).

Durante o encontro de líderes em Salzburgo, em setembro de 2018, a Comissão Europeia divulgou um documento orientativo destinado a esclarecer as responsabilidades dos intervenientes no contexto eleitoral, especialmente à luz dos eventos ligados ao caso *Cambridge Analytica*, reforçando a imperatividade da proteção de dados pessoais (Comissão Europeia, 2018b).

Conforme estipulado pela Comissão, os controladores – sejam partidos, candidatos, fundações ou plataformas digitais - deveriam adotar medidas de proteção de dados desde o início de suas atividades. Eles deveriam demonstrar total conformidade com o General Data Protection Regulation (GDPR), garantindo que os dados sejam tratados com base em princípios claros, como o consentimento do usuário, cumprimento de uma obrigação legal, realização de

uma tarefa de interesse público e interesses legítimos, desde que tais interesses não infrinjam os direitos fundamentais dos indivíduos envolvidos (Comissão Europeia, 2018b).

Sabe-se que a transparência é uma pedra angular do GDPR. O caso *da Cambridge Analytica* evidenciou a necessidade de combater práticas obscuras e de garantir que os indivíduos estejam plenamente informados sobre quem trata seus dados e para quais finalidades. Diante dessa situação, a Comissão estabeleceu que os controladores de dados esclarecessem a finalidade do tratamento, bem como quaisquer outras informações relevantes para garantir um tratamento justo e transparente (Comissão Europeia, 2018b).

Dentro do contexto eleitoral, técnicas de perfilagem e microdirecionamento, que buscam analisar e prever características individuais para enviar mensagens personalizadas, tornaram-se especialmente críticas. Com base nisso, a Comissão enfatizou a necessidade de clareza quanto ao uso dessas técnicas e destacou os potenciais riscos das decisões baseadas em automação. Ela apontou para os possíveis efeitos do microdirecionamento, como influenciar ou até mesmo dissuadir o ato de votar, sublinhando a importância de seguir rigorosamente os princípios do GDPR ao tratar tais dados (Comissão Europeia, 2018b).

Além disso, a Comissão Europeia ressaltou a primazia da segurança dos dados pessoais, especialmente considerando a magnitude dos conjuntos de dados e a presença potencial de dados sensíveis. O GDPR prescreve medidas robustas para assegurar a integridade desses dados e estipula prazos rigorosos para notificação de qualquer violação. A precisão é igualmente enfatizada, exigindo correções imediatas em caso de discrepâncias (Comissão Europeia, 2018b).

Por fim, a Comissão destacou a necessidade de uma avaliação prévia do impacto na proteção de dados, sobretudo quando há um risco elevado para os direitos dos indivíduos, bem como reforçou os direitos dos cidadãos no cenário eleitoral, garantindo acesso, retificação e objeção ao tratamento de seus dados, bem como a possibilidade de intervenção humana em decisões automatizadas. Essas orientações ressaltam o compromisso da Comissão em proteger os direitos individuais e assegurar a integridade do processo eleitoral na era digital (Comissão Europeia, 2018b).

De forma similar, o Comitê Europeu para a Proteção de Dados (CEPD) divulgou a Declaração nº 2/2019 sobre o uso de dados pessoais durante campanhas políticas. Esse documento destaca diversas considerações a serem observadas pelos partidos políticos ao utilizar dados pessoais em contextos eleitorais (CEPD, 2019).

O CEPD ressaltou que os dados pessoais que refletem opiniões políticas são vistos como uma categoria especial de dados sob o GDPR. Normalmente, o tratamento desses dados é

proibido, exceto quando há um consentimento claro, direto e bem informado do sujeito. O Comitê também apontou que dado pessoal divulgado publicamente ou compartilhado, mesmo que não revele opiniões políticas, ainda está protegido pela legislação da União Europeia. Isso inclui dados coletados em redes sociais, que devem ser tratados com transparência e legalidade (CEPD, 2019).

De acordo com o Comitê, é imperativo que as organizações sejam transparentes ao tratar dados pessoais, fornecendo informações aos indivíduos e demonstrando conformidade com os princípios do GDPR. Decisões tomadas de forma automatizada, como a criação de perfis para campanhas, têm suas limitações e, em sua maioria, necessitam do consentimento explícito do titular dos dados. Ademais, o Comitê sugeriu que os eleitores sejam esclarecidos sobre o motivo de receberem determinadas mensagens e quem está por trás delas. Em alguns países, há também requisitos de transparência sobre pagamentos para publicidade política (CEPD, 2019).

Nesse sentido, considerando os pontos abordados e a importância de aderir às normas de proteção de dados, particularmente em campanhas eleitorais, e com o objetivo de consolidar a confiança dos eleitores, garantir a integridade eleitoral e fortalecer a democracia, apresentamos, a seguir, recomendações de boas práticas aos atores envolvidos no processo eleitoral brasileiro.

Inicialmente, é necessário que sejam identificadas as figuras do controlador, do operador e do encarregado pela proteção de dados, estipulando claramente suas responsabilidades (Magrani, 2020). Ao fazer isso, assegura-se que os dados sejam manuseados em conformidade com a legislação, fortalecendo a confiança dos eleitores e reduzindo o risco de infrações.

Para ilustrar, imagine um cenário em que, durante uma eleição municipal, um partido político lança uma plataforma online para coletar opiniões dos cidadãos sobre temas locais. Esse partido contrata uma empresa especialista em desenvolvimento web e análise de dados. Nessa situação, o partido, que determina o que será coletado e como será utilizado, é o controlador dos dados. A empresa contratada, que trata esses dados seguindo as diretrizes do partido, atua como operadora. O representante no partido responsável por assegurar a conformidade da plataforma com a LGPD é o encarregado pela proteção de dados. Graças a essa clara atribuição de papéis, os cidadãos conseguem discernir quem está por trás do tratamento de seus dados e de que maneira. Isso os habilita a tomar decisões mais esclarecidas sobre o compartilhamento de suas informações e a exercer plenamente seus direitos, como os de acesso, correção e exclusão de seus dados, em linha com o previsto pela LGPD.

