

# OS LIMITES DO CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS E A PRIVACIDADE DOS TITULARES DE DADOS SOB A PERSPECTIVA DA MERCANTILIZAÇÃO DE DADOS

Caroline Albuquerque Gadêlha de Moura<sup>1</sup>

Maria Marconiete Fernandes Pereira<sup>2</sup>

Resumo: A era digital transformou profundamente a forma como as pessoas vivem, interagem e compartilham informações. Nesse contexto, a mercantilização de dados emergiu como uma questão crucial, levantando preocupações sobre a proteção dos dados pessoais e a privacidade. A expansão tecnológica e a grande produção e compartilhamento de dados no mundo virtual, fez surgir a necessidade de regulamentação da matéria de proteção de dados, com a finalidade de preservar os direitos dos titulares que têm seus dados circulando no ambiente digital. Nessa conjuntura, foi instituída a Lei nº 13.709 de 2018, uma legislação brasileira que estabelece diretrizes para o tratamento adequado e consentido de dados pessoais. Deste modo, a presente pesquisa tem por objetivo geral investigar os limites do consentimento do titular de dados, consagrados na referida Lei, como instrumento de garantia da proteção à privacidade, no

---

<sup>1</sup> Mestranda em Direito e Desenvolvimento Sustentável pela UNIPÊ- Centro Universitário de João Pessoa. Graduada em Direito pela Universidade Federal da Paraíba (UFPB). Advogada e Técnica Administrativa da Universidade Estadual da Paraíba (UEPB).

<sup>2</sup> Doutora em Direito pela Universidade Federal de Pernambuco (UFPE). Mestre em Ciências Jurídicas pela Universidade Federal da Paraíba (UFPB). Professora do Programa de Pós Graduação em Direito/Mestrado e da Graduação em Direito do Centro Universitário de João Pessoa/PB (UNIPÊ). Professora da Graduação em Direito da Faculdade Internacional Cidade Viva (FICV). Auditora de Contas Públicas/CGE/PB.

cenário de mercantilização de dados. Para tanto, será adotada uma abordagem dedutiva, realizando-se pesquisa de natureza qualitativa, com método descritivo e exploratório e procedimento bibliográfico e documental. A compreensão dessa questão visa garantir uma abordagem legalmente adequada no uso, compartilhamento e mercantilização de dados na era digital, frente a necessidade de garantir direitos fundamentais do usuário, como o direito Constitucional à privacidade.

Palavras-Chave: Mercantilização de Dados. LGPD. Consentimento. Privacidade.

## THE BOUNDARIES OF CONSENT IN THE GENERAL DATA PROTECTION LAW AND THE PRIVACY OF DATA SUBJECTS UNDER THE PERSPECTIVE OF DATA COMMERCIALIZATION

Abstract: The digital era has profoundly transformed the way people live, interact, and share information. In this context, data commodification has emerged as a crucial issue, raising concerns about personal data protection and privacy. Technological expansion and the large production and sharing of data in the virtual world have given rise to the need to regulate the matter of data protection, with the aim of preserving the rights of holders who have their data circulating in the digital environment. At this juncture, Law No. 13.709 of 2018 was established, a Brazilian legislation that establishes guidelines for the adequate and consented processing of personal data. Therefore, the general objective of this research is to investigate the limits of the data subject's consent, enshrined in the aforementioned Law, as an instrument to guarantee privacy protection, in the scenario of data commodification. To this end, a deductive approach will be adopted, carrying out qualitative research, with a descriptive and exploratory method and bibliographic and documentary

procedure. Understanding this issue aims to ensure a legally adequate approach to the use, sharing and commodification of data in the digital era, given the need to guarantee fundamental user rights, such as the Constitutional right to privacy.

Keywords: Data Commoditization. LGPD (Brazilian General Data Protection Law). Consent. Privacy.

## 1 INTRODUÇÃO



acelerado desenvolvimento tecnológico vem ocasionando alterações em diversos aspectos da vida social, modificando hábitos e incluindo cada vez mais a tecnologia da informação na vida cotidiana. No entanto, embora o acesso à essas tecnologias e ao mundo virtual tenha propiciado inúmeros benefícios nas esferas econômica, social e da comunicação, também fez surgir novos problemas e dilemas para o mundo jurídico.

Na realidade, os recentes avanços tecnológicos impulsionaram o surgimento de outros modelos de negócio jurídico, que operam e monetizam novas atividades econômicas e novas oportunidades para obtenção de lucro (Guimarães Filho; Ferneda; Ferraz, 2020). Consequentemente, as tecnologias emergentes aproximaram o usuário à oferta de diferentes bens e serviços virtuais, como é o caso das redes sociais, implicando na constante troca de informações (dados) nos ambientes virtuais.

Tal cenário de produção e compartilhamento de dados na sociedade da informação, à medida que possibilitou maior facilidade na vida cotidiana, também inseriu dificuldades no âmbito de defesa ao titular de dados, tornando-o vulnerável, posto que, para a obtenção de permissão para utilização de plataformas virtuais (redes sociais, bancos digitais, jogos, plataformas de *streaming* de vídeo e música, dentre outros), passou a ser frequente a prática de fornecer e consentir com o tratamento dos dados

personais (Yandra; Silva; Santos, 2020).

Nesse contexto, emergiu a indústria bilionária de mineração de dados, que possibilitou maior amplitude de poder e controle aos detentores dos dados, sendo a informação utilizada para influenciar o usuário, interferindo no livre desenvolvimento de sua personalidade, transformando o usuário (titular de dados) em um produto. Cabe ressaltar que essa indústria é praticamente universal e se operacionaliza por meio da abertura da privacidade e a captura dos dados pessoais de usuários (Guimarães Filho; Ferneda; Ferraz, 2020). Esse mercado de comportamentos futuros, que comercializa produtos de predição, fazem parte do denominado capitalismo de vigilância (Zuboff, 2021).

Dessa conjuntura de vigilância descentralizada, com múltiplos atores envolvidos no processamento de dados, conforme descreve Bioni (2019), sobreveio a necessidade de regulamentação das atividades de coleta, tratamento, armazenamento e descarte de informações, realizadas por pessoa natural ou por pessoa jurídica de direito público ou privado, com a finalidade de preservação dos direitos fundamentais da personalidade, privacidade e liberdade dos usuários (Ferreira; Araújo, 2020). Foi justamente por essa necessidade de regulamentar a proteção dos dados, que foi institucionalizada a Lei Geral de Proteção de Dados.

Apesar do tema acerca da proteção de dados já ser tratado de maneira indireta em legislações esparsas como o Código de Defesa do Consumidor (Lei nº 8.078/90), a Lei do Habeas Data (Lei n.º 9.507/1997), a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet (Lei nº 12.965/2014), entre outras, havia uma omissão legislativa sobre a matéria no Brasil, ou seja, não existia um regulamento específico acerca da questão da proteção de dados, notadamente no âmbito virtual, o que colocou em evidência a importância de se ter uma legislação própria.

Na realidade, para possibilitar uma resposta adequada às

novas demandas sociais relacionadas com a revolução tecnológica, é essencial que a Teoria do Direito se renove e se reconstrua, permitindo a compreensão e a entrega de soluções para os novos problemas. Nesse sentido, o presente estudo tem como foco o advento da Lei n. 13.709, de 12 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD) e que se apresenta como a mais recente resposta do Direito à proteção de dados pessoais dos usuários da rede no Brasil.

Desta feita, segundo Pereira e Medeiros (2023), o ordenamento jurídico-constitucional brasileiro estabelece o liame do direito de proteção dos dados pessoais com os consignados nos ordenamentos jurídicos contemporâneos, por meio da proposição da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que inseriu no art. 5º o inciso LXXIX, incluindo a proteção de dados no rol dos direitos e garantias fundamentais, dispondo então: “assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (Brasil, 2023).

Ao buscar equilibrar a necessidade de proteção de dados, compreendido como um aspecto da personalidade do indivíduo, e o dinamismo econômico imperativo à inovação e à competitividade, a LGPD trouxe inúmeros desafios às organizações empresariais que atuam na esfera dos dados pessoais, bem como ao Governo e aos juristas. Visando fortalecer a autodeterminação informacional do titular de dados, a referida legislação deu um lugar de destaque ao consentimento, como uma das hipóteses legais que daria ensejo ao tratamento de dados.

Nesse sentido, o problema de pesquisa a ser abordado neste projeto requer um diálogo constante entre o Direito e a Tecnologia. Desse modo, diante das constatações já descritas, surgiu a seguinte problemática: O consentimento do titular, nos moldes previstos pela LGPD, se constitui como limite protetivo suficiente para garantir a proteção da privacidade do titular de dados frente à mercantilização de dados?

Em suma, tem-se por objetivo geral investigar a

disciplina da proteção de dados pessoais no Brasil, frente aos novos desafios impostos ao Direito pelo desenvolvimento de novas tecnologias da informação e comunicação, sobretudo quanto aos limites do consentimento previsto na LGPD, abordando-se, inicialmente a sociedade da informação, na qual os dados pessoais tornaram-se uma mercadoria valiosa para a prática empresarial, acarretando a vulnerabilidade do usuário e a necessidade da proteção de dados como forma de assegurar o Direito Constitucional à Privacidade.

O desenvolvimento do estudo está dividido em três capítulos. No primeiro capítulo, será analisada as características da Sociedade de Informação e o cenário da Mercantilização de Dados. No segundo capítulo será investigado o processo de institucionalização da LGPD no Brasil e seus principais aspectos. Por fim, no terceiro capítulo, será explorada a LGPD no tocante aos limites do consentimento do titular de dados, como limite garantidor da proteção da privacidade, sob a ótica da mercantilização de dados. No que se refere à metodologia abordada, será adotada uma abordagem dedutiva, realizando-se pesquisa de natureza qualitativa, com método descritivo e exploratório e procedimento bibliográfico e documental.

## 2 A SOCIEDADE DA INFORMAÇÃO E O CENÁRIO DO MERCANTILISMO DE DADOS

O avanço tecnológico é uma realidade que integra a evolução da sociedade. Dessa forma, ao longo dos anos, a tecnologia permeou por diversos setores, trazendo profundas transformações nas relações sociais, econômicas e políticas. Nesse contexto, Schwab (2018) defende a existência de uma Quarta Revolução Industrial, por observar características que a distinguiria da Terceira Revolução Industrial: velocidade (evolução exponencial); amplitude e profundidade (revolução digital como base, combinando várias tecnologias e levando a mudanças de

paradigmas nos mais diversos setores); impacto sistêmico (envolve transformação de sistemas inteiros entre países e dentro deles). Assim, a Quarta Revolução não seria apenas sobre sistema e máquinas inteligentes e conectadas, mas algo muito mais amplo.

Na mesma direção, Castells (2016, p. 135) assevera que: Sem dúvida, informação e conhecimento sempre foram elementos cruciais no crescimento da economia, e a evolução da tecnologia determinou em grande parte a capacidade produtiva da sociedade e os padrões de vida, bem como formas de organização econômica.

Na realidade, o renomado sociólogo desenvolve seu pensamento aduzindo que no último quartel do século XX, a revolução da tecnologia da informação forneceu a base material imprescindível para a criação de uma nova economia, que ele descreve como informacional, global, possuindo um funcionamento em rede. Conseqüentemente, a própria informação teria se tornado o produto do processo produtivo. Nesse contexto, surge a ideia de Sociedade da Informação, onde a informação se torna a matéria-prima básica da vida social, política, econômica e cultural. Essa sociedade seria caracterizada por redes interconectadas, fluxos de informação em tempo real e um novo paradigma de produção baseado no conhecimento. Deste modo, a consequência dessas mudanças revela implicações profundas para os indivíduos, as instituições e as estruturas sociais, somados a desafios de aperfeiçoar mecanismos instrumentais das relações virtuais e digitais de proteção de dados (Castells, 2016).

A revolução tecnológica ocorreu no contexto de um amplo processo de reestruturação global do capitalismo, pautado por suas lógicas e interesses de produção e poder. Diferentemente do modelo industrial de desenvolvimento, a principal fonte de produção não advém substancialmente da mão de obra, mas da tecnologia, da geração de conhecimentos e processamento de informações (Morellato; Santos, 2021).

A produtividade desse sistema econômico e o seu

principal ativo passou a residir na extração e utilização constante de dados pessoais dos indivíduos. Dessa forma, desenvolve-se um complexo constituído por uma rede crescente e estruturada de monitoramento que dão lugar a novas formas de acumulação, que é denominado de “capitalismo de vigilância” (Zuboff, 2021, p. 18).

Corroborando com o entendimento, Han (2022, p. 7-8) descreve a existência de um regime de informação, como forma de dominação através da qual as informações processadas por algoritmos e inteligência artificial determinam processos sociais econômicos e políticos. Diferentemente do regime disciplinar (forma de dominação do capitalismo industrial), que tinha como foco a exploração dos corpos e energias, sendo a posse dos meios de produção o fator decisivo para o ganho de poder, no regime de informação, o foco seriam as informações (dados) e o ganho de poder se daria por meio do acesso a dados utilizados para vigilância, controle e prognóstico de comportamento psicopolíticos. Assim, o regime de informação estaria enlaçado ao capitalismo da informação, que se desenvolve em capitalismo da vigilância, degradando os seres humanos em animais de consumo e dados.

O capitalismo da vigilância, dessa forma, postula de maneira unilateral a experiência humana como matéria-prima gratuita para transformação em dados comportamentais. Assim, uma parte desses dados são utilizados para melhoria dos produtos e serviços, restando um superávit comportamental do proprietário que serve de base para a fabricação de produtos de predição que se propõe a antecipar o que o indivíduo faria, agora ou mais tarde. Desse modo, os produtos de predição passam a ser comercializados num novo tipo de mercado que se denomina mercados de comportamentos futuros (Zuboff, 2021).

Segundo Bioni (2021, p.40) “ainda que essa nova forma de organização social não se resuma apenas ao meio ambiente virtual, a computação eletrônica e a internet são as ferramentas



de destaque desse processo”. Assim, ante o desenvolvimento das tecnologias emergentes e a intensificação dos fluxos de informação e expansão do acesso à internet, surgiram novas possibilidades de armazenamento, utilização e manipulação de informações pessoais, dentro desta sociedade da informação, regida pelo capitalismo da vigilância. Nas palavras de Rigon Filho e Nepomuceno (2021, p. 1139), “a internet tornou acessível a um toque de “mouse” ou a poucas teclas de celular de distância todo o conhecimento acumulado na história humana”.

Atualmente, é quase impossível imaginar uma vida desconectada, tanto no âmbito pessoal quanto profissional. Essa necessidade se traduz, inclusive, em números. Segundo um levantamento da Fundação Getúlio Vargas (FGV), em 2023, existem 2,2 dispositivos digitais – computadores, notebooks, tablets e smartphones – para cada habitante no Brasil. Os *smartphones* (celulares inteligentes) somam, sozinhos, 249 milhões, um número 20% maior do que o total da população. Os dados corroboram com a Pesquisa Nacional por Amostra de Domicílios (Pnad) de 2021, que apontou que 90% dos domicílios brasileiros já possuem conexão à internet (Meirelles, 2023).

A celeridade e o acesso à informação acarretaram, para além da facilidade de contratação de bens e serviços, o surgimento de novas formas de relações jurídicas. À vista disso, monetizaram-se novas atividades econômicas, visando as possibilidades de lucro, decorrendo daí o surgimento de relações de consumo disruptivas, que vão para além da venda de um produto, transformando o usuário (titular de dados) em produto (Guimarães Filho; Ferneda, Ferraz, 2020).

Assim, os dados passaram a ser considerados uma matéria prima para a segmentação e personalização dos anúncios publicitários, com a finalidade de influenciar os hábitos consumidores conforme os interesses dos agentes econômicos que utilizam o banco de dados, materializando-se através da aceitação dos termos e condições pelo usuário. Deste modo, estabeleceu-

se uma vigilância nos possuidores de dados, criando-se sua personalidade online, transformando-o em produto a ser comercializado (Almeida; Gervásio; Américo, 2020).

Desta maneira, remete-se à sociedade da informação que tem como papel central “a mudança qualitativa no tratamento de dados pessoais baseia-se na utilização de novos métodos, algoritmos e técnicas. Dentre elas está a elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas” (Fernandes, 2017, p. 378).

Com a prática da utilização da base de dados dos usuários para finalidade de marketing e negócio, a condição de vulnerabilidade do usuário (titular de dados) no ambiente digital tem um considerável agravo, isto porque, por diversas vezes, a coleta e tratamento dos dados são realizados sem o conhecimento e/ou consentimento do mesmo (Almeida; Gervásio; Américo, 2020).

De acordo com Bioni (2019), a maioria dos conteúdos disponibilizados de forma gratuita na internet, mascaram a existência de uma relação de consumo, visto que se distanciam do padrão de consumo normal em que se exige uma contraprestação pelo produto/serviço. Deste modo, no mundo virtual, as empresas têm se beneficiado com a transformação do usuário em produto, impondo o fornecimento de seus dados como uma contraprestação.

Partindo-se da constatação de que os usuários, no ambiente virtual, são considerados vulneráveis, deve-se buscar a compreensão de como o usuário cede seus dados, analisando se há consentimento, autonomia e consciência acerca do destino e utilização dos dados coletados e tratados, entendendo como este pode exercer a sua autodeterminação informativa perante o mercado que tem como base a mercantilização dos dados. A autodeterminação, nesse sentido, corresponde à segurança do titular de dados, onde o sujeito assume uma postura ativa no exercício do controle dos dados pessoais que lhes pertence, exercendo seu poder de escolha contra as empresas (Almeida; Gervásio;

Américo, 2020).

Nesse contexto, fica evidente a necessidade de proteção dos dados. Primeiramente, pela possibilidade de uso indiscriminado das informações, uma vez que os dados coletados e tratados pelas empresas podem ser vendidos para outras organizações, que poderão ofertar seus produtos e serviços de maneira mais assertiva. Segundo, pela possibilidade de vazamento de dados por parte das corporações, deixando o titular desses dados em risco de ser vítima de delitos e/ou crimes (D’ávila; Silva; Araújo, 2021).

Assim, a cidadania digital, ao implicar na existência de direitos atinentes aos dados digitais do sujeito de direito digitalizado, trouxeram graves problemas relacionados à privacidade e à proteção de dados pessoais. Segundo Alcantara (2017, p. 67):

O maior desafio quando mencionado a coleta de dados pessoais é, justamente, a dificuldade em preservá-los de modo correto; tratá-los, armazená-los e descartá-los, tudo isso sem ferir os direitos de seus cidadãos. E, um dos principais direitos, o que causa preocupação em todo internauta na hora de divulgar algo é, sem dúvidas, a privacidade.

Nesse sentido, observa-se que o direito à proteção de dados está intimamente ligado ao conceito de direito à privacidade, embora não se limite apenas à proteção deste direito fundamental. Assim, nas palavras de Doneda (2019, p. 128-129):

A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é um pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos.

Pereira e Medeiros (2023, p. 22) aduzem ainda que, evidentemente: “[...] há riscos à privacidade na sociedade da informação por meio da internet, tanto na esfera privada como pública, por isso justifica-se a tutela legislativa garantidora dos dados informacionais pessoais”. Restando, assim, indubitável a

necessidade de instrumentos que colaborem com a proteção de dados pessoais no ambiente virtual. É imprescindível, portanto, que haja uma regulação efetiva no tocante à proteção de dados, de maneira a garantir os direitos fundamentais da personalidade, privacidade e liberdade dos usuários.

### 3 A INSTITUCIONALIZAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL E SEUS PRINCIPAIS ASPECTOS

Segundo se tem evidenciado, a necessidade de proteção de dados pessoais nasceu como consequência da importância da garantia do direito à privacidade e liberdade do indivíduo, tornando-se imperativa na era das tecnologias da informação e comunicação. Os dados assumiram uma posição de extrema relevância para a formação da personalidade e gerência da vida do usuário, ao mesmo passo em que se ampliou sua valia no mercado de consumo atual.

Diante do protagonismo dos dados na sociedade atual foi detectada a necessidade de criar uma efetiva proteção integral “aos dados que são coletados e armazenados, assegurando os direitos fundamentais previstos no artigo 5º da Constituição Federal de 1988, tais como a liberdade, a privacidade e a segurança.” (Ferreira; Araújo, 2020, p. 57).

Desse modo, a revolução tecnológica e o uso ampliado das tecnologias da informação e comunicação implicaram numa busca por normatização da matéria de proteção de dados, com a finalidade de preservar os direitos dos titulares que têm seus dados circulando no ambiente digital. Nesse contexto, é que foi desenvolvido o *General Data Protection Regulation* (GDPR), regulamento da União Europeia de maio de 2018, que revolucionou o Direito atinente à proteção de dados pessoais, uma vez que o referido diploma legal passou a exigir que, para as empresas europeias realizarem a transferência internacional de dados

para fora da Europa, o país destinatário mantivesse padrões mínimos de Privacidade e Proteção de Dados. Assim, tal diploma gerou uma restrição radical ao tratamento de dados pessoais fora da Europa, pressionando diversos países a criar normas que visassem a proteção dos dados pessoais (D'ávila; Silva; Araújo, 2021).

Nesse contexto, sob a influência internacional europeia, foi promulgada, no Brasil, a Lei n. 13.709/18, conhecida como Lei Geral de Proteção de Dados (LGPD). Segundo Bioni (2019), até a aprovação da referida legislação, o Brasil possuía apenas leis esparsas de proteção de dados, correspondendo a uma verdadeira “colcha de retalhos” que não abarcava campos importantes da economia, não havendo uniformidade em seu regramento. Desse modo, conforme lecionam Almeida, Gervásio e Américo (2020, p. 8):

[...] o que se observa é que a legislação de proteção de dados no Brasil, se deu de forma progressiva com a constituição de 88. Desde o habeas data, perpassando pelo Código Civil de 2002, o Código de Defesa do Consumidor, a Lei do Cadastro positivo, a Lei de Acesso à Informação, o Marco Civil da Internet, passando pelos acordos com os quais o Brasil foi signatário, como na Declaração de Santo Cruz de Lá Sierra, até finalmente a chegar na proposição do projeto de Lei Geral de Proteção de Dados (lei da LGPD) e suas longas discussões até que fosse promulgada, em 2018, vindo a entrar em vigor apenas no ano de 2021.

Assim, a Lei Geral de Proteção de Dados Pessoais (LGPD) foi promulgada com o intuito de garantir a privacidade e proteger direitos fundamentais ao normatizar sobre a metodologia a ser utilizada na manipulação de dados pessoais, tanto na esfera privada quanto pelo poder público e ainda, posicionar o Brasil no mesmo patamar de outros países que são exemplos em legislação atinente a proteção de dados (Andrade; Barreto, 2020).

Desse modo, o que conduziu a promulgação da LGPD no Brasil foi uma série de parâmetros extraídos de uma

compreensão mais extensa do direito à privacidade e liberdade, correspondendo aos fundamentos elencados no artigo 2º da Lei, quais sejam: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

Constata-se ainda, que a Lei Geral de Proteção de Dados estipulou diversos princípios (art. 6º da LGPD) que devem ser respeitados por todos os órgãos e empresas que processam e armazenam dados, exigindo a efetivação de algumas adaptações, tornando-se necessária uma reanálise e reestruturação dos métodos e procedimentos internos para possibilitar adequação aos princípios e procedimentos previstos na referida Lei. Na mesma direção, Guimarães Filho, Ferneda e Ferraz (2020, p. 48) citam que:

Inicialmente, a questão se ilustra no corpo do art. 6º, inc. I e IV, respectivamente, na medida em que prevê que as atividades de tratamento de dados pessoais devem observar a boa-fé e princípios, tais como a finalidade (tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades) e transparência (garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial).

Para além destes, o artigo 6º da Lei nº 13.709/2018, ainda estabeleceu a observância dos seguintes princípios: princípio da adequação, princípio da necessidade, princípio do livre acesso, princípio da qualidade de dados, princípio da segurança, princípio da prevenção, princípio da não discriminação e princípio da responsabilização e prestação de contas (Brasil, 2018).

Outrossim, com a finalidade de assegurar a eficácia e a

aplicação prática das normas estabelecidas pela regulação da proteção de dados no Brasil e visando atingir o nível da regulamentação europeia, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), através da Medida Provisória n. 869, de 27 de dezembro de 2018, convertida na Lei nº 13.853, de 8 de julho de 2019 (Angelo, 2021).

Desse modo, a ANPD é o órgão com autonomia técnica e decisória, que tem dentre as suas competências a deliberação acerca da interpretação da LGPD, a elaboração de diretrizes e normas para a sua implementação, bem como a fiscalização e aplicação de sanções em caso de tratamento de dados realizado em descumprimento à referida legislação (BRASIL, 2018).

A LGPD trouxe inúmeras inovações, dentre elas: a responsabilização dos agentes diante do tratamento de dados, a participação dos titulares desde a coleta até a transferência a terceiros, conceitos próprios para o processamento de dados e hipóteses em que este tratamento poderá ocorrer. No entanto, uma das maiores reverberações da lei, diz respeito a grande relevância dada ao consentimento do usuário (Lugati; Almeida, 2020).

Nessa esteira, o consentimento simboliza a base legal da autodeterminação e da livre manifestação individual, possibilitando o manuseio de dados pessoais, mediante autorização do titular ou de seu representante legal de maneira inequívoca e evidente, para um propósito determinado (Frazão; Tepedino; Oliva, 2020)

Diante de todo o exposto, apesar da LGPD ter representado importante marco regulatório quanto a matéria de proteção de dados pessoais e ter suprido algumas lacunas legais, tendo em vista que, antes de sua promulgação haviam apenas legislações esparsas no tocante ao tema no ordenamento jurídico brasileiro, a LGPD precisa continuar evoluindo para acompanhar o acelerado desenvolvimento tecnológico, sendo extremamente necessário um estudo aprofundado acerca da Lei, nesse curto período de sua vigência, para permitir a verificação dos pontos a serem

atualizados para que a norma não se torne obsoleta e possa acompanhar as transformações do mundo globalizado.

#### 4 OS LIMITES DO CONSENTIMENTO DO TITULAR DE DADOS NA LGPD E PROTEÇÃO DA PRIVACIDADE: ANÁLISE SOB A ÓTICA DA MERCANTILIZAÇÃO DE DADOS

O consentimento, apesar de representar apenas uma das hipóteses legais que ensejam o tratamento de dados (art. 7º da Lei nº 13.709/2018), assume um lugar de protagonismo. Tal percepção é inferida através de uma análise mais aprofundada dos princípios e a maneira pela qual a LGPD trata tal elemento, revelando uma preocupação sobre qual deve ser a carga participativa do indivíduo no fluxo de suas informações pessoais, buscando conformar a ideia de que o titular deve ser empoderado com o controle de suas informações pessoais e na autonomia da sua vontade. Na referida Lei há 35 menções ao termo “consentimento”, constatação que faz compreender, numa análise quantitativa e qualitativa, a importância do referido elemento (Bioni, 2021, p. 215-216).

A Lei Geral de Proteção de Dados considera como consentimento, a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (Brasil, 2018). Desta forma, conforme já elucidado anteriormente, o consentimento seria o símbolo da base legal da autodeterminação e da livre manifestação individual. Sendo o instrumento por meio do qual se possibilita o manuseio de dados pessoais, mediante autorização do titular ou de seu representante legal de maneira inequívoca e evidente, para um propósito determinado (Frazão; Tepedino; Oliva, 2020).

Verifica-se que o consentimento pode ser visto pela perspectiva implícita, quando uma pessoa entende que consentiu em



razão de sua própria conduta, passando, então, ao consentimento informado o qual orienta por normas relativas à circulação de informações. Essas normas permitirão que o usuário seja parte no processo de consentimento, por meio da autorização (Tepe-dino; Teffé, 2020). Conforme lecionam Ferreira e Araújo (2020), essa autorização deverá ser obtida no momento da coleta dos dados, necessitando a empresa esclarecer de forma simples e objetiva o propósito da concessão dessas informações. Deste modo, a autorização não poderá ser concedida de maneira genérica, devendo a empresa expor a finalidade para qual as informações estão sendo coletadas.

De outro lado, a referida Lei ainda prevê algumas hipóteses em que o consentimento do titular de dados é dispensada, mesmo para a utilização dos dados pessoais sensíveis, estando as referidas hipóteses elencadas no art. 11, inciso II da LGPD, quais sejam: cumprimento de obrigação legal; tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa; exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo ou arbitral; proteção da vida ou da incolumidade física do titular ou de terceiros; tutela da saúde; ou garantia da prevenção à fraude e à segurança do titular (Brasil, 2018).

Desse modo, apesar de ser um instrumento que visou a proteção da privacidade do titular de dados, transferindo para este o controle sobre suas informações pessoais, é possível observar que, na sociedade da informação, boa parte das relações jurídicas se transformaram em relações de consumo, o que acarretou grandes desafios à garantia da privacidade do titular de dados tendo em vista a expansão da mercantilização de dados.

Ocorre que, os usuários da internet (titulares de dados), em sua grande maioria, reconhecem apenas como relação de consumo virtual, aquela tipicamente tradicional, em que se compra ou se contrata algum tipo de produto/serviço. No entanto, a

relação de consumo do mundo virtual não tem se resumido ao conceito tradicional. Ao utilizar a internet para as mais diversas finalidades (compras, diversão, comunicação, entre outros) os usuários fornecem seus dados pessoais, consentindo, em um genuíno desconhecimento, que alguns sites/aplicativos coletem seus dados pessoais e os tratem para algoritmicamente traçar perfis de consumo, que poderão ser comercializados/utilizados posteriormente para várias finalidades, dentre elas o direcionamento de publicidade. Assim, Bioni (2021, p. 50) aduz que:

No modelo de negócio “tradicional”, consumidores trocam uma quantia pecuniária por um bem de consumo. Por exemplo, cada item de um carrinho de supermercado tem o preço exato a ser pago para a aquisição. Trata-se de uma relação bilateral entre consumidor e fornecedor, cuja transação econômica é aperfeiçoada por uma transferência pecuniária. