RPPGD/UFBA
ISSN 2358-4777

DADOS PESSOAIS DIGITAIS E MEDIDAS LEGAIS DE PROTEÇÃO: PREOCUPAÇÕES DEMOCRÁTICAS ACERCA DA UTILIZAÇÃO DE DADOS PESSOAIS DIGITAIS COMO ESTRATÉGIA POLÍTICA

DIGITAL PERSONAL DATA AND PROTECTIVE LEGAL MEASURES: DEMOCRATIC CONCERNS ABOUT THE USE OF DIGITAL PERSONAL DATA AS A POLITICAL STRATEGY

Elisangela Maria Andrioli

Bacharel em Direito pela IMED.
E-MAIL: andrioli.elisangela@gmail.com
Orcid: https://orcid.org/0000-0002-6609-8069

Tássia Aparecida Gervasoni

Doutora em Direito pela Universidade do Vale do Rio dos Sinos, com período sanduíche na Universidad de Sevilla (Espanha). Mestre e Graduada em Direito pela Universidade de Santa Cruz do Sul. Professora de Direito Constitucional e Ciência Política na Faculdade Meridional - IMED.
E-mail: tassiagervasoni@gmail.com
Orcid: http://orcid.org/0000-0002-8774-5421

DOI: XXXXXXX

RESUMO O presente artigo pretende responder ao questionamento: qual a relevância democrática da proteção dos dados pessoais digitais no contexto de sua utilização como estratégia política? Para tanto, aplica-se como metodologia o método de abordagem dedutivo, o método de procedimento monográfico e a técnica de pesquisa a documentação indireta mediante pesquisa bibliográfica. O estudo é organizado em três tópicos, percorrendo três pontos principais que contribuem à solução do problema de pesquisa, quais sejam: a) análise sobre o que são dados pessoais, bem como sobre alguns precedentes relacionados a violações de dados pessoais; b) análise sobre algumas das medidas legais tomadas pelo Brasil a fim de proteger dados pessoais; e c) análise sobre como são utilizados dados pessoais digitais como estratégia política e sobre quais são as preocupações democráticas acerca de sua utilização. Por fim, em síntese, conclui-se que a relevância democrática da proteção de dados pessoais digitais no contexto de sua utilização como estratégia política encontra-se na constatação da atual insuficiência dos meios legais protetivos. Tal situação gera impactos no sistema democrático, notadamente: a) enfraquecimento do pluralismo político; b) retração da

liberdade de expressão, de informação e de escolha; c) mitigação da autonomia privada e política; e d) desconfiança dos cidadãos na própria democracia.

PALAVRAS-CHAVE: Dados pessoais digitais. Democracia. Direito fundamental. Estratégia Política. Proteção de dados pessoais.

ABSTRACT: This article aims to answer the question: which is the democratic relevance of the protection of digital personal data in the context of its use as a political strategy? Therefore, the deductive approach method is applied as a methodology, the procedure method is monographic, and the research technique is indirect documentation through bibliographic research. The study is organized into three topics, covering three main points that contribute to the solution of the research problem, namely: a) analysis of what personal data is, as well as some precedents related to personal data breaches; b) analysis of some of the legal measures taken by Brazil to protect personal data; and c) analysis of how digital personal data is used as a political strategy and what are the democratic concerns about its use. Finally, in summary, it is concluded that the democratic relevance of the protection of digital personal data in the context of its use as a political strategy is found in the verification of the current insufficiency of protective legal means. This situation has an impact on the democratic system, notably: a) weakening of political pluralism; b) retraction of freedom of expression, information and choice; c) mitigation of private and political autonomy; and d) distrust of citizens in democracy itself.

KEY-WORDS: Digital personal data. Democracy. Fundamental Right. Political Strategy. Protection of personal data.

SUMÁRIO: 1. Introdução; 2. Dados pessoais e precedentes internacionais de violações; 3. Medidas legislativas brasileiras de resguardo ao direito fundamental à proteção de dados pessoais; 4. Uso de dados pessoais como estratégia política e preocupações democráticas; 5. Conclusão. 6. Referências.

1 Introdução

Mais do que parte fundamental no cotidiano, os meios digitais se tornaram a principal ferramenta de expressão e descoberta da atualidade. A imersão tecnológica em que a sociedade se encontra incita aos indivíduos a necessidade de que estejam ininterruptamente conectados às redes. Essa condição deixa rastros, mais especificamente, grandes volumes de dados digitais - os quais são coletados e incorporados a uma estrutura capitalista que visa obter rendimentos com sua exploração. Esse mercado de dados não tardou a atingir as campanhas políticas, as quais vislumbraram o cenário ideal para desenvolver novas estratégias.

Diante disso, o ambiente digital, marcado pela versatilidade e pela escassez de regulamentação legal, proporciona um campo aberto tanto a inovações quanto ao cometimento de abusos a direitos já consolidados. A título de exemplo, destaca-se o

escândalo envolvendo as empresas Cambridge Analytica e Facebook. No caso, a descoberta sobre a coleta de dados de milhares de cidadãos para serem utilizados na campanha presidencial de Donald Trump causou impactos internacionais e reflexões acerca da utilização de dados pessoais como estratégia política, invocando incertezas sobre sua legitimidade quando se avalia sob a égide de um sistema pautado na democracia.

Destarte, entende-se significativo discutir sobre dados pessoais digitais e medidas legais que visam sua proteção ante a significativa e constante utilização dos meios tecnológicos, bem como frente aos antecedentes internacionais de violações de dados. Nesse contexto, diante das atuais discussões jurídicas envolvendo dados pessoais digitais, delimita-se a temática às preocupações concernentes à utilização de dados pessoais digitais como estratégia política. Desse modo, questiona-se: qual a relevância democrática da proteção dos dados pessoais digitais no contexto de sua utilização como estratégia política? Assim, o objetivo geral pretende trazer a resolução do referido questionamento, verificando qual a relevância democrática diante do contexto apresentado.

De forma específica, a resposta à questão acima aludida percorrerá três pontos principais, quais sejam: a) análise sobre o que são dados pessoais, bem como sobre alguns precedentes relacionados a violações de dados pessoais que tiveram repercussão internacional; b) análise sobre algumas das medidas legais tomadas pelo Brasil para proteger dados pessoais (Código de Defesa do Consumidor, Marco Civil da Internet, Lei Geral de Proteção de Dados Pessoais, dispositivos constitucionais – artigo 5º, incisos X, XII, LXXIII e LXXIX; e c) análise sobre como são utilizados dados pessoais digitais como estratégia política e sobre quais são as preocupações democráticas acerca de sua utilização. Dessa maneira, os aspectos supracitados serão examinados, respectivamente, em três tópicos ao longo do trabalho.

A metodologia a ser utilizada compõe-se do método de abordagem dedutivo, vez que os conteúdos das premissas de propósito geral serão analisados a fim de responder satisfatoriamente à questão específica relatada. Como método de procedimento, estabeleceu-se que será o monográfico, pois a pesquisa firmada terá como escopo, a partir das generalizações, a análise pontual sobre qual a relevância democrática da proteção dos dados pessoais digitais no contexto de sua utilização como estratégia política. Ou seja, a pesquisa desenvolve-se a partir de um recorte bem delimitado. Por fim, a técnica de pesquisa adotada será realizada por meio de documentação indireta, a qual possui como fundamento o levantamento de dados de variadas fontes (MARCONI; LAKATOS, 2003). Por esse motivo, apresenta-se hábil a orientar o presente estudo, o qual será desenvolvido mediante pesquisa bibliográfica.

Seção 1.01 2 DADOS PESSOAIS E PRECEDENTES INTERNACIONAIS DE VIOLAÇÕES

Na sociedade da informação, o uso constante das tecnologias é tido como basilar à economia e à participação social. Assim, os meios tecnológicos mudaram as relações – conectaram e desconectaram indivíduos, produziram e extinguiram profissões e, acima de tudo, transformaram o modo de visualizar (ou não) a realidade. Na concepção da internet, a anonimização e a impessoalidade eram tidas como características das redes: o potencial econômico das informações ainda era desconhecido (SILVEIRA, 2017). Hoje, as plataformas digitais e os indivíduos tornaram-se mutuamente dependentes da constante disposição de dados: as plataformas para lucrarem[1] e os indivíduos para utilizarem as ferramentas fornecidas pela tecnologia.

Destarte, essa nova perspectiva, diante do grande volume e variabilidade de dados digitais, é pautada no *big data*, ou seja, na capacidade de gerenciamento e armazenamento dos bancos de dados de megaempresas digitais (SILVEIRA, 2019). Dessa forma, dados são extraídos em cada pesquisa, preenchimento de formulário, clique e interação com as plataformas digitais - operando-se até mesmo quando não há interação direta com elas, por meio de serviços de localização, voz e imagem (PARISER, 2012). Assim, embora a maioria dos dados lançados sejam de difícil coleta e, por vezes, descartáveis, aqueles que são significativos - como é o caso de dados pessoais - merecem o empenho. De fato, como será visto adiante, há significativas vantagens a quem os detenha.

Diante disso, imprescindível a conceituação de dado pessoal. Na legislação brasileira, há referência deste como sendo o que possui "informação relacionada à pessoa natural identificada ou identificável" (BRASIL, 2018). Entretanto, não são todas e quaisquer informações, mas somente aquelas que se vinculam objetivamente a um indivíduo, ou seja, quando este é o objeto da informação, viabilizando a identificação de sua pessoa e de suas características (DONEDA, 2011, p.93). Dessa forma, são alguns exemplos de dados pessoais, segundo o Serviço Federal de Processamento de Dados:

[1] Nesse sentido, a obra de Zuboff explora, inclusive, uma nova forma do capitalismo, que é chamado pela autora de "capitalismo de vigilância", o qual "reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para tradução em dados comportamentais". Alguns desses dados servem ao aprimoramento de produtos e serviços, o restante, porém, "é declarado como *superávit comportamental* do proprietário, alimentando avançados processos de fabricação conhecidos como 'inteligência de máquina' e manufaturado em *produtos de predição* que antecipam o que um determinado indivíduo faria agora, daqui a pouco ou mais tarde". Justamente para a comercialização desses produtos, afirma a autora, há um novo tipo de mercado, os *mercados de comportamentos futuros*, no âmbito do qual "os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro" (ZUBOFF, 2020, p. 18-19).

> [...] nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies, entre outros (SERPRO, 2019).

Nesse contexto, conforme afirma Doneda (2010, p.39), "os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantém uma ligação concreta e viva com a pessoa". Mais que isso, "os dados pessoais são a pessoa" (DONEDA, 2010, p.39), pois exprimem as características mais íntimas e singulares dos indivíduos, desejáveis ou não por estes. Também, conforme recente disposição legal[2], poderão ser considerados dados pessoais aqueles que forem utilizados para formar perfis comportamentais dos indivíduos. Todavia, não serão considerados como dados pessoais aqueles que forem anonimizados, ou seja, desassociados, de forma direta ou indireta, a uma pessoa específica (BRASIL, 2018).

É notável que, quando isolados, os dados se apresentam apenas como fragmentos de informação, diferenciando-se desta por ostentarem elementos brutos, descontextualizados e, geralmente, com irrisório potencial lesivo. No entanto, quando os dados são agrupados, permitem uma identificação detalhada sobre a personalidade do indivíduo, confundindo-se com esta e, por isso, aptos a ferir a intimidade, a imagem e até mesmo a dignidade do ser humano. Sob essa perspectiva, expõe Magrani: "[...] devemos ter em mente que essas informações pessoais estão ligadas aos direitos da personalidade dos usuários. Para protegê-las, bem como proteger a dignidade humana, é necessário assegurar a tutela dos dados pessoais" (2019, p.58).

À luz da proteção da dignidade da pessoa humana, o ordenamento jurídico faz distinção quanto aos dados pessoais sensíveis. A definição é trazida pela Lei Geral de Proteção de Dados (LGPD):

> Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

O conceito definido explicita os dados que possuem elementos íntimos e sensíveis à eventual utilização discriminatória. Por isso, demandam maior grau de

[2] Art. 12, caput e §2º, da Lei nº 13.709/18.

prudência e resguardo, principalmente no que tange às atividades de tratamento[3]. Sendo assim, ao protegê-los, estar-se-á salvaguardando a dignidade da pessoa humana, uma vez que a plena tutela da pessoa deve considerar aspectos atinentes à identidade e à privacidade – elementos notáveis no amparo a atributos da personalidade, como, por exemplo, dados pessoais (MULHOLLAND, 2018).

Outro fator importante refere-se ao fato de que os dados pessoais, quando incorporados aos meios digitais, adquirem características próprias, demandando maior tutela devido ao excepcional grau de vulnerabilidade, maleabilidade e difusão de que dispõem. Em geral, eles são veiculados na internet quando se utilizam serviços gratuitos, que, por terem essa qualidade, auferem lucros mediante a venda daqueles (BIONI, 2019, p.47). Além disso, sabe-se que "os dados são facilmente vendidos no mercado negro (sic), pois não carregam consigo nenhum indício sobre o local de onde vieram ou por onde passaram pelo caminho lavagem de dados" (PARISER, 2012, p.144-145). Geralmente, a venda é realizada por empresas que produzem *spywares* e *spams*, conhecidas por obterem dados de forma clandestina e por repassá-los a bancos de dados de grandes empresas para fins de marketing segmentado (PARISER, 2012).

Com o intuito de dar uma dimensão da atual utilização dos meios digitais, estatísticas de janeiro de 2019 mostram que 70% dos brasileiros possuem acesso à internet, ou seja, mais de 149 milhões de pessoas. Nessa acepção, em média 3 horas e 24 minutos por dia são despendidos nas redes sociais, dentre as quais as mais acessadas são: Youtube (95%), Facebook (90%), WhatsApp (89%) e Instagram (71%) (KEMP, 2019). Também, além da utilização convencional da internet por meio de computadores, laptops, celulares, tablets, etc., vem ganhando espaço a interação entre vários tipos de objetos – chamada de Internet das Coisas. A exemplo, vestuários, eletrodomésticos e automóveis que utilizam sensores que captam aspectos do mundo real e os transformam em informações inteligentes para auxiliar no cotidiano (SANTOS, 2016).

Sob esse viés, o uso constante dessas tecnologias permite que haja uma ininterrupta vigilância sobre o indivíduo frente à multiplicidade de dados coletados e processados diariamente (MAGRINI, 2019). Desse modo, o indivíduo torna-se identificável por seus hábitos e interesses online, possibilitando a criação de um perfil de usuário e a consequente personalização de seus acessos digitais (HANKEY; MORRISON; NAIK, 2019). Destarte, essa personalização baseada no comportamento online gera, de acordo com Pariser (2012, p.11), "um universo de informações exclusivo para cada um de nós – o que passei a chamar de bolha dos filtros – que

[3] Tratamento conceitua-se como: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018).

altera fundamentalmente o modo como nos deparamos com ideias e informações". Dessa forma, a "bolha de filtros" limita o poder de escolha, dificultando o contato com novas experiências e perspectivas de vida.

À vista disso, de modo a introduzir os precedentes sobre violações que aqui serão especificados, há que se demonstrar o trâmite entre o lançamento de um dado até seu agrupamento e posterior transformação em informação útil. Em síntese, conforme explicam Silveira, Avelino e Souza (2017, p. 224), preliminarmente os dados são coletados e armazenados em bancos de dados, por vezes, compartilhados entre empresas. Após, ocorre a fase de processamento e mineração, que possui como fim agregar informações sobre um indivíduo de modo a criar um perfil detalhado sobre este. Em seguida, os perfis são analisados e dispostos em segmentos de públicos semelhantes para serem vendidos. Por fim, são modulados, ou seja, ofertados às entidades por meio de serviços e produtos, como marketing segmentado e filtragem de conteúdo, de modo a atender estratégias e necessidades específicas.

Assim ilustra Sergio Amadeu da Silveira:

> Algumas companhias desenvolvem softwares que geram estatísticas e analisam o comportamento pessoal, outras criam soluções para obter dados das pessoas e acompanhar sua navegação na internet com o objetivo de analisar suas escolhas, o tempo em que permanecem em uma página da web, as cores e textos que prendem a atenção nos anúncios em redes sociais e o tipo de postagem que repele indivíduos de determinados segmentos sociais (2017, p.21).

Apesar disso, na maioria das vezes, os usuários não sabem que seus dados pessoais estão sendo coletados e utilizados indistintamente, acreditam que sua navegação e seus compartilhamentos são visíveis tão somente a eles e a seus destinatários (DONEDA, 2010, p.66). O consentimento dado aos corretores de dados (*brokers*)[4] para que os vendam é, por vezes, inexistente ou insuflado nas entrelinhas do termo de uso. Assim, o indivíduo encontra-se vulnerável a interferências dos que possuem o controle sobre essas informações, propenso a ser intimamente afetado em suas decisões.

Sob esse viés, alguns precedentes internacionais relacionados a violações de dados pessoais resultaram discussões acerca do modo como a coleta dos dados é

[4] "Os chamados corretores de dados (brokers) são empresas que recolhem e mesclam informações agregadas sobre os indivíduos, podendo atuar em duas, três ou quatro camadas desse mercado de dados. Algumas dessas empresas são bem conhecidas, tais como a antiga Serasa, no Brasil, adquirida pela Experian." (SILVEIRA; AVELINO; SOUZA, 2017, p. 224).

realizada e sua legitimidade jurídica. Aqueles que aqui serão elencados atuaram como precursores de mudanças legislativas em diversos países, as quais serão posteriormente relatadas. Assim, de modo introdutório, cabe uma breve explanação sobre os casos.

O episódio que primeiramente demonstrou a massiva coleta de dados ocorreu em junho de 2013, quando Edward Snowden, um ex-contratado da National Security Agency (NSA)[5], divulgou informações referentes à espionagem efetuada pela referida agência estadunidense. No caso, eram espionados, entre outros, registros telefônicos, envios e recebimentos de e-mails, dados de navegação em plataformas - como Google, Facebook e Yahoo - de milhões de indivíduos pelo mundo, sob a justificativa de prevenir ataques terroristas. A espionagem ocorria de forma obscura, sem qualquer tipo de consentimento dos titulares, e irritou alguns chefes de poder pelo mundo, como Dilma Rousseff - na época, presidente do Brasil - que teve seus dados violados pela agência (MACASKILL; DANCE, 2013).

Em 2018 irrompeu o escândalo ligado à eleição presidencial estadunidense de 2016, na qual Donald Trump foi eleito. O caso envolveu a Cambridge Analytica, empresa de mineração e análise de dados contratada por Trump para o auxiliar na campanha política, e o Facebook, rede social amplamente utilizada pelo mundo. Nesse contexto, há evidências de que o Facebook concedia à Cambridge Analytica os dados de cerca de 87 milhões de usuários. Para adquiri-los, além de métodos usuais de coleta, como *cookies*, testes de quiz ofertados na rede social coletavam dados dos indivíduos e de seus amigos, sem ambos saberem. Após, unindo esses dados com outros já adquiridos pela plataforma, eram formados perfis comportamentais dos usuários a fim de que fossem separados em audiências específicas para serem vendidas (ISAAK; HANNA, 2018).

Nota-se que as técnicas não eram apenas utilizadas aos usuários do Facebook, mas a vários indivíduos que a empresa Cambridge Analytica de alguma forma possuía os dados, atingindo-os por meio de diversas plataformas online (ISAAK; HANNA, 2018). Conforme afirma Hankey, Morrison e Naik (2019, p.16, tradução nossa), "a companhia gabava-se de possuir 5000 a 7000 pontos de dados de 230 milhões de cidadãos dos Estados Unidos". Dessa forma, múltiplos dados pessoais eram utilizados para formar grupos de personalidades. A esse propósito, os indivíduos eram divididos em 5 modelos de perfis com base em seus principais atributos: abertura, consciência, extroversão, agradabilidade e neuroticismo – intitulada escala OCEAN[6] (DAVIES, 2015). Com base nessa listagem, as audiências específicas eram analisadas em relação a suas características predominantes, regiões geográficas e possíveis perfis eleitorais, que

[5] Agência de Segurança Nacional dos Estados Unidos.
[6] OCEAN: openness, conscientiousness, extraversion, agreeableness, neuroticism.

demonstravam se o indivíduo estava indeciso e propenso a ser influenciado em seu voto (PRIVACIDADE, 2018).

Desse modo, a "bolha" em que eram inseridos distorcia a realidade clandestinamente, de modo que os cidadãos recebiam diferentes tipos de informações, muitas vezes falsas ou tendenciosas, em forma de anúncios, mensagens e publicações personalizadas, conforme seu tipo de personalidade (HANKEY; MORRISON; NAIK, 2019). Assim, no que se refere à utilização de dados pessoais na campanha de Donald Trump, embora não tenha sido a única razão de sua vitória nas eleições, contribuiu-lhe significativamente, visto que milhões de cidadãos foram atingidos pelos anúncios comportamentais que objetivavam os influenciar em suas escolhas eleitorais (ISAAK; HANNA, 2018).

Além da utilização indevida de dados pessoais de milhões de indivíduos na eleição presidencial dos Estados Unidos, há sólidos indícios de que foram também utilizados na saída do Reino Unido da União Europeia (*Brexit*). No testemunho de Brittany Kaiser, ex-contratada da Cambridge Analytica, há relatos de que ela teria sido convidada a elaborar uma estratégia de campanha em conjunto com uma empresa de seguros que possuía dados de quase 24 milhões de britânicos. Sabe-se, ainda, que 98% do orçamento para a campanha do *Brexit* foi gasto em mídia digital (HANKEY; MORRISON; NAIK, 2019, p.23-24). Além disso, no depoimento prestado por Shahmir Sanni, ex-voluntário da campanha do *Brexit*, ele relata que esta infringiu a lei ao afirmar que doaria 625 mil euros e, posteriormente, desviar o dinheiro a uma empresa de anúncios e análise de dados vinculada à Cambridge Analytica. O fato foi confirmado pela Comissão Eleitoral meses depois (CADWALLADR, 2019).

Desse modo, por terem aptidão de lesar a democracia e a privacidade dos indivíduos, essas violações foram tidas como precedentes de incentivo à criação de leis protetivas ou à modernização das já existentes. Uma das mudanças mais significativas foi a criação em 2016 de um regulamento chamado *General Data Protection Regulation* (GDPR), vigente na União Europeia desde 2018 (MAGRANI, 2019). O regulamento substituiu e ampliou a legislação anterior que já previa dispositivos de proteção de dados.

Outrossim, a Lei Geral de Proteção de Dados brasileira (LGPD), aprovada em 2018, inspirou-se diretamente no regulamento europeu e propôs um novo *standart* protetivo aos dados pessoais, o qual será analisado nos próximos tópicos. Além disso, a Emenda Constitucional 115/2022 elevou expressamente a proteção de dados pessoais digitais ao status de direito fundamental ao incluir, no artigo 5º, o inciso LXXIX, o qual prevê: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 1998).

Fora isso, nos Estados Unidos, um dos países mais afetados pelas violações, não há uma lei geral que preveja a proteção de dados. No entanto, existem algumas leis federais esparsas e algumas leis protetivas estaduais bem rigorosas - como nos estados de Califórnia e Nova York, que possuem legislações que entraram em vigor em 2020 e preveem aos residentes garantias e controles em face da utilização de seus dados (GATEFY, 2020).

Com efeito, os casos acima explorados demonstram como os dados pessoais são vulneráveis e podem ser explorados de forma inconsequente quando não há um sistema de proteção eficaz. A realidade tecnológica atual exprime a ideia de que é imprescindível que se sucedam incessantes adaptações e mudanças no ordenamento jurídico a fim de que os direitos fundamentais sejam resguardados. De tal modo, por serem os indivíduos os mais vulneráveis nessa relação, cada vez mais são necessários, de acordo com Doneda (2011, p.92), "mecanismos que proporcionem à pessoa efetivo conhecimento e controle sobre seus próprios dados, dados estes que são expressão direta de sua própria personalidade".

À vista disso, pertinente a análise de Pariser quanto à relação entre a democracia e a "bolha de filtros" formada quando o controle e a proteção aos dados pessoais demonstram-se insuficientes:

> Em última análise, a democracia só funciona se os cidadãos forem capazes de pensar além de seu interesse próprio limitado. No entanto, para isso precisamos de uma imagem comum do mundo que coabitamos. Precisamos entrar em contato com a vida de outras pessoas, seus desejos e necessidades. A bolha dos filtros nos move na direção oposta – cria a impressão de que nosso interesse próprio é tudo que existe. E embora isso seja ótimo quando o objetivo é vender produtos on-line, não ajuda as pessoas a tomar melhores decisões juntas (2012, p.112).

Isso posto, tendo em vista a constante necessidade de adaptação do direito frente às mudanças tecnológicas, o Brasil vem adotando uma série de medidas legislativas a fim de coibir violações e possíveis rupturas no Estado democrático de direito. No próximo tópico, algumas dessas medidas serão analisadas a fim de averiguar se são eficientemente hábeis a proteger os dados pessoais nos meios digitais e, de forma consequente, a democracia.

ARTIGO II. 3 MEDIDAS LEGISLATIVAS BRASILEIRAS DE RESGUARDO AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Acompanhar as inovações tecnológicas e suas relações subsequentes sempre foi um desafio para o Direito. Por certo, o volume de dados veiculados nas redes se expandiu, assim como a capacidade de armazenamento dos bancos de dados. Além disso, amplificaram-se as formas de extração de informações destes por meio de práticas de coleta, tratamento e análise - até então impossíveis ou injustificáveis de serem realizadas de forma manual (DONEDA, 2010).

Assim, a utilização prática das informações subsequentes, tanto na vigilância dos cidadãos quanto na ingerência de métodos aptos a influir determinada conduta - como o consumo - traz insegurança no emprego das tecnologias, além de suscitar dúvidas quanto à eficiência do direito à privacidade. Não é por acaso que, nas últimas décadas, vários países implementaram medidas legais tentando normatizar a internet e suas relações. No Brasil não foi diferente: várias medidas legislativas foram adotadas visando regular a rede e proteger os dados pessoais.

De modo geral, as medidas tomadas tiveram como base comum um núcleo de princípios elaborados na década de 70 pela *Secretary for Health, Education and Welfare* (HEW) - após a tentativa falha de criação, nos Estados Unidos, de um banco de dados sobre os cidadãos para uso estatal. Os preceitos passaram a ser referidos como *Fair Information Principles* e influenciaram diversas diretrizes e normas de proteção de dados, como as *Guidelines* da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), sustentando-se até os dias atuais por meio de revisões e atualizações (DONEDA, 2010, p.43-45).

Destarte, a enunciação mais recente desses princípios, feita pelo *Department of Homeland Security* norte-americano, pode ser assim sintetizada:

> 1 - Princípio da transparência, pelo qual o tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados [...];
>
> 2 - Princípio da qualidade, pelo qual os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes [...];
>
> 3 - Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados [...];
>
> 4 - Princípio do livre acesso, pelo qual o indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros [...];

> 5 - Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado (DONEDA, 2010, p.46).

Sob esse viés, a aplicação precursora dos *Fair Information Principles* no ordenamento jurídico brasileiro deu-se no âmbito do Código de Defesa do Consumidor (CDC - Lei 8.078/90), encarado como o marco normativo na esfera protetiva de dados brasileira (DONEDA, 2011, p. 103). Na seção VI, valendo-se dos princípios da transparência, da qualidade e do livre acesso, o Código versa sobre a proteção dos bancos de dados e cadastros de consumidores.

No segmento normativo, zela aos consumidores o acesso às informações pessoais existentes (art. 43, caput), descritas de forma objetiva, com clareza e fidedignidade, não sendo possível a manutenção de informações negativas por mais de cinco anos (Art. 43, §1º). Além disso, o consumidor possui o direito de que eventuais incorreções sejam corrigidas (art. 43, §º3º). Outrossim, deve ser notificado da abertura de cadastros, fichas e registros de dados pessoais quando não por ele solicitada (Art. 43, §2º) (BRASIL, 1990).

Em que pese o CDC represente um avanço na proteção de dados e possibilite interpretações irradiantes ao ordenamento jurídico, sua incidência se limita às relações de consumo. De fato, por ter como foco os bancos de dados creditícios - porém não a eles limitado - o diploma normativo não assegura o sistema de proteção de dados requerido atualmente (DONEDA, 2010, p. 52-53). De todo modo, diante da pluralidade de circunstâncias hábeis a gerar violações de dados, principalmente na internet, normas subsequentes destinaram-se à regulação desta.

A Lei nº 12.965/2014, intitulada como Marco Civil da Internet (MCI), foi a primeira norma específica a estabelecer direitos aos usuários da rede no Brasil. Sua criação pautou-se em deliberações da sociedade civil e foi uma reação desta contra propostas legislativas que visavam regular penalmente a internet. Na época, o vazamento de informações por *Edward Snowden* sobre a vigilância exercida pela NSA repercutiu na elaboração do MCI, o qual se preocupou em resguardar, ainda que de forma principiológica, os dados pessoais e a privacidade dos cidadãos nos meios digitais (BIONI, 2019).

A normativa elenca princípios norteadores do uso da internet, tais como: liberdade de expressão, proteção da privacidade, proteção dos dados pessoais e neutralidade de rede. Além disso, são garantidos aos usuários diversos direitos que perpassam desde a inviolabilidade e o sigilo de suas comunicações privadas, conforme

garantido constitucionalmente, até direitos que amparam situações inerentes ao tratamento de dados (BRASIL, 2014).

Quanto à temática de dados pessoais, o MCI dispõe que não poderá haver fornecimento a terceiros, salvo em hipóteses legais ou mediante consentimento livre, expresso e informado. Além disso, quando houver coleta, as informações sobre a atividade deverão ser claras e completas. Também, os dados pessoais só poderão ser utilizados para finalidades que a justifiquem, não sejam ilegais e estejam de acordo com o contrato ou termo de uso (BRASIL, 2014).

Destarte, o Marco Civil da Internet deu enfoque ao consentimento do titular de dados, devendo ser atribuído de forma expressa e destacada de outras cláusulas. Ademais, atentando-se à autodeterminação informativa, há previsão de que, ao término da relação e mediante requerimento do titular, deverá haver a exclusão definitiva dos dados pessoais fornecidos, salvo hipóteses legais de manutenção dos registros (BRASIL, 2014).

Quanto à abrangência territorial, o art. 11 menciona que qualquer operação de coleta, armazenamento, guarda e tratamento realizada no território nacional deverá respeitar a legislação brasileira, bastando que apenas uma dessas atividades seja realizada no país. O artigo aplica-se mesmo que a pessoa jurídica se situe no exterior, desde que seja ofertado serviço ao público brasileiro ou haja no grupo econômico pessoa jurídica sediada no Brasil (BRASIL, 2014).

Ainda, a lei prevê sanções aos que descumprirem os dispositivos pertinentes à proteção de registros, dados e comunicações (arts. 10 e 11). Desse modo, poderá ser cominada, isolada ou cumulativamente: advertência, multa, suspensão temporária de exercício das atividades referidas no art. 11, além da proibição destas, sem prejuízo de demais sanções cíveis, penais ou administrativas (BRASIL, 2014).

Sob esse viés, percebe-se que o MCI é referência na esfera principiológica, garantindo inclusive os *Fair Information Principles* da transparência e finalidade em suas disposições. Contudo, por ter tido como enfoque a disposição de direitos dos usuários e de regras relacionadas aos registros de conexão e de acesso a aplicações[7], a lei não regulamentou suficientemente questões referentes à privacidade e proteção de dados pessoais. Sendo assim, pelo avanço da tecnologia, a legislação aos poucos se evidenciou defasada e novas disposições demonstraram-se imprescindíveis.

[7] O MCI dispõe sobre esses conceitos no art. 5º, inciso VI e VII: "registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado [...]" e "registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (BRASIL, 2014), tais como redes sociais, contas de e-mail, etc.

Depois de muitos anos de debate e de pressão internacional pela convergência de normas protetivas, a Lei nº 13.709/2018, intitulada Lei Geral de Proteção de Dados (LGPD), inaugurou no sistema jurídico brasileiro a regulamentação elementar no que tange a dados pessoais. Por ter sido inspirada no modelo europeu, guarda com a GDPR algumas similitudes, tais como: a definição de dados pessoais e dados sensíveis, a indicação de direitos dos titulares de dados, o dever dos provedores de serviço na designação de um encarregado de proteção de dados, a concepção de uma agência reguladora nacional, a responsabilização dos agentes, a delineação de penalidades, entre outros procedimentos. Entretanto, difere em alguns pontos, sobretudo quanto à autonomia dada pela lei europeia às suas agências reguladoras, as quais se desvinculam de qualquer órgão - contrário do que ocorre no Brasil, em que a agência responsável, dotada de autonomia técnica e decisória, vincula-se à Casa Civil da Presidência da República (LORENZON, 2021).

Isso posto, o principal objetivo da LGPD é dispor sobre o tratamento de dados pessoais de modo a proporcionar "garantias aos direitos do cidadão, ao mesmo tempo em que fornece as bases para o desenvolvimento da economia da informação, baseada nos vetores da confiança, segurança e valor" (MENDES, DONEDA, 2018, p. 470). Sendo assim, verifica-se que a lei pretende proteger as pessoas naturais, e tão somente estas, independente de quem seja o responsável pelo tratamento. Dessa forma, os responsáveis podem ser pessoais naturais, jurídicas (públicas ou privadas), independente de modalidade, meio de tratamento ou país de origem, desde que se enquadrem nos incisos do art. 3º da LGPD. Não obstante, especificadas no art. 4º, existem exceções de não aplicação, embasadas em direitos fundamentais ou em interesse público relevante - como atividades relativas à segurança pública (MENDES, DONEDA, 2018).

Conferindo unidade sistêmica à disciplina, a LGPD estabelece princípios que deverão nortear as atividades relacionadas ao tratamento de dados, indo além aos já consolidados *Fair Information Principles.* Dentre os "novos", destacam-se os princípios da adequação e da necessidade, os quais dispõem que deverá haver compatibilidade entre o tratamento e o fim informado, limitando-se ao mínimo necessário. Ressalta-se também o princípio da não discriminação, o qual veda potencial uso discriminatório de dados pessoais e corrobora com a proteção especial conferida aos dados pessoais sensíveis. Ademais, o princípio da boa-fé - já conhecido no ordenamento jurídico brasileiro - denota fundamental importância ao reger as relações elencadas no diploma, tendo em vista a opacidade e a diversidade de operações de tratamento de dados (MENDES, DONEDA, 2018).

De forma conexa, aos titulares de dados pessoais são conferidos direitos imprescindíveis ao resguardo da privacidade, da autodeterminação informativa e da

liberdade de expressão. Assim, é garantido ao titular, dentre outras disposições, a confirmação da existência de tratamento; o acesso aos dados; correção de dados incorretos; anonimização, bloqueio ou eliminação de dados desnecessários; portabilidade de dados a outro fornecedor, além da possibilidade de solicitar revisão de decisões tomadas com base em tratamento automatizado de dados pessoais, inclusive as que definam seu perfil (BRASIL, 2018).

No que concerne à legitimação ao tratamento de dados, a atividade deverá enquadrar-se em uma das hipóteses autorizativas previstas no art. 7º ou no art. 23 da LGPD. Dentre elas, destaca-se a hipótese de consentimento, o qual deverá ser expresso e especifico à finalidade informada, podendo ser revogado a qualquer momento. Entretanto, conforme art. 7º, §4º, dispensa-se o consentimento se os dados foram tornados manifestamente públicos pelo titular, condição esta que pode abrir brechas à utilização indevida de, por exemplo, publicações em redes sociais - muito embora tal condição deva obedecer à sistemática legal de direitos e princípios vigentes (BRASIL, 2018).

Outrossim, a lei estabelece obrigações aos agentes de tratamento de dados, os quais deverão adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais dos indivíduos contra acessos não autorizados; bem como estabelece procedimentos de segurança e prevenção (BRASIL, 2018). Importa destacar três inovações: a) exigência de medidas que certifiquem a integridade, confidencialidade e disponibilidade dos dados; b) dever de comunicar à autoridade de proteção de dados quando ocorrerem incidentes de segurança; e c) obrigação de garantir a proteção de dados desde o início da operação, nos moldes do *Privacy by Design*[8] (MENDES, DONEDA, 2018).

De tal modo, em caso de danos, a LGPD dispõe sobre a responsabilização dos agentes de tratamento, especificando-os, e preceituando, na consideração das sanções, a natureza e a finalidade das atividades praticadas (BRASIL, 2018). Trata-se, conforme prevê Mendes e Doneda, de responsabilidade objetiva, "vinculando a obrigação de reparação do dano ao exercício de atividade de tratamento de dados pessoais" (2018, p. 477). Destarte, a lei prevê penalidades administrativas que vão desde advertência até proibição total do exercício das atividades (BRASIL, 2018).

Por último, mas não menos importante, no capítulo IX da LGPD, há previsão da criação da Autoridade Nacional de Proteção de Dados (ANPD) na forma de autarquia especial, dotada de autonomia técnica e decisória. A ANPD, regulamentada pelo Decreto 10.474/2020, detém papel central na fiscalização das atividades de tratamento, além de poder regulamentá-las, sancionar os agentes violadores e

[8] Termo que se refere à preservação da privacidade desde a concepção até a execução da operação, ou seja, durante todo o ciclo de processamento, fulcro art. 46 §2º da Lei 13.709/2018 (BRASIL, 2018)

promover o conhecimento das normas à população (BRASIL, 2018). Nesse sentido, não se trata de simples coadjuvante, mas "o pilar de sustentação, sem o qual todo o arcabouço normativo e principiológico não está apto a funcionar de forma adequada" (MENDES, DONEDA, 2018, p. 478).

À vista disso, a Lei Geral de Proteção de dados, totalmente em vigor desde agosto de 2021, representa um grande avanço no ordenamento jurídico brasileiro e traz mais transparência e responsabilidade ao tratamento de dados pessoais. Destarte, vale citar a concepção de Mendes e Doneda sobre a referida Lei:

> Do exposto, percebe-se que LGPD foi um importante passo rumo ao fortalecimento do marco normativo da sociedade da informação no Brasil. É preciso agora desenvolver uma cultura de proteção de dados, construir uma sólida estrutura institucional para a aplicação da LGPD, assim como uma doutrina aprofundada sobre os diferentes temas tratados pela Lei, propiciando segurança jurídica para os atores da economia digital, a proteção da confiança do titular dos dados e incentivando o desenvolvimento econômico do país nessa área (2018, p.482).

Sem dúvida, as leis aqui mencionadas destacam-se na composição do sistema protetivo de dados pessoais no Brasil e convergem no sentido de integrar o direito fundamental à proteção de dados pessoais - o qual já se mostrava implícito no ordenamento jurídico muito antes de ser efetivamente positivado pela EC 115/2022. Assim, quanto ao viés constitucional, a referida tutela correlaciona-se com o direito à intimidade e à vida privada, com o direito à inviolabilidade do sigilo de dados e com a garantia constitucional de Habeas Data - ambos previstos, respectivamente, no art. 5º, incisos X, XII e LXXIII, da Constituição Federal (BRASIL, 1988).

Diante do exposto, no que tange à salvaguarda da intimidade e da vida privada, tem-se que - pelo fato de revelarem atributos da personalidade e possuírem aptidão de expor a vida privada e a intimidade dos indivíduos -, notavelmente, o uso de dados pessoais possui capacidade de violar o direito à privacidade. Este, em sua concepção tradicional, refere-se "ao direito de ser deixado só", assim entendido como a proteção contra intromissões alheias no que é particular ao indivíduo, protegendo-o contra a exposição não autorizada de informações pessoais (MULHOLLAND, 2018).

À luz disso, ao derivar a tutela de dados pessoais diretamente do direito à privacidade – sob a visão clássica - corre-se o risco de limitar seu alcance, uma vez que é necessário um olhar mais amplo deste direito frente às tecnologias atuais (DONEDA, 2019). Assim, há que se destacar a tendência em buscar redefinições ao conceito de privacidade. Seguindo tal acepção, cita-se Stefano Rodotá:

> Na sociedade da informação tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas. Assim, a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações (2008, p. 92).

De fato, as relações cibernéticas são insuficientemente protegidas ao admitir tão somente o sentido negativo do direito à privacidade. É necessário contemplá-lo, também, em sua forma positiva (BIONI, 2019), sob a figura da autodeterminação informativa - vislumbrada como a "faculdade de o particular determinar e controlar a utilização dos seus dados pessoais" (CANOTILHO, 2003, p. 515). À vista disso, o referente entendimento, ainda que não plenamente difundido, alcança a devida compreensão que merece ser dada ao conceito de privacidade nos tempos atuais.

Além disso, como desdobramento do direito à privacidade, pode-se vislumbrar o direito à extimidade, que visa proteger exposições voluntárias, porém que não são atingidas a todos de forma pública. Assim, tem-se o direito de desfrutar da própria intimidade em ambientes sociais – como por meio de publicações em redes sociais - sem, no entanto, perder o controle sobre os dados ali veiculados. De igual modo, os dados pessoais expostos são protegidos contra a utilização de terceiros, os quais não possuem legitimidade de usufruir daqueles sob a justificativa de autoexposição ou espaço público (BOLESINA, GERVASONI, 2019, p.15).

Conquanto, vê-se que, embora as novas significações ao conceito de privacidade representem um avanço no que tange à proteção de dados pessoais, a tutela vindicada não fica a ele restrita. Destarte, pertinente a análise de Bioni:

> O direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica [...] foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade [...] Além disso, observa-se que cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, em particular quando elas são submetidas a processos de decisões automatizadas que irão definir seu próprio futuro. Nesse contexto, o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana, em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade (2019, p. 126-127).

Quanto à inviolabilidade do sigilo de dados, há entendimento firmado pelo Supremo Tribunal Federal de que a salvaguarda é tão somente relativa à comunicação destes. Assim sendo, em que pese a tutela acerca da comunicação ser indispensável, a interpretação dada não abrange a complexidade de situações a serem protegidas (DONEDA, 2019). Outrossim, nota-se que "tal interpretação traz consigo o risco de sugerir uma grande permissividade em relação à utilização de informações pessoais" (DONEDA, 2019, p. 262) - o que pode se demonstrar prejudicial ao indivíduo por sugerir a escusa de proteção mais ampla.

Por fim, no que tange ao instrumento dedicado à proteção de dados, notabiliza-se a ação mandamental de Habeas Data. Concebido na Constituição Federal de 1988, em um contexto pós-ditatorial, o Habeas Data - instituto destinado a assegurar o conhecimento e a retificação de informações pessoais contidas em bancos de dados de entidades governamentais ou de caráter público - visou consolidar bases democráticas a um sistema assombrado pela ditadura. Ainda visto por alguns como uma ação simbólica, o instrumento assegura implicitamente dois direitos essenciais à proteção de dados pessoais: o de acesso e o de retificação (DONEDA, 2019).

Contudo, a ação de Habeas Data, apesar de bem-intencionada e satisfatória à época de sua concepção, possui algumas limitações contemporâneas: a) a amplitude estrita a bancos de dados de entidades governamentais ou de caráter público; b) a necessidade da postulação administrativa e sua negativa para que seja requerida judicialmente; c) a exigência de advogado para a impetração; e d) a consequente morosidade nesse trâmite. Além disso, observa-se que sua robusta estrutura processual, vislumbre da Lei 9.507/1997, obscurece os desígnios de expandir o instrumento a outras funções que não o conhecimento e a retificação de dados (DONEDA, 2019).

Por conseguinte, "o recurso a princípios não basta frente à maleabilidade e dinamicidade do fenômeno tecnológico, que requer instrumentos com alto grau de objetividade para uma tutela efetiva dos interesses em questão" (DONEDA, 2019, p. 287). Assim, a fim de garantir a proteção adequada, há que se redefinir o papel do Habeas Data. Alternativas podem surgir no intuito de pluralizar a abrangência do instituto, tornando-o central na proteção de dados, ou de assentir suas funções atuais e estruturar novos instrumentos aptos a efetivamente fornecer a proteção requerida atualmente, legando ao Habeas Data um caráter residual (DONEDA, 2019).

Diante do que foi exposto, no que tange à proteção de dados pessoais no Brasil, há ainda um longo caminho a percorrer. Os primeiros passos já foram dados, haja vista a incorporação, no artigo 5º, do inciso LXXIX, que estabeleceu o direito fundamental à proteção de dados pessoais. Sabidamente, a incorporação ao rol de direitos fundamentais traz harmonia ao sistema protetivo, além de evidenciar a

magnitude relativa à tutela de dados pessoais na sociedade da informação. Nesse sentido, vale ressaltar a conexão entre democracia e direitos fundamentais sob a ótica da expertise de J.J. Gomes Canotilho:

> Tal como são um elemento constitutivo do estado de direito, os **direitos fundamentais** são um elemento básico para a realização do princípio democrático. [...] os direitos fundamentais, como *direitos subjectivos de liberdade*, criam um espaço pessoal contra o exercício de poder antidemocrático, e, como direitos legitimadores de um domínio democrático, asseguram o exercício da democracia mediante a exigência de *garantias de organização* e de *processos* com transparência democrática (2003, p.291-292, grifos do autor).

Destarte, ante o olhar substancial de democracia, é reivindicada não somente a positivação de direitos fundamentais, mas sua efetiva concretização. Ressalta-se que estes direitos não ficam restritos aos intitulados direitos políticos, mas também englobam contrapoderes como direitos sociais e de liberdade (FERRAJOLI, 2014, p.81). Dito isso, ao mesmo tempo em que a democracia é acautelada pelos direitos fundamentais, perfaz o alicerce para que estes direitos sejam plenamente exercidos. Dessa forma, coexistem de forma simbiótica, vinculando-se, conforme enuncia Ferrajoli, dentro da própria definição de democracia: "O significado profundo da democracia consiste nesta relação entre os meios institucionais e os fins sociais e na consequente primazia dos direitos fundamentais sobre os poderes públicos[9]" (2014, p.83, tradução nossa).

À vista disso, importante notar que o sistema democrático há tempos vem sendo fragilizado pelo hiato entre Direito e tecnologia, principalmente no que tange ao uso indevido de dados pessoais digitais como estratégia política, conforme alguns exemplos já citados. Por essa razão, desvelando as percepções acima referidas, tem-se que - ao incorporar o direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro – é dado, além de um novo amparo aos indivíduos contra os abusos cometidos nas redes, um novo alicerce a sustentar a democracia frente a poderes antidemocráticos.

[9] Texto original: "El significado profundo de la democracia consiste en esta relación entre medios institucionales y fines sociales y en la consiguiente primacía de los derechos fundamentales sobre los poderes públicos".

ARTIGO III. 4 USO DE DADOS PESSOAIS COMO ESTRATÉGIA POLÍTICA E PREOCUPAÇÕES DEMOCRÁTICAS

A quantidade massiva de informações geradas pelos indivíduos e por eles recebidas permite afirmar que viver em uma sociedade sem filtros possa beirar ao caos informativo. Nos meios digitais essa afirmação é ainda mais perspicaz – estima-se que cerca de 45 Zettabytes (ZB) de dados foram produzidos em 2019 e que em 2025 esse número subirá para 175 ZB (REINSEL; GANTZ; RYDNING, 2020). Sendo assim, para que os conteúdos digitais sejam filtrados, utilizam-se algoritmos capazes de analisar grandes quantidades de dados e de selecionar o que aparecerá aos usuários.

Sem dúvida, filtros são necessários à organização das ideias e à tomada de decisões rápidas e assertivas – essenciais em tempos nos quais a fluidez rege as relações. Entretanto, percebe-se que a lógica algorítmica é, por vezes, obscura e apta a desfigurar a realidade. Vale mencionar que algoritmos nada mais são que instruções destinadas à solução de um problema, fundamentais à lógica e ao funcionamento de sistemas digitais. Registra-se a seguinte explicação:

> Em contato com um conjunto de dados, os algoritmos selecionam aqueles que foram definidos como úteis para a finalidade a que foram programados. Enquanto certos algoritmos atuam em busca de padrões, outros realizam uma sequência de operações mais simples. Muitos são exímios ordenadores e organizadores de hierarquias. Algoritmos podem ser determinísticos, probabilísticos, prescritivos, entre outras possibilidades de seu desenvolvimento. Servem como verdadeiros filtros informacionais (SILVEIRA, 2019, p.15).

Basicamente, para que a filtragem seja realizada, dados pessoais são coletados por meio do que é publicado, curtido ou compartilhado nas redes sociais e por meio de *cookies* de navegação instalados no computador ao vaguear pela internet. Desse modo, o algoritmo compreende os interesses particulares dos indivíduos e segmenta estes em públicos semelhantes a fim de personalizar o conteúdo que lhes será mostrado, priorizado e anunciado. Assim, cria-se um ambiente exclusivo, perfeito para mantê-los por mais tempo conectados à plataforma, dispondo de mais dados e propensos a adquirirem mais serviços ofertados (SILVEIRA, 2019, p.44).

Dessarte, a "bolha de filtros" cerca o usuário de tudo aquilo que ele aparentemente gosta, associando-o a uma identidade única com base em suas interações passadas. De maneira evidente, demonstra-se confortável a concepção de visualizar tão somente ideias, pessoas e interesses simpáticos, ficando longe de tudo

aquilo que é desagradável ou incompatível com valores particulares. Desse modo, confia-se na filtragem algorítmica, sem distinguir seu alcance – por vezes sem ao menos saber de sua existência - e sem suspeitar de sua tendente parcialidade. Contudo, como uma lente embaçada, a percepção da realidade pode ser facilmente distorcida por quem detenha o controle sobre os códigos algorítmicos (PARISER, 2012).

Assim sendo, o indivíduo, quando fornece dados pessoais à plataforma, permite que esta realize uma análise completa sobre sua personalidade. Os fins para os quais o perfil comportamental é usufruído são diversos: para selecionar o conteúdo que será visualizado pelos indivíduos, para auxiliar a plataforma no desenvolvimento de layouts e conteúdos relevantes aos usuários, para ofertar a empresas de marketing segmentado, dentre outros. Habitualmente, as plataformas que coletam dados são gratuitas e cobertas por anúncios. Por vezes, para se ver livre de anúncios, o usuário precisa pagar pela versão *premium*. Logo, não é à toa que dados pessoais se tornaram um dos capitais mais rentáveis atualmente: são eles que remuneram os serviços prestados pelas plataformas digitais (PARISER, 2012).

O capitalismo de plataforma[10] que opera nas redes permite que dados coletados sejam vendidos como produtos a anunciantes ou a quem possua poder econômico e esteja interessado em persuadir determinado grupo. Já se tornou comum entrar em uma página da web e visualizar inúmeros anúncios baseados em navegações de outros sites, em localização e, até mesmo, em conversas de voz captadas pelo celular. Dessa forma, por vezes, já não se tem a plena consciência entre o que é consumido advindo de necessidades e interesses próprios do que é comprado ou utilizado nas redes por influência da visualização de reiterados anúncios.

Nesse sentido, é comum que a maioria das práticas envolvendo coleta e disseminação de informações utilize *bots* (robôs, em inglês), que são programas que visam automatizar tarefas. Destarte, além de serem capazes de coletar e inspecionar dados pessoais, os *bots* podem ser utilizados para aumentar o engajamento de postagens e espalhar desinformação. Além disso, muito embora existam tecnologias que busquem impedir a ação de *bots* maliciosos, estes são cada vez mais aprimorados com técnicas que os camuflam nas redes (FORNASIER, 2020).

Sob esse viés, aplicando tal lógica ao cenário político, é possível perceber o risco democrático envolvido – seja durante o período eleitoral ou fora deste. Sabe-se que atualmente existem milícias digitais formadas por gabinetes políticos e apoiadores que utilizam *bots* de contas automatizadas e de disparo em massa de mensagens. Com

[10] Termo que ganhou contornos mais definidos a partir da obra de Nick Srnicek, "Platform Capitalism". Substancialmente, refere-se ao novo arranjo capitalista proporcionado pela tecnologia, o qual tem como cerne a utilização de plataformas que - em troca da oferta de serviços - aufiram lucros com o monopólio, a extração e a análise de grandes quantidades de dados por elas registrados (SRNICEK, 2016, p.34-36).

isso, fomentam campanhas de autopromoção e de ataques a opositores, recorrendo a estratégias que se utilizam de *fake news e* de *bots* para impulsionar o engajamento nas postagens e alcançar um número maior de indivíduos (LOBO; DE MORAIS; NEMER, 2020). Assim sendo, "os robôs podem dar a impressão de que uma informação é altamente importante, precisa, difundida e endossada por muitas pessoas, influenciando o comportamento dos usuários de mídia social" (FORNASIER, 2020, p.16).

No Brasil, há indícios de que, já nas eleições de 2014, *bots* foram utilizados pelas campanhas de Dilma Rousseff, Eduardo Campos e Aécio Neves. Vislumbra-se que o partido deste último foi o que mais investiu em contas automatizadas nas redes sociais, desembolsando cerca de dez milhões de reais (ARNAUDO, 2017, p. 12-13). Nas eleições de 2018, há indícios de que apoiadores do, então candidato, Jair Bolsonaro contrataram serviços de disparos de mensagem e de ferramentas automatizadas. Além disso, há alegações de que foram adquiridos irregularmente cadastros de usuários e de que foram utilizados perfis falsos em redes sociais para promover a campanha presidencial (RUEDIGER, 2019, p.13). Há ainda vinculações a um suposto "gabinete do ódio", formado por assessores presidenciais, utilizado para comandar essas operações e para enfraquecer as instituições democráticas (MELLO, 2020).

Destaca-se que a legislação eleitoral brasileira, na Resolução TSE nº 23.551/178 e na Lei nº 9.504/97, traz regulamentação específica acerca das propagandas eleitorais que poderão ser difundidas na internet. Dessa forma, "apenas duas modalidades pagas de divulgação de propaganda eleitoral na internet são lícitas: o impulsionamento e o uso de links patrocinados" (RUEDIGER, 2019, p.10). Em ambas modalidades, a contratação não poderá ser feita por terceiros, mas tão somente pelos partidos ou candidatos políticos, devendo o conteúdo ser identificado como eleitoral e vinculado a um partido ou candidato específico – conforme previsão do art. 57-C, caput e §3º da Lei 9.504/97 (BRASIL, 1997). Todavia, há dificuldades em distinguir o que é propaganda eleitoral do que é conteúdo orgânico, referido como manifestações pessoais dos usuários – obstando muitas vezes a aplicação das regras eleitorais (RUEDIGER, 2019).

Além disso, embora não haja uma regulamentação específica acerca do uso de *bots*, o art. 57-B aduz não ser possível a utilização de ferramentas digitais não disponibilizadas pelo provedor. Por isso, entende-se que a aplicação de *bots* para fins eleitorais não é viável, uma vez que não é uma ferramenta posta à disposição pelo provedor – sendo sua utilização por vezes repudiada e combatida pelas plataformas (RUEDIGER, 2019). Ademais, o art. 57-B, §2º, prevê que é proibida a criação de perfis falsos nas redes para fins de veiculação de conteúdos de cunho eleitoral. Também, o art. 57-D enuncia não ser possível a divulgação de campanhas eleitorais de forma

anônima na internet (BRASIL, 1997). De fato, percebe-se que o impulsionamento online de campanhas políticas - para que seja condizente com as normas eleitorais - deve ser realizado de forma transparente e de forma harmônica às diretrizes de um sistema pautado na democracia.

Para além disso, embora partidos e candidatos políticos devam obedecer à LGPD, operam-se ocultamente algumas estratégias políticas envolvendo dados pessoais para influenciar possíveis eleitores: a) coleta de dados como ferramenta política para subsidiar métodos envolvendo mineração de dados, *bots*, etc.; b) utilização de dados como inteligência para interpretar as preferências dos eleitores de modo a adaptar estratégias de campanha; e c) utilização de dados como método de identificação de potenciais eleitores a fim de alcançá-los nas plataformas e, dessa forma, influenciá-los em seus votos. Outrossim, observa-se que a personalidade do cidadão interfere no método de abordagem a ser utilizado e se será empregue ou não. Dependendo do indivíduo, podem ser operados anúncios personalizados, e-mails e postagens direcionadas, mensagens de texto, dentre outros recursos tecnológicos (HANKEY; MORRISON; NAIK, 2019).

À vista disso, agregar análise comportamental de perfis e filtragem de conteúdo pode ser catastrófico quando se faz a análise sob a ótica eleitoral. Ao enxergar o mundo dentro da "bolha" tem-se apenas uma parte da realidade - por vezes distorcida: o que o algoritmo acredita ser interessante com base no perfil comportamental do indivíduo e o que os detentores de poder econômico acham por bem patrocinar. Por isso, espaços segmentados não estimulam a empatia e a discussão de ideias políticas, pelo contrário: estimulam a intolerância e a opressão. Nesse sentido, expõe Pariser:

> As notícias moldam a nossa visão do mundo, do que é importante, da escala, tipo e caráter dos problemas que enfrentamos. O mais significativo, no entanto, é o fato de nos darem a base das experiências e dos conhecimentos comuns sobre a qual se constrói a democracia. A menos que entendamos os grandes problemas de nossa sociedade, não conseguiremos agir juntos para resolvê-los (2012, p.38).

Sendo assim, muito embora não seja possível dominar todas as informações, é essencial que o cidadão ao menos saiba da existência de situações complexas que demandem da coletividade alguma ação ou sejam a ela pertinentes. A personalização com base nos dados pessoais dificulta o contato com situações desagradáveis, mas que merecem atenção – como por exemplo, índices de pobreza, violência urbana, casos de corrupção, etc. Significa dizer que, quando se enxerga apenas uma amostra da

realidade, não se tem consciência do todo. Além disso, “é impossível sabermos o quanto uma amostra é parcial se examinarmos apenas a amostra” (PARISER, 2012, p. 74).

Dessa forma, a personalização das plataformas interfere no modo como o cidadão vê a realidade, afetando substancialmente sua decisão eleitoral. Para que um cidadão seja ativo em uma democracia, é necessário que possua conhecimento sobre o que está acontecendo na sociedade. A “bolha de filtros” aprisiona o indivíduo dentro de suas ideias, sendo inclinado a acreditar em informações que consolidam suas crenças pessoais, fechando-se a novas concepções de mundo (PARISER, 2012, p. 59-60).

Além disso, de forma inconsciente, a repetição de uma ideia faz com que o indivíduo a internalize e passe a aceitá-la como verdade. Assim, visualizar inúmeras vezes publicações de candidatos infladas por *bots*, mensagens repetitivas no *WhatsApp* e anúncios em diversos locais da rede podem ter forte influência na modulação da opinião política. Para o cérebro humano, “quanto mais pessoas relatam a mesma coisa, mais credível e provável que uma informação seja” (FORNASIER, 2020, p.19).

Nota-se que a internet, em sua concepção inicial, demonstrava-se um local democrático, onde todos poderiam expor suas opiniões de forma igual, e que essas informações chegariam a todos sem distinções. Entretanto, não é o que se vê. Atualmente, a internet se tornou um local segmentado, no qual expor e entrar em contato com diferentes realidades se revela improvável. Não obstante, a imagem de um ambiente democrático é utilizada como estratégia de venda aos usuários, que acreditam na falácia ofertada sem notar que estão cada vez mais segmentados em “bolhas” e propensos a serem induzidos a uma visão irreal de mundo.

À luz disso, a percepção de uma “*fake* democracia” deve-se predominantemente ao fato de que não há transparência quanto aos algoritmos utilizados pelas plataformas e ao fato de que o ambiente digital, por vezes gerenciado por inteligência artificial (IA), dificulta a prestação de contas sobre o que foi realizado e eventual responsabilização dos infratores (*accountabillity*) (MENEZES NETO et al., 2018, p.4). Além do mais, “empresas que desenvolvem softwares e algoritmos alegam que eles não podem ser abertos nem transparentes, uma vez que elas precisam proteger seus segredos de negócios e sua propriedade intelectual diante de concorrentes” (SILVEIRA, 2019, p.19). Também, como as plataformas são utilizadas em escala global, frequentemente não se submetem às determinações de jurisdição nacional.

Outrossim, há incompreensibilidade (e até desconhecimento) quanto às decisões algorítmicas por grande parte da sociedade. Mais que isso: quando são utilizadas tecnologias de IA, como *machine learning* e *deep learning*, o algoritmo aumenta sua complexidade, visto que estabelece aprendizado com base nas ações dos usuários, alterando-se a partir dessas – o que pode dificultar inclusive a compreensão do código pelos programadores. Desse modo, postagens em que haja muito engajamento, como, por exemplo, notícias sensacionalistas, têm mais chances de serem amplificadas aos usuários. Logo, quanto mais o algoritmo é executado mais se torna obscuro, sendo capaz de possuir vieses, ou seja, tendências a certas ações com base em como foi projetado e em como os usuários interagiram – podendo, até mesmo, adquirir características discriminatórias (SILVEIRA, 2019, p. 48-49).

Nesse sentido, demonstra-se substancialmente antidemocrático a imagem de um poder invisível operando nos meios digitais. Nos Estados Democráticos, há uma relação de dependência entre a opinião pública e a visibilidade dos atos daqueles que detêm o poder (BOBBIO, 1986, p. 88-89). Sob essa perspectiva, a transparência, essencial ao controle democrático, não é identificada nos códigos comandados pelos poderes invisíveis - por vezes centralizados a empresas privadas, como Facebook e Amazon. Há então uma visão assimétrica da realidade, na qual se revela apenas o que interessa aos detentores de poder e não aos cidadãos (MENEZES NETO, et al., 2018).

Desse modo, a possibilidade deliberativa, inerente à democracia, é corrompida pela manipulação das opções disponíveis no ambiente digital. Com efeito, a democracia só funciona quando existem cidadãos aptos a deliberar sobre questões atinentes à sociedade em que coabitam - e não somente sobre interesses individuais. Para que isso aconteça, são necessários espaços nos quais a pluralidade de ideias possa fluir – espaços onde sejam visualizados diferentes grupos e realidades, permitindo o verdadeiro debate entre opiniões.

Nesse contexto, recepciona-se a figura do pluralismo político, um dos fundamentos da República brasileira (art. 1, V, CF/88) e elemento indispensável à democracia. A liberdade do dissenso, fruto do pluralismo - conforme ensina Norberto Bobbio (1986, p. 61-63) - é característica fundamental dos regimes democráticos. Segundo ele, o consenso real entre os cidadãos em uma democracia é apenas visível se o dissenso for manifestamente livre, ou seja, quando ideias opostas puderem ser vistas e debatidas. Dessa forma, a tomada de decisões conjuntas correlaciona-se e subordina-se à união de diferentes opiniões. Nesse sentido:

> O pluralismo político, necessário para os regimes democráticos, só pode ser obtido através da fertilização cruzada de ideias. Esse nível de interação com o outro se torna extremamente difícil sem uma visão de mundo

> compartilhada, conhecendo o outro e as suas necessidades. O que ocorre é exatamente o contrário, ou seja, o filtro-bolha cria a ilusão de que os interesses do indivíduo correspondem à totalidade do mundo (MENEZES NETO, et al., 2018, p.17).

Intrinsecamente a esse fundamento, de modo a garanti-lo, deve-se assegurar a plena liberdade do indivíduo em todas as suas acepções, principalmente no que tange à liberdade de expressão e informação (PEIXOTO, 2019). O debate de ideias só funciona quando os cidadãos são livres para receber informações e livres para expor suas ideias a partir do que foi recebido. Os algoritmos interferem em ambas liberdades, pois dificultam o livre acesso de informações entre os indivíduos, interferindo também em sua liberdade de escolha. De fato - ao enxergarem a realidade de forma parcial – não captam a complexidade dos problemas inerentes à sociedade e podem estar sendo manipulados a uma visão parcial, tendenciosa.

Ademais, destaca-se que:

> Tão importante quanto a liberdade de expressão é a liberdade de visualização. Todas as pessoas têm o direito de ver, ler e ouvir conteúdos políticos sem que sejam filtrados por algoritmos cujos critérios e parâmetros de operação são ocultados ou ofuscados pelas plataformas onde ocorrem os debates públicos (SILVEIRA, 2019, p.44).

Nota-se que a democracia é consubstanciada pela participação popular e pela livre escolha de governantes, traduzida pela autonomia política. A “bolha de filtros”, além de afetar a autonomia privada, referente à autodeterminação do indivíduo - a qual dá a este o controle sobre suas decisões -, prejudica a autonomia política; ou seja, a participação nas decisões legislativas de forma plural e livre de interferências (PILAU SOBRINHO; SANTOS, 2014). Como ambas as autonomias são recíprocas e essenciais à manutenção de um sistema democrático, ao prejudicá-las, retirando o poder conferido à população de decidir sobre seus governantes, fere-se a democracia em seu cerne.

Outrossim, a obscuridade dos códigos faz com que o sistema democrático e suas instituições sejam vistos com desconfiança. Quando existem poderes invisíveis operando, os indivíduos tendem a acreditar que suas escolhas políticas pouco importam, que suas vozes não serão ouvidas por refletirem a minoria ignorada pelos filtros e que não haverá de fato legitimação no poder político representativo. Assim, ao crer que as regras democráticas não estão sendo respeitadas, os valores

democráticos[11] perdem força. Por consequência, a democracia é ameaçada – fortalecendo o surgimento de poderes autoritários.

Dessa maneira, entende-se que:

> A construção da democracia reivindica a transparência do poder das instituições e dos seus mecanismos fundamentais, mas isso não é suficiente. É improvável que a democracia consiga se consolidar e existir se a maioria das pessoas não acreditar nos valores democráticos. Democracia não é apenas o governo da maioria. A democracia exige o respeito às minorias (SILVEIRA, 2019, p.40).

Sob esse viés, muito embora não seja simples, a transparência nos meios digitais denota-se elementar à manutenção da democracia. Para que isso aconteça, cabem às empresas e ao governo ações que tornem as plataformas mais transparentes, no sentido de que sejam demonstrados quais filtros estão sendo utilizados, quais dados foram analisados para chegar neles e por que estão sendo aplicados. Também, o controle sobre os filtros deve ficar com quem possui o maior interesse na plataforma: o usuário. Dessa forma, será possível conferir a este maior autonomia e gerência sobre os algoritmos que utilizam seus dados pessoais (PARISER, 2012, p. 155-156).

À luz disso, é cada vez mais essencial que os indivíduos entendam como funcionam os sistemas digitais, para que estejam aptos a escolher sites e aplicações que os deem "mais controle e visibilidade sobre como funcionam seus filtros e como eles utilizam as nossas informações pessoais" (PARISER, 2012, p.152). A esse propósito, demonstra-se necessária uma verdadeira educação digital aos cidadãos e, até mesmo, aos representantes eleitos, para que entendam as demandas oriundas dos meios digitais e estejam aptos a legislar e a executar ações hábeis a proteger os indivíduos nas redes.

Nessa acepção, os indivíduos precisam enxergar seus dados pessoais como atributos individuais, de sua propriedade, e perceber que estes estão sendo utilizados indistintamente. Diante disso, ainda que existam leis que proíbam a utilização não consentida de dados, sabe-se que a corrupção de dados é realizada às escuras, por trás dos códigos. Logo, o consentimento dado às plataformas para que utilizem dados pessoais é por vezes desconsiderado, inexistente e/ou coercitivo. Não traduz, na

[11] " Os valores democráticos contemporâneos, além do respeito às decisões da maioria, ou seja, da autonomia e da soberania popular, incorporam um conjunto de liberdades, sem as quais a democracia não pode existir [...]. Um dos elementos indispensáveis às democracias contemporâneas é a garantia da diversidade e das diferenças culturais, de gênero, ideias, religiões, entre outras" (SILVEIRA, 2019, p.41).

maioria, a vontade do usuário, mas sim a necessidade social de utilização das plataformas. Fora isso, existem tecnologias, como *spywares e spams*, que são utilizadas para furtar dados e vendê-los clandestinamente – o que torna o ambiente digital ainda mais inseguro (PARISER, 2012, p. 144-145).

Por essa razão, soluções tecnológicas precisam continuar sendo desenvolvidas a fim de redemocratizar as redes. As atuais alternativas compreendem tecnologias envolvendo criptografia, método que pode auxiliar na segurança de dados, ferramentas informatizadas que sejam céleres ante a suspeita da utilização clandestina de dados pessoais e hábeis a desmantelar "bolhas de filtros", *bots* e perfis comportamentais não consentidos, além da implementação da Autoridade Nacional de Proteção de Dados, a fim de fiscalizar as operações envolvendo tratamento de dados pessoais. Ademais, ressalta-se que o problema envolvendo proteção de dados não é meramente técnico, mas sim social: falta ética nas relações, principalmente por parte de políticos mal-intencionados que se aproveitam da psique humana em suas estratégias políticas (FORNASIER, 2019).

De todo modo, a reflexão que aqui se faz não tem o intuito de desencorajar o uso das tecnologias. Pelo contrário, suas ferramentas devem ser bem usufruídas pelos indivíduos. No entanto, seu uso deve se dar de modo responsável e transparente - tanto por parte do governo quanto por parte dos indivíduos e das empresas que comandam as plataformas digitais. O olhar crítico frente às tecnologias demonstra-se substancial em uma sociedade na qual o termo de uso é aceito sem avaliar suas condições. O que está em jogo não é somente o dissabor de vislumbrar anúncios persuasivos ou não visualizar as publicações de alguém, mas o enfraquecimento causado na democracia quando as "bolhas" que segmentam os cidadãos os afastam de sua própria governança e os tornam vulneráveis a poderes invisíveis.

ARTIGO IV.

ARTIGO V. 5 CONCLUSÃO

O cenário tecnológico atual, marcado pela disposição e pelo consumo de dados, traz consigo discussões acerca dos fins atribuídos aos meios digitais. No presente artigo, questionou-se, especificamente, a relevância democrática da proteção dos dados pessoais digitais no contexto de sua utilização como estratégia política. Tal qual já consubstanciado, dados pessoais digitais são mais do que rastros cibernéticos: revelam elementos característicos de seus titulares. Por isso, atinente à tutela da pessoa, a proteção específica aos dados pessoais digitais agrega-se aos direitos de

personalidade, de modo a fortalecer o sistema protetivo a garantias já solidificadas, como dignidade e privacidade. Conforme se pode vislumbrar com os casos narrados sobre violações a dados pessoais - os quais tiveram como fim ilustrar de forma realista situações democraticamente preocupantes -, a proteção vindicada é essencial para que os dados pessoais não sejam explorados de forma inconsequente.

Sob essa perspectiva, é indispensável que o Direito constantemente se adapte às inovações tecnológicas a fim de contemplar em seu bojo situações jurídicas advindas do uso das redes. Especialmente no que tange à utilização de dados pessoais, analisou-se algumas das principais normas atinentes ao tema (Código de Defesa do Consumidor, Marco Civil da Internet, Lei Geral de Proteção de Dados Pessoais, art. 5º, X, XII, LXXIII e LXXIX da Constituição Federal). Assim, pode-se constatar que as disposições mencionadas convergem no sentido de integrar o direito fundamental à proteção de dados pessoais no sistema jurídico brasileiro.

Diante disso, muito embora o ordenamento se encaminhe a um protótipo sofisticado no que se refere à proteção de dados pessoais, está longe de ser o ideal. Nesse sentido, as recentes mudanças trazidas pela LGPD, principalmente no que concerne à regulamentação sobre transparência e segurança no tratamento de dados, à imposição de sanções administrativas e à instituição da ANPD, contribuirão para que inúmeros abusos nas redes sejam evitados. Destaca-se também a incorporação, no sistema protetivo atual, do direito fundamental à proteção de dados pessoais, pela Emenda à Constituição nº 115/2022. Com efeito, sua corporificação traz - além de um novo amparo aos indivíduos contra violações cometidas nas redes - um novo alicerce a sustentar a democracia frente a poderes antidemocráticos.

Destarte, ante a insuficiência de métodos hábeis a proteger os dados pessoais, estes são utilizados na formação de perfis comportamentais de indivíduos - de modo a viabilizar a filtragem de conteúdo conforme sua personalidade. Nota-se que essa atividade não se limita a fins lucrativos advindos da venda de dados por empresas privadas a anunciantes - sua utilização vem sendo agregada às estratégias políticas de candidatos e representantes. Assim, são utilizados subterfúgios cujo objetivo é

influenciar eleitores a apoiar (ou não) determinado candidato ou campanha, procedendo-se frequentemente de forma clandestina - o que faz com os indivíduos estejam constantemente propensos a serem controlados por poderes invisíveis.

À luz de tudo disso, defronte ao cerne do problema inquirido, a relevância democrática da proteção de dados pessoais digitais no contexto de sua utilização como estratégia política encontra-se na constatação da atual insuficiência dos meios legais protetivos. Assim, em que pesem as recentes medidas legislativas referentes a dados pessoais, o quadro normativo não se verifica hábil a proteger de modo eficaz os indivíduos nos meios digitais, ou seja, não enfrenta todos os problemas advindos do uso de dados pessoais digitais como estratégia política. Tal situação gera impactos no sistema democrático, notadamente: a) enfraquecimento do pluralismo político, diante da manipulação das opções disponíveis no ambiente digital; b) retração da liberdade de expressão, de informação e de escolha, frente aos obstáculos impostos à livre disposição e ao livre recebimento de conteúdo; c) mitigação da autonomia privada e política, pelo fato de deturpar a autodeterminação do indivíduo e a livre escolha de governantes; e d) desconfiança dos cidadãos na própria democracia, ante a crença de que as regras democráticas não estão sendo respeitadas.

6 REFERÊNCIAS

ARNAUDO, Dan. Computational Propaganda in Brazil: Social Bots during Elections. **Project on Computational Propaganda.** Oxford, UK. ago. 2017. Disponível em: https://comprop.oii.ox.ac.uk/research/computational-propaganda-in-brazil-social-bots-during-elections/. Acesso em: 5 out. 2020.

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

BOBBIO, Norberto. **O futuro da democracia:** uma defesa das regras do jogo. Tradução de Marco Aurélio Nogueira. Rio de Janeiro: Paz e Terra, 1986.

BOLESINA, Iuri; GERVASONI, Tássia A. Responsabilidade civil por violação do direito à extimidade. In: **Congresso Internacional de direito e contemporaneidade: mídias e direitos da sociedade em rede**, 5., 2019, Santa Maria. Anais [...]. Santa Maria: UFSM, 2019. p. 1-17. Disponível em: https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/wp-content/uploads/sites/563/2019/09/5.7.pdf . Acesso em: 4 out. 2020

BRASIL. Constituição (1998). **Constituição da República Federativa do Brasil.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 dez. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 27 abr. 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 ago. 2020.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências.** Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 31 ago. 2020.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. **Estabelece normas para as eleições.** Diário Oficial da União, Brasília, DF, 30 set. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 4 out. 2020.

CADWALLADR, Carole. **The Vote Leave scandal, one year on: 'the whole thing was traumatic'**. 2019. Disponível em: https://www.theguardian.com/uk-news/2019/mar/17/vote-leave-scandal-one-year-on-shahmir-sanni-whistleblower-cambridge-analytica. Acesso em: 12 mai. 2020.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. 7. ed. Coimbra: Almedina, 2003.

DAVIES, Harry Fox. **Ted Cruz using firm that harvested data on millions of unwitting Facebook users.** 2015. Disponível em: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data. Acesso em: 12 maio 2020.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. V.2. Brasília: SDE/DPDC, 2010.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Joaçaba, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 23 maio 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019.

FERRAJOLI, Luigi. **La democracia a través de los derechos:** El constitucionalismo garantista como modelo teórico y como proyecto político. Tradução de Perfecto Andrés Ibáñez. Madrid, ES: Trotta, 2014.

FORNASIER, Mateus de Oliveira. O uso de bots sociais como ameaça à democracia. **Revista Brasileira de Políticas Públicas**, [S.L.], v. 10, n. 1, p. 13-30, 4 jun. 2020. Centro de Ensino Unificado de Brasilia. http://dx.doi.org/10.5102/rbpp.v10i1.6453. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/6453. Acesso em: 4 out. 2020.

GATEFY. **Como funcionam as leis de proteção de dados nos Estados Unidos**. 2020. Disponível em: https://gatefy.com/pt-br/postagem/como-funcionam-leis-protecao-dados-estados-unidos/ Acesso em: 10 maio 2020.

HANKEY, Stephanie; MORRISON, Julianne Kerr; NAIK, Ravi**. Data and Democracy in the Digital Age**. Londres: The Constitution Society, 2018.

ISAAK, Jim; HANNA, Mina J. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. **Computer**, [S. l.], v. 51, n. 8, p. 56–59, 2018. DOI: 10.1109/MC.2018.3191268.

KEMP, Simon. Digital 2019: Brazil. **Datareportal**, 2019. Disponível em: https://datareportal.com/reports/digital-2019-brazil. Acesso em: 26 abr. 2020.

LOBO, Edilene; MORAIS, José Luis Bolzan de; NEMER, David. Democracia Algoritmica: o futuro da democracia e o combate às milícias digitais no brasil. **Culturas Jurídicas**, [S.L], v. 7, n. 17, p. 255-276, ago. 2020. Disponível em: https://periodicos.uff.br/culturasjuridicas/article/view/45443. Acesso em: 4 out. 2020.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de *enforcement*. **Revista do programa de direito da União Europeia.** v. 1, p. 39-52, 2021. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/article/view/83423. Acesso em 7 dez. 2022.

MACASKILL, Ewen; DANCE, Gabriel. **NSA files: decoded**: what the revelations mean for you. 2013. Disponível em: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Acesso em: 8 maio 2020.

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

MARCONI, M. D. A; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

MELLO, Patrícia Campos. **Por que os brasileiros deveriam ter medo do gabinete do ódio**. The New York Times. São Paulo. 4 ago. 2020. Disponível em: https://www.nytimes.com/pt/2020/08/04/opinion/international-world/bolsonaro-gabinete-do-odio.html. Acesso em: 4 out. 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**. vol. 120. ano 27. p. 469-483. São Paulo: Thomson Reuters Brasil, 2018.

MENEZES NETO, Elias Jacob de; et al. Accountability, transparência e assimetria das relações de visibilidade virtuais: análise dos aspectos antidemocráticos das novas tecnologias da informação e comunicação a partir da ideia de filtro bolha. **Direito, Estado e Sociedade**, Rio de Janeiro, v. 53, p. 62-87, dez. 2018. Disponível em: https://revistades.jur.puc-rio.br/index.php/revistades/article/view/886. Acesso em: 4 out. 2020.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**. Vitória, v. 19, n. 3, p. 159-180, 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 31 ago. 2020.

O que são dados pessoais, segundo a LGPD. Serpro, 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd. Acesso em: 26 abr. 2020.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

PEIXOTO, Geovane. Pluralismo Político e Liberdade de Expressão**:** A Concretização da Democracia substancial pela Salvaguarda dos Direitos Fundamentais. In Direito Unifacs – **Revista Debate Virtual**, n. 225, março de 2019. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/5947. Acesso em: 4 out. 2020.

PILAU SOBRINHO, Liton Lanes; SANTOS, Rafael Padilha dos. A autonomia privada e a autonomia pública no pensamento de Jurgen Habermas. **Revista Direitos Culturais**, Santo Ângelo, v. 8, p. 15-31, 2014. Disponível em: http://srvapp2s.santoangelo.uri.br/seer/index.php/direitosculturais/article/view/1320/616. Acesso em: 24 maio 2020.

PRIVACIDADE Hackeada. Direção de Karim Amer e Jehane Noujaim. Produção de Karim Amer, Geralyn Dreyfus e Judy Korin. Estados Unidos: Netflix, 2019. 114 min. Disponível em: https://www.netflix.com/br/title/80117542. Acesso em: 23 maio 2020.

REINSEL, David; GANTZ; John; RYDNING; John. **The Digitization of the World**: From Edge to Core. IDC White Paper. Massachusetts, US. mai. 2020. Disponível em: https://www.seagate.com/files/www-content/our-story/trends/files/dataage-idc-report-final.pdf. Acesso em: 5 out. 2020.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: privacidade hoje, Rio de Janeiro: Renovar, 2008.

RUEDIGUER, Marcos (Coord.). **Bots e o Direito Eleitoral brasileiro nas Eleições de 2018.** Rio de Janeiro: FGV, DAPP, 2019. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/26227. Acesso em: 4 out. 2020.

SANTOS, Pedro Miguel Pereira. **Internet das Coisas**: o desafio da privacidade. 2016. Dissertação (Mestrado em sistemas de informação organizacionais) - Escola Superior de Ciências Empresariais, Instituto Politécnico de Setúbal, Setúbal, 2016.

SILVEIRA, Sergio Amadeu da; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, [S. l.], v. 12, n. 1, p. 217–230, 2017. DOI: 10.22478/ufpb.1981-0695.2017v12n1.34409.

SILVEIRA, Sergio Amadeu da. **Democracia e os códigos invisíveis:** como os algoritmos estão modulando comportamentos e escolhas políticas. São Paulo: Sesc São Paulo, 2019.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s**: redes digitais, privacidade e venda de dados pessoais. São Paulo: Sesc São Paulo, 2017.

SRNICEK, Nick Srnicek. **Platform Capitalism.** Cambridge, UK: Polity Press, 2016.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

Como citar:
ANDRIOLI, Elisangela Maria. GERVASONI, Tássia Aparecida. Dados pessoais digitais e medidas legais de proteção: preocupações democráticas acerca da utilização de dados pessoais digitais como estratégia política. **Revista do Programa de Pós-Graduação em Direito**, Salvador-ba, (v.32/2022), número (p.1-33). Data de publicação 25/12/2022. DOI: (endereço do DOI desse artigo). Disponível em: endereço eletrônico. Acesso em: xx mês abreviado. xxxx.

Originais recebido em: 19/12/2020.
Texto aprovado em: 04/11/2022.