Outra etapa importante consiste no mapeamento dos dados, que envolve verificar todos os pontos de coleta e tratamento, determinar o período de retenção, identificar os meios de

armazenamento e reconhecer quem tem acesso a essas informações (Magrani, 2020). Esse mapeamento não só é fundamental para o gerenciamento e a proteção dos dados, mas também serve como um guia para as campanhas eleitorais.

Ao verificar todos os pontos de coleta, como formulários online, inscrições em eventos ou pesquisas, é possível ter uma visão clara de onde os dados estão sendo obtidos. Além disso, ao determinar o período de retenção, as organizações podem garantir que os dados não sejam mantidos por mais tempo do que o necessário, minimizando riscos e cumprindo com seu propósito inicial.

Identificar os meios de armazenamento é outra questão de destaque. No mundo digital, os dados podem ser armazenados em servidores locais, na nuvem, em dispositivos móveis ou até mesmo em mídias físicas, como pen drives ou discos rígidos externos. Cada método de armazenamento possui suas próprias vulnerabilidades e requer medidas de segurança específicas. Não menos importante, é saber quem tem acesso a esses dados. Mais do que simplesmente coletar e armazenar informações de forma segura, garantir que apenas pessoas devidamente autorizadas tenham acesso a elas reduz os riscos de vazamentos.

Outra orientação importante para as campanhas eleitorais refere-se à escolha das bases legais para o tratamento de dados. Os dados considerados sensíveis merecem especial atenção, sendo imprescindível que sua base seja claramente estabelecida, nos termos do art. 11 da LGPD. Caso haja dificuldade sobre qual base aplicar, a melhor prática é excluir os dados em questão (Magrani, 2020).

Para determinar a base legal mais apropriada e segura para o tratamento de dados, o controlador deve avaliar a finalidade, levando em consideração o contexto da situação. Assim, para garantir que o tratamento de dados pessoais seja lícito e legítimo, além de aderir aos princípios da LGPD, o agente responsável deve, antes de qualquer uso dos dados, verificar a presença de uma das bases estipuladas na lei (Brasil, 2018).

Atendendo ao princípio da necessidade ou minimização, recomenda-se que as campanhas eleitorais coletem apenas os dados estritamente necessários para atingir a finalidade proposta. Uma vez alcançado o objetivo da coleta, esses dados devem ser prontamente descartados, conforme estipulado nos arts. 15 e 16 da LGPD (Magrani, 2020).

Considere-se, por exemplo, um partido político que busca compreender as inquietações predominantes dos eleitores de uma certa área e, para tal, elabora um questionário online. Adotando o princípio da minimização, o questionário requer somente o CEP (para assegurar a localização do respondente na área alvo) e as respostas às indagações pertinentes. Mesmo que haja um interesse em coletar dados demográficos adicionais, como faixa etária ou gênero, o

partido opta por omiti-los, visto que não são essenciais para a pesquisa em questão. Uma vez concluída a análise e tomadas as decisões com base nas informações, a agremiação procede com a eliminação dos dados coletados. Tal prática não só se alinha com a LGPD, mas também solidifica a relação de confiança com os eleitores, evidenciando um comprometimento genuíno com a proteção de suas informações pessoais.

Outra importante recomendação é a de manter toda a documentação referente às bases legais devidamente arquivada. Os responsáveis pelo tratamento devem conservar um registro das operações, descrevendo as categorias de dados e seus titulares, a finalidade do tratamento, as medidas de segurança adotadas, os fluxos de dados externos, o prazo para descarte dos dados, sobretudo quando fundado no legítimo interesse, para o caso de uma eventual auditoria (art. 37 da LGPD) (Magrani, 2020).

Ilustrando essa prática, considere uma campanha política que, visando uma conexão mais próxima com o eleitorado, desenvolve um aplicativo. No ato de inscrição, os eleitores inserem dados como nome, idade, localização e inclinações políticas. Consciente das responsabilidades previstas na LGPD, a campanha mantém um registro rigoroso de todas essas atividades. Esse registro inclui não apenas os dados coletados, mas também informações detalhadas sobre como esses dados são usados, quem tem acesso a eles, por quanto tempo são retidos e quais medidas de segurança são implementadas para protegê-los. Além disso, o registro documenta as bases legais que justificam a coleta e o tratamento desses dados, seja o consentimento explícito do eleitor, o cumprimento de uma obrigação legal ou o legítimo interesse da campanha, e está sujeito à fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD), se necessário.

Na hipótese de o partido ou o candidato já possuir dados de eleitores colhidos antes da vigência da LGPD, a recomendação é que se obtenha um novo consentimento do titular desses dados. Recomenda-se também estabelecer uma política de privacidade clara e transparente, que detalhe como os dados são gerenciados e informe os direitos dos titulares sobre esses dados (Magrani, 2020).

Imagine um partido que tenha uma longa história em uma determinada cidade e, ao longo dos anos, coletou uma vasta quantidade de dados dos eleitores, incluindo nomes, endereços, números de telefone e até mesmo preferências políticas anteriores. Esses dados foram coletados em diferentes campanhas, eventos e inscrições antes da vigência da LGPD. Com a nova legislação em vigor, o partido reconhece a necessidade de regularizar essa situação. Em vez de usar os dados diretamente para a próxima campanha, o partido decide lançar uma campanha de reengajamento. Ele envia comunicações (por exemplo, e-mails ou mensagens

SMS) para todos os eleitores em sua base de dados, explicando as mudanças na legislação e solicitando um novo consentimento para manter a comunicação e usar seus dados para fins eleitorais. Na mesma comunicação, o partido apresenta sua nova política de privacidade, que foi elaborada em conformidade com a LGPD. Essa política detalha como os dados dos eleitores são usados, armazenados e protegidos, e também esclarece os direitos dos titulares dos dados e como podem exercê-los.

É de suma importância que as campanhas eleitorais adotem uma postura transparente e proativa ao lidar com os dados dos titulares. Sempre que solicitado, e especialmente no momento de buscar o consentimento, as campanhas devem fornecer informações claras e detalhadas sobre como os dados pessoais serão tratados (Magrani, 2020).

De acordo com o artigo 9º da LGPD, os responsáveis pelo tratamento devem garantir que as informações sobre o processo e a duração do tratamento, assim como a identificação do controlador, sejam acessíveis e de fácil compreensão. Já o artigo 18 estabelece os direitos do titular, incluindo a confirmação da existência de tratamento, acesso aos dados, correção de dados incompletos, anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos, entre outros. Desse modo, as campanhas devem estar preparadas para atender a essas solicitações, garantindo que os titulares dos dados estejam sempre informados e empoderados em relação às suas informações pessoais.

Considere a situação em que uma candidata à prefeitura de uma cidade lança um site para coletar sugestões dos cidadãos sobre melhorias urbanas. Durante o processo de inscrição no site, os usuários são convidados a fornecer dados como nome, e-mail e bairro. Antes de prosseguir, uma janela *pop-up* surge, detalhando quais dados serão coletados, a finalidade da coleta, o período de retenção e como os usuários podem gerenciar seus dados. Além disso, um *link* direciona para a política de privacidade completa. Esse procedimento garante que os usuários estejam bem informados e possam decidir conscientemente sobre o compartilhamento de suas informações.

Recomenda-se que as campanhas eleitorais ofereçam um meio de comunicação para que os titulares dos dados possam solicitar acesso às suas informações (Magrani, 2020). Como prática exemplar, uma campanha poderia incluir em seu site uma aba denominada “Acesso aos seus dados”. Nesse espaço, os eleitores teriam à disposição um formulário prático para inserir dados básicos e requisitar informações sobre o que a campanha detém a seu respeito. Além disso, o site poderia listar o nome e o contato do encarregado pelo gerenciamento dos dados, garantindo que os eleitores saibam a quem se dirigir com questões específicas ou preocupações relacionadas à sua privacidade.

É aconselhável assegurar que, quando a base jurídica empregada for o consentimento, este seja obtido sob condições adequadas. Tal prática demanda uma estratégia multidisciplinar, envolvendo desde a área Jurídica até a Tecnologia da Informação, e inclusive o Design, para garantir que o consentimento seja específico, informado, concedido de maneira livre e inequívoca (Magrani, 2020).

Durante a navegação em sites e plataformas digitais, é comum que os usuários se deparem com pedidos para coleta de cookies. No ato de solicitação de permissão, deve-se possibilitar que o usuário selecione as categorias de cookies que deseja ativar, esclarecendo quais são necessários para o funcionamento adequado do site (Magrani, 2020).

Recomenda-se também que, ao trabalhar com um operador de dados, se estabeleça um contrato claro e detalhado. Esse contrato deve definir os padrões de segurança a serem seguidos, bem como as responsabilidades do operador. Tal documento serve como um guia para a gestão adequada das informações pessoais, estabelecendo não apenas as expectativas e obrigações das partes, mas também reforçando a importância de medidas rigorosas para prevenir acessos indevidos, perdas ou vazamentos de dados. Ao fazer isso, cria-se um ambiente de confiança e transparência entre os envolvidos (Magrani, 2020).

Outra orientação importante é assegurar que os provedores tratem os dados com a devida segurança e que essas informações estejam em servidores localizados em territórios que atendam aos regulamentos de proteção de dados (Magrani, 2020). Por exemplo, durante as eleições presidenciais, muitos partidos recorrem a plataformas digitais para conectar-se com seus eleitores. Os dirigentes dessas legendas precisam assegurar que tais plataformas protejam adequadamente os dados dos votantes e que essas informações estejam hospedadas em áreas que respeitem as normativas de proteção de dados.

Em caso de incidentes de segurança que possam acarretar riscos ou danos relevantes aos titulares dos dados, a LGPD, no art. 48, estabelece a obrigatoriedade de notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos indivíduos impactados (Magrani, 2020). Essa medida visa garantir transparência e permitir que medidas corretivas sejam tomadas rapidamente. A comunicação deve ser feita em um prazo razoável, especificado pela ANPD, e deve conter informações sobre a natureza dos dados afetados, os riscos relacionados ao incidente, as medidas que foram ou serão adotadas para contornar a situação e os contatos para mais informações. Essa prática não apenas cumpre com a legislação, mas também reforça a confiança dos titulares dos dados, mostrando comprometimento e responsabilidade por parte das campanhas que tratam tais informações.

Toda campanha eleitoral deve implementar medidas de segurança capazes de proteger

os dados pessoais, tais como política de senha de segurança obrigatória, política de segurança interna, anonimização, autenticação multifatorial, criptografia, entre outros (Magrani, 2020). Em um cenário político, onde a confiança é fundamental, a proteção adequada dos dados pode influenciar positivamente a percepção do público em relação a um candidato ou partido. Ademais, a adoção dessas práticas reduz o risco de vazamentos ou uso indevido de informações, que podem ter consequências legais e reputacionais significativas. Por exemplo, uma iniciativa eleitoral que utiliza uma plataforma online para coletar apoio pode ser alvo de ataques cibernéticos. Implementando autenticação multifatorial e criptografia, essa plataforma pode se proteger melhor contra acessos não autorizados.

A elaboração de um relatório de impacto à proteção de dados pessoais é uma prática recomendada, especialmente quando se trata de operações de tratamento de dados que possam gerar riscos à liberdade e aos direitos fundamentais dos titulares. Esse relatório, muitas vezes referido como "Relatório de Impacto à Proteção de Dados" (RIPD), é uma ferramenta de avaliação que permite identificar e minimizar os riscos associados ao tratamento de dados pessoais.

No contexto de campanhas eleitorais, onde grandes volumes de dados sensíveis podem ser coletados e processados, o relatório de impacto se torna ainda mais relevante. Ele deve detalhar as operações de tratamento de dados realizadas, os riscos associados, as medidas de mitigação adotadas e a justificativa para a realização dessas operações, considerando a necessidade e a proporcionalidade.

Além de ser uma ferramenta de gestão de riscos, o relatório de impacto também serve como um documento de responsabilização. Ele demonstra o compromisso da campanha em proteger os dados dos eleitores e em cumprir com as obrigações legais. Em caso de auditorias ou investigações por parte de autoridades reguladoras, como a Autoridade Nacional de Proteção de Dados (ANPD), o relatório pode ser uma evidência valiosa de que a campanha adotou medidas proativas para garantir a conformidade com a LGPD e outras normativas aplicáveis.

Por fim, cumpre pontuar que os processos de tratamento de dados pessoais devem ser constantemente monitorados e revisados para se assegurar a adequação e o êxito da campanha. Em um cenário onde a informação é poder, assegurar a integridade dos dados é também uma maneira de proteger a soberania do voto, um dos pilares da democracia.

A tarefa de persuasão dos cidadãos é um fator elementar do processo eleitoral e do êxito de uma candidatura (embora não seja elemento exclusivo, evidentemente). Com orçamentos restritos, campanhas político-eleitorais necessitam aprimorar suas estratégias de acesso e de convencimento. Assim, não representa novidade que os dados pessoais podem contribuir nessa

tarefa. Contudo, a escala atual de relevância dada a esse "ativo" é muito peculiar. Primeiro, levando em consideração o vasto volume de dados produzidos em intensa velocidade nas redes sociais. Segundo, esse cenário está inserido em um movimento histórico de crescimento do poder computacional e dos métodos de análise desse "mar" de dados.

A controvérsia da *Cambridge Analytica* retratou a relevância do combate à falta de transparência e de informação adequada à população. Não se pode admitir que o que aconteceu com essa consultoria política se repita. Mesmo que seja imensurável em que medida a referida companhia e outros esforços similares tiveram êxito em influenciar as eleições, o que resta incontestável é que o seu objetivo era contornar o livre exercício da democracia. Eles buscavam *hackear* os eleitores. A finalidade não era disseminar informações verdadeiras e levantar argumentos pertinentes para justificar por que o eleitorado deveria votar em determinado candidato. Ao contrário, eles apelaram para os sentimentos mais primitivos dos indivíduos, se afastando da verdade.

Em uma época de conectividade constante, em que informações, conceitos e convicções são disseminados de maneira imediata e indiscriminada, opiniões podem ser afetadas por filtros digitais, e o ambiente público se conecta inexoravelmente às inovações no campo da informação e comunicação. Disfunções no sistema, decorrentes de equívocos ou de uma estrutura inerentemente falha, podem comprometer a capacidade das pessoas de alcançar consensos e estabelecer acordos de maneira harmoniosa e equilibrada, como ilustrado recentemente pelas interferências em processos eleitorais ao redor do mundo.

Para aqueles que lidam com dados, especialmente partidos políticos e candidatos, cumprir rigorosamente as normas não é somente um dever jurídico, mas também um critério fundamental para se posicionar perante a sociedade como um indivíduo ético, merecedor de respeito, confiança e votos. Essa afirmação ganha ainda mais peso considerando os episódios recentes mencionados anteriormente, em que técnicas de tratamento de dados foram empregadas em campanhas eleitorais, trazendo o assunto à discussão e intensificando a vigilância dos eleitores.

Desconsiderar a privacidade, o direito à proteção de dados e o direito à autodeterminação informacional das pessoas torna-se cada vez mais inaceitável no âmbito do marketing político, especialmente à medida que cresce a conscientização sobre essas problemáticas. Candidatos e partidos políticos devem zelar pela forma como manuseiam dados em suas campanhas ao longo dos pleitos eleitorais, buscando adotar as melhores práticas vigentes, não apenas em benefício próprio, mas também em prol dos titulares de dados e da sociedade em geral.

5 CONCLUSÃO

Ao longo desta dissertação, adentrou-se na complexa malha que une o avanço tecnológico, a coleta e tratamento de dados pessoais, e sua influência nas campanhas eleitorais. A era digital trouxe consigo uma série de desafios e oportunidades para a sociedade contemporânea, transformando dados pessoais em *commodities* valiosas. Esses dados apresentam uma dualidade notável: por um lado, possuem uma dimensão existencial, representando a identidade e a privacidade de um indivíduo; por outro, possuem uma dimensão funcional, sendo empregados, por empresas e governos, para uma variedade de fins, desde comerciais até estratégicos.

Com a digitalização crescente da sociedade, a relevância dos dados pessoais tornou-se mais evidente do que nunca. A habilidade dos algoritmos de criar perfis detalhados e direcionar conteúdo personalizado para cada usuário tem revolucionado campos como marketing e publicidade. Contudo, essa mesma capacidade também abre caminho para riscos significativos, como a propagação de desinformação e a manipulação de opiniões, ameaçando o cerne da democracia, particularmente em períodos eleitorais.

Nesse contexto, a intersecção entre tecnologia, dados pessoais e democracia torna-se um campo fértil para investigações e discussões. A dinâmica atual mostra que, enquanto a tecnologia oferece ferramentas poderosas para aprimorar a comunicação e a participação cidadã, ela também apresenta riscos significativos à democracia.

O objetivo central deste estudo é investigar como as salvaguardas estabelecidas pelos regulamentos gerais de proteção de dados pessoais, especialmente a Lei Geral de Proteção de Dados (LGPD) no Brasil, influenciam o fortalecimento do Estado Democrático de Direito. Além disso, busca-se entender de que forma essas normativas podem promover um diálogo construtivo com os princípios do Direito Eleitoral.

Conforme evidenciado, as normativas de proteção de dados são de suma importância na defesa dos direitos dos cidadãos. Ao assegurar esses direitos, contribuem significativamente para a manutenção de um ambiente democrático onde a privacidade é respeitada e a manipulação indevida de dados é evitada. Essa proteção é essencial para assegurar que as decisões eleitorais sejam tomadas de maneira livre e justa, sem influências indevidas baseadas no uso impróprio de dados pessoais.

Além disso, é importante destacar a inter-relação direta entre a proteção de dados pessoais e o Direito Eleitoral, especialmente no que se refere ao uso de dados em campanhas eleitorais e na microssegmentação política. As práticas de coleta e uso de dados devem ser

transparentes e éticas para assegurar que a tecnologia seja empregada como uma ferramenta de fortalecimento da democracia, e não como um meio para subvertê-la. A legislação de proteção de dados pode oferecer um marco regulatório para garantir que as campanhas eleitorais sejam conduzidas de maneira justa e que a privacidade dos eleitores seja protegida, prevenindo assim a manipulação e a disseminação de desinformação.

A Lei Geral de Proteção de Dados Pessoais (LGPD) representa um avanço significativo na proteção dos direitos dos titulares de dados no Brasil. No entanto, sua efetividade em contextos eleitorais ainda é uma questão em aberto. A microssegmentação política, por exemplo, permite a criação de mensagens altamente personalizadas para eleitores, o que pode ser benéfico para a comunicação política, mas também pode ser usado para manipular e influenciar indevidamente as opiniões.

O conceito de "democracia hackeada" ilustra vividamente o desafio contemporâneo, revelando a vulnerabilidade do sistema democrático. No entanto, a partir das análises realizadas, observou-se que os regulamentos gerais de proteção de dados pessoais possuem o potencial de equilibrar essa balança, colocando em destaque os direitos dos cidadãos em contraponto aos interesses comerciais e políticos.

Com base nessa compreensão, este trabalho propõe recomendações de boas práticas baseadas nas leis de proteção de dados do Brasil e da União Europeia. Essas recomendações, focadas no uso de dados pessoais em campanhas eleitorais, são apresentadas não como soluções definitivas, mas como alicerces para o desenvolvimento de marcos regulatórios que harmonizem as complexidades do ambiente digital. Elas visam orientar a formulação de regulamentações que enfrentem eficientemente os desafios do universo digital, com especial atenção ao cenário eleitoral, reconhecendo a importância da proteção de dados pessoais para a integridade da democracia.

Ademais, procurou-se contribuir para a reflexão sobre os caminhos que a democracia deve trilhar em um mundo hiperconectado. A sociedade precisa estar ciente de seus direitos e exigir sua proteção. A academia, os setores governamentais, as organizações civis e os partidos políticos precisam colaborar na busca por soluções que garantam a integridade do sistema democrático.

É imperativo ressaltar a urgência de um diálogo mais amplo e integrado entre os setores de proteção de dados e as instituições. Este diálogo é importante para garantir a segurança dos dados, adaptando-se às novas tecnologias e regulamentações, e promovendo uma compreensão mútua entre os diferentes *stakeholders*.

Os partidos políticos, ao se engajarem ativamente na proteção de dados e na promoção da privacidade, podem contribuir significativamente para a confiança do público no processo democrático. Eles devem estar na vanguarda da implementação de políticas de proteção de dados, garantindo que suas estratégias de campanha e comunicação estejam alinhadas com as normativas vigentes, bem como da promoção da conscientização sobre a importância da proteção de dados entre seus membros e eleitores, incentivando uma cultura de respeito à privacidade e segurança da informação.

A responsabilidade não recai apenas sobre essas entidades, mas sobre todos os cidadãos. Cada indivíduo, ao exercer seus direitos digitais e ao se informar sobre as práticas de coleta e uso de seus dados, contribui para a construção de uma democracia mais resiliente e robusta. É um esforço coletivo que requer a participação ativa de todos para garantir um futuro seguro e protegido.

Outrossim, é fundamental que haja uma cooperação internacional entre as Autoridades Nacionais de Proteção de Dados para abordar esses desafios. A natureza global da internet e das plataformas digitais significa que as campanhas de desinformação e os ataques à privacidade podem originar-se em qualquer lugar e afetar eleições e democracias em todo o mundo. Portanto, faz-se primordial que os países compartilhem melhores práticas, estratégias e soluções para proteger a integridade do processo democrático.

Diante disso, a conclusão que se extrai deste estudo não é de um fim, mas sim de um começo. A temática da proteção de dados e sua relação com o direito eleitoral demanda uma contínua revisão e atualização. O cenário tecnológico está em constante mudança, e as normativas devem acompanhar esse ritmo para assegurar a preservação dos valores democráticos.

Que esta dissertação sirva, então, como um estímulo para ações, pesquisas e debates futuros, reforçando a imperiosa necessidade de proteger nossa democracia diante dos avanços e desafios do mundo digital. A jornada é longa e complexa, mas, como demonstrado, não se carece de recursos e saberes necessários para o seu enfrentamento.

Por fim, ciente das limitações e da amplitude do tema, este trabalho espera ter semeado mais perguntas do que respostas, instigando futuras pesquisas e reflexões. Que, à luz da proteção de dados, a democracia possa ser fortalecida, não minada, e que a era digital seja sinônimo de uma sociedade mais justa, informada e participativa.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ANPD. **Guia orientativo**: aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral [recurso eletrônico]. – Dados eletrônicos (65 páginas). Brasília: Tribunal Superior Eleitoral, 2021.

ARISTOTLE. 2023. **Dados Políticos.** Disponível em https://www.aristotle.com/data/political-data/ . Acesso em: 23 set. 2023.

AULETTA, Tommaso Amadeo. **Riservatezza e tutela della personalità**. Milano: Giuffrè, 1978.

BARIANI JR., Percival José; MARTINS, Victor Silveira. A autoridade nacional de proteção de dados: um organismo ainda a ser desenvolvido. *In*: MARINHO, Gustavo; VALIM, Rafael; WARDE, Walfrido; SIMÃO, Valdir. **Aspectos relevantes da Lei Geral de Proteção de Dados**. São Paulo. Editora Contracorrente, 2021.

BARROSO, Luís Roberto. **Interpretação e aplicação da Constituição**: fundamentos de uma dogmática constitucional transformadora. 7. ed. São Paulo: Saraiva, 2012.

BAYER, J. Duplo dano aos eleitores: microdirecionamento baseado em dados e discurso público democrático. **Revisão da Política da Internet**, 9(1), 2020. Disponível em: https://doi.org/10.14763/2020.1.1460. Acesso em: 23 set. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BLACKSTONE, William. **Commentaries on the Laws of England**. Oxford: Clarendon Press, 1765.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Campus, 1992.

BOBBIO, Norberto. **O futuro da democracia**: uma defesa das regras do jogo. 6. ed. Paz e Terra, 1986.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 10 out. 2020.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 10 mai. 2022.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 02 mai. 2022.

BRASIL. **Exposição de motivos da medida provisória n. 954, de 17 de abril de 2020**. Brasília: Presidência da República, 2020b. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Exm/Exm-MP-954-20.pdf. Acesso em: 03 abr. 2023.

BRASIL. **Lei Complementar nº 166, de 8 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm. Acesso em: 06 mai. 2022.

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?msclkid=ccc0d7c4d08f11ecadf4116c541dd294. Acesso em: 02 maio 2022.

BRASIL. **Lei nº 9.096, de 19 de setembro de 1995.** Dispõe sobre partidos políticos, regulamenta os arts. 17 e 14, § 3º, inciso V, da Constituição Federal. Diário Oficial da União, Brasília, DF, 20 set. 1995. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9096.htm. Acesso em: 20 ago. 2023.

BRASIL. **Lei nº 9.504, de 30 de setembro de 1997.** Dispõe sobre normas para as eleições. Diário Oficial da União, Brasília, DF, 1º de outubro de 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 20 abr. 2023.

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm?msclkid=d32333c5d08b11ec8d348f6fac47360e. Acesso em: 02 maio 2022.

BRASIL. **Lei nº 12.034, de 29 de setembro de 2009.** Altera as Leis nos 9.096, de 19 de setembro de 1995 - Lei dos Partidos Políticos, 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, e 4.737, de 15 de julho de 1965 - Código Eleitoral. Diário Oficial da União, Brasília, DF, 30 set. 2009. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12034.htm. Acesso em: 05 set. 2023.

BRASIL. **Lei n. 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm?msclkid=10be0c50d09011ec9024389b1a0da6bb. Acesso em: 03 maio. 2022.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm?msclkid=64a7c5d6d09011ecbe45c53964477825.Acesso em: 03 maio 2022.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm?msclkid=ab0502c9d09011ecb55d657603e53c33.Acesso em: 03 maio 2022.

BRASIL. **Lei nº 13.488, de 6 de outubro de 2017**. Altera as Leis nº 9.504, de 30 de setembro de 1997 (Lei das Eleições), 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 (Código Eleitoral), e revoga dispositivos da Lei nº 13.165, de 29 de setembro de 2015 (Minirreforma Eleitoral de 2015), com o fim de promover reforma no ordenamento político-eleitoral. Diário Oficial da União, Brasília, DF, 6 out. 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13488.htm. Acesso em: 04 set. 2023.

BRASIL. **Lei nº 13.709, de 14 agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 maio. 2022.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Diário Oficial da União, Brasília, DF, 9 jul. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 18 ago. 2023.

BRASIL. **Lei nº 14.460, de 6 de julho de 2022**. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Diário Oficial da União, Brasília, DF, 7 jul. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14460.htm. Acesso em: 16 ago. 2023.

BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2190283#:~:text=MPV%20869%2F2018%20Inteiro%20teor,Medida%20Provisória&text=Altera%20a%20Lei%20nº%2013.709,Dados%2C%20e%20dá%20outras%20providências. Acesso em: 25 ago. 2023.

BRASIL. **Medida Provisória nº 1.124, de 31 de janeiro de 2022.** Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade

Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/153611. Acesso em: 15 ago. 2023.

BRASIL. **Proposta de Emenda à Constituição n° 17, de 2019**. Proteção de dados pessoais. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 05 mai. 2022.

BRASIL. Supremo Tribunal Federal. **ADI 4650/DF.** Tribunal Pleno. Rel. Min. Luiz Fux. Data de Julgamento: 17/09/2015. Data de Publicação: 24/02/2016. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/864003307. Acesso em: 04 set. 2023.

BRASIL. Supremo Tribunal Federal. **ADI 6.387.** Rel. Min. Rosa Weber. Brasília, DF, 06 de maio de 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 07 jan. 2021.

BRASIL. Supremo Tribunal Federal. **ADI 6390/DF**. Tribunal Pleno. Rel. Min. Rosa Weber. Data de Julgamento: 07/05/2020. Data de Publicação: 12/11/2020.

BRASIL. Supremo Tribunal Federal. **ADI 6.388 MC-Ref.** Distrito Federal. Relatora: Ministra Rosa Weber. Plenário. Data de Julgamento: 07/05/2020.

BRASIL. Tribunal Superior Eleitoral (TSE) e Autoridade Nacional de Proteção de Dados (ANPD). **Acordo de Cooperação Técnica nº 4/2021.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/TSEANPDacordocooperacaotecnica.pdf Acesso em: 16 ago. de 2023.

BRASIL. Tribunal Superior Eleitoral. **Guia Orientativo Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral.** Brasília TSE: 2021.

BRASIL. Tribunal Superior Eleitoral. **Processo Administrativo nº 0600448-51.2019.6.00.0000**. Relator Ministro Og Fernandes, [s.d.].

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 22.718, de 28 de fevereiro de 2008.** Dispõe sobre a propaganda eleitoral e as condutas vedadas aos agentes públicos em campanha eleitoral (eleições de 2008). Diário de Justiça Eletrônico, Brasília, DF, 3 mar. 2008. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2008/5. Acesso em: 05 ago. 2023.

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. Diário de Justiça Eletrônico, Brasília, DF, 20 dez. 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 04 set. 2023.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.671, de 14 de dezembro de 2021.** Altera a Resolução-TSE nº 23.610, de 18 de dezembro de 2019, que dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral.

Diário de Justiça Eletrônico, Brasília, DF, 16 dez. 2021. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-671-de-14-de-dezembro-de-2021. Acesso em: 04 set. 2023.

BRITO CRUZ, Francisco (coord.); MASSARO, Heloisa; OLIVA, Thiago; BORGES, Ester. **Internet e eleições no Brasil**: diagnósticos e recomendações. InternetLab, São Paulo, 2019.

CATALIST. **Dynamic National Database.** Disponível em: <https://catalist.us/data/>. Acesso em: 04 out. 2023.

COMISSÃO EUROPEIA. **Estado da União 2018:** A Comissão Europeia propõe medidas destinadas a garantir eleições europeias livres e justas. 2018a. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681. Acesso em: 06 out. 2022.

COMISSÃO EUROPEIA. **Orientação da Comissão sobre a aplicação da legislação de proteção de dados da União no contexto eleitoral:** Uma contribuição da Comissão Europeia para o encontro dos líderes em Salzburgo. 2018b. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/66295074-b65c-11e8-99ee-01aa75ed71a1/language-en. Acesso em: 17 mar. 2021.

COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS. **Declaração 2/2019 sobre o uso de dados pessoais no decurso de campanhas políticas**. 2019. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political-campaigns_pt . Acesso em: 07 maio 2023.

CORDEIRO, António Menezes. **Tratado de direito civil português**. 2. ed. Coimbra: Almedina, 2007.

COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981**. Disponível em: https://rm.coe.int/1680078b37. Acesso em: 12 abr. 2023.

CROWE, Pascal. **Imprints**: Who's Responsible? ORG: Open Rights Group, [S.I] 31 mar. 2020. Disponível em: https://www.openrightsgroup.org/blog/imprints-whos-responsible/. Acesso em: 12 mai. 2022.

DAHL, Robert A. **Sobre a Democracia**. Tradução de Beatriz Sidou. Brasília: Universidade de Brasília. 2001.

DEMARTINI, Felipe. **Dados pessoais de brasileiros estão entre os mais baratos do mundo no cibercrime.** 2022. Disponível em: https://canaltech.com.br/seguranca/dados-pessoais-de-brasileiros-estao-entre-os-mais-baratos-do-mundo-no-cibercrime-218546/. Acesso em: 05 maio 2023.

DOBBER, Tom; FATHAIGH, Ronan Ó.; BORGESIUS, Frederik J. Zuiderveen. The regulation of online political micro-targeting in Europe. **Internet Policy Review**, vol. 8, iss. 4, dez. 2019. Disponível em: https://doi.org/10.14763/2019.4.1440 . Acesso em: 12 mai. 2022.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**: teoria geral do direito civil. 25. ed. São Paulo: Saraiva, 2007.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

EUROPEAN PARLIAMENT. **MEPs vote for tougher rules on political advertising**. 2023. Disponível em: https://www.europarl.europa.eu/news/pt/press-room/20230130IPR70208/eurodeputados-a-favor-de-regras-mais-rigorosas-em-materia-de-propaganda-politica . Acesso em: 04 out. 2023.

EUROPEAN PARLIAMENT. **Towards new rules on transparency and targeting of political advertising.** 2023a. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733592/EPRS_BRI(2022)733592_EN.pdf. Acesso em: 04 out. 2023.

FRAUDE na cota de gênero do PL deve cassar todos os deputados estaduais do partido no Ceará; entenda. **Estadão**, 16 maio 2023. Disponível em: https://www.estadao.com.br/politica/fraude-na-cota-de-genero-do-pl-deve-cassar-todos-os-deputados-estaduais-do-partido-no-ceara-entenda/. Acesso em: 06 out 2023.

GHEDIN, Rodrigo. Discador e mensagens, apps básicos do android enviam dados ao google sem consentimento dos usuários. **Núcleo**, 23 mar. 2022. Disponível em: https://nucleo.jor.br/curtas/2022-03-23-discador-mensagens-android-google-privacidade/. Acesso em: 05 maio 2022.

GHEDIN, Rodrigo. França multa Apple em € 8 milhões. **Núcleo**, 5 jan. 2023. Disponível em: https://nucleo.jor.br/curtas/2023-01-05-franca-multa-apple-8-milhoes/. Acesso em: 28 jun. 2023.

HACKERS vendem 8 milhões de números ativos de WhatsApp no Brasil. Convergência Digital, 12 dez. 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Hackers-vendem-8-milhoes-de-numeros-ativos-de-WhatsApp-no-Brasil-62136.html?UserActiveTemplate=site. Acesso em: 28 jun. 2023.

KAISER, Brittany. **Manipulados**: Como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque. 1. ed. Rio de Janeiro: Harper Collins, 2020.

KLEE, Antonia Espíndola Longoni; MARTINS, Guilherme Magalhães. **A privacidade, a proteção de dados e dos registros pessoais e a liberdade de expressão:** algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965/2014). *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Coord.). **Direito e Internet III**: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo: Quartier Latin. 2014.

LAFER, Celso. **A reconstrução dos direitos humanos**: um diálogo com o Pensamento de Hanna Arendt. São Paulo: Companhia das Letras, 1988.

LIMA NETO, Nelson. Eleitor processa Malafaia após receber carta em que o pastor pede votos para Bolsonaro, Castro e o irmão. **O Globo**, 27 set. 2022. Disponível em:

https://oglobo.globo.com/blogs/ancelmo-gois/post/2022/09/eleitor-processa-malafaia-apos-receber-carta-em-que-o-pastor-pede-votos-para-bolsonaro-castro-e-o-irmao.ghtml. Acesso em: 02 abr. 2023.

LINDON, Raymond. **Une création prétorienne**: Les droits de la personnalité. Paris: Dalloz, 1974.

MACHADO, Raquel Cavalcanti Ramos; FERREIRA, Desirée Cavalcante. Limites à intimidade e responsabilidade nos espaços públicos digitais: análise da possibilidade de bloqueio de contas de usuários por agentes públicos. **Interesse Público – IP**, Belo Horizonte, ano 23, n. 130, p. 129-152, nov./dez. 2021.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MAGRANI, Eduardo. **Hacheando o Eleitorado** - sobre o uso de dados pessoais em campanhas eleitorais**.** Berlin: Konrad-Adenauer-Stiftung, 2020.

MARQUES JÚNIOR, William Paiva. Obstáculos impostos à efetividade do direito personalíssimo à privacidade na Era do Big Data: uma problemática da sociedade contemporânea. In: Larissa Maria de Moraes Leal; Roberto, Senise Lisboa. (Org.). Direito Civil Contemporâneo II. Florianópolis: CONPEDI, 2018, v.01, p. 23-43. Disponível em: http://site.conpedi.org.br/publicacoes/0ds65m46/41oo8qd1/85w1vH9UyXUZr709.pdf. Acesso em: 03 fev. 2022.

MASSARO, Heloisa; SANTOS, Bruna; BIONI, Bruno; BRITO CRUZ, Francisco; RIELLI, Mariana; VIEIRA, Rafael. **Proteção de Dados nas Eleições:** democracia e privacidade. Grupo de Estudos em Proteçãode Dados e Eleições, 2020.

MELLO, Patrícia Campos. Empresas burlam regras e mantêm disparos em massa de mensagens eleitorais. Folha de São Paulo, 5 out. 2020. Disponível em: https://www1.folha.uol.com.br/poder/2020/10/empresas-burlam-regras-e-mantem-disparos-em-massa-de-mensagens-eleitorais.shtml. Acesso em: 6 out. 2022.

PAPAKYRIAKOPOULOS, Orestis et al. Social media and microtargeting: Political data processing and the consequences for Germany. **Big Data & Society**, vol. 5, n. 2, p. 205395171881184, 2018.

PEDIDO de dados a redes sociais por parte do governo e autoridades saltou 89% no Brasil. **Convergência Digital**, 03 ago. 2022. Disponível em: https://www.convergenciadigital.com.br/Internet/Pedido-de-dados-a-redes-sociais-por-parte-do-governo-e-autoridades-saltou-89%25-no-Brasil-61028.html?UserActiveTemplate=mobile. Acesso em: 28 jun. 2023.

PRESSE, France. Microsoft é multada em US$ 20 milhões por coletar dados de crianças em jogos online do Xbox. **G1**, 6 jun. 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/06/06/microsoft-e-multada-em-us-20-milhoes-por-coletar-dados-de-criancas-em-jogos-online-do-xbox.ghtml. Acesso em: 5 ago. 2023.

PRIMEIRA multa da ANPD foi para disparo eleitoral por celular e WhatsApp. **Convergência**

Digital, 07 jul.2023. Disponível em: https://www.convergenciadigital.com.br/Governo/Primeira-multa-da-ANPD-foi-para-disparo-eleitoral-por-celular-e-WhatsApp-63680.html?UserActiveTemplate=mobile. Acesso em: 07 ago. 2023

RODAS, Sérgio. Constitucionalização da proteção de dados é marco e aumenta segurança jurídica. **Conjur**, 11 fev. 2022. Disponível em: https://www.conjur.com.br/2022-fev11/constitucionalizacao-protecao-dados-marco-aumenta-seguranca. Acesso em: 03 mar. 2023.

RODOTÀ, Stefano. **A vida na sociedade de vigilância** – A privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUEDIGER, Marco Aurélio (Dir.). **Robôs, redes sociais e política:** Estudo da FGV/DAPP aponta interferências ilegítimas no debate público na web. Levantamento mostra que contas automatizadas motivam até 20% de debates em apoio a políticos no Twitter, impondo riscos à democracia e ao processo eleitoral de 2018. FGV/DAPP, 2017. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/18695/Robos-redes-sociais-politica-fgv-dapp.pdf?sequence=1&isAllowed=y. Acesso em: 6 out. 2022.

SANTOS, Bruna et al. **Proteção de dados pessoais e eleições- relatório de recomendações para o quadro brasileiro atual.** Grupo de Estudos em Proteção de Dados e Eleições, versão digital, 2021.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 43. ed. São Paulo: Malheiros, 2020.

SILVEIRA, Marilda de Paula. **As novas tecnologias no processo eleitoral:** existe um dever estatal de combate à desinformação nas eleições? In: ABBOUD, Georges; NERY JUNIOR, Nelson; CAMPOS, Ricardo. *Fake news* e regulação. São Paulo: Thomson Reuters Brasil, 2021, p. 315-339.

SIMONS, J.; GHOSH, D. **Utilities for democracy**: Why and how the algorithmic infrastructure of Facebook and Google must be regulated. Washington, DC: Brookings, 2020. Disponível em: https://www.brookings.edu/wp-content/uploads/2020/08/Simons-Ghosh_Utilities-for-Democracy_PDF.pdf. Acesso em: 12 mai. 2022.

SCHENDES, William. Google multado por coleta abusiva de dados? Esta não é a primeira vez! **Olhar Digital**, 15 ago. 2022. Disponível em: https://olhardigital.com.br/2022/08/15/seguranca/google-multado-rastreamento-abusivo-localizaca. Acesso em: 02 abr. 2023.

SOUZA, Bruno Cezar Andrade de. **Dados pessoais**: LGPD e as eleições, de acordo com a Emenda Constitucional nº 115/2022. Belo Horizonte, D'Plácido, 2022.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Parlamento Europeu, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 12 abr. 2023.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de**

outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. EUR-Lex: Acesso ao direito da União Europeia, [s.d.]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 12 abr. 2023.

UNIÃO EUROPEIA. **General Data Protection Regulation**. 2018. Disponível em: eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=em. Acesso em: 01 maio 2022.

VINTE e cinco contas sofrem violação de dados por minuto no Brasil. **Convergência Digital**, 18 jul. 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Vinte-e-cinco-contas-sofrem-violacao-de-dados-por-minuto-no-Brasil-60887.html?UserActiveTemplate=mobile. Acesso em: 28 jun. 2023.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini. **Tratamento de dados pessoais na LGPD**: estudo sobre as bases legais dos artigos 7º e 11. In: MENDES; Laura Schertel et al. (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2023, p. 115-146.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, vol. 4, n. 5, p. 193-220, dec. 1890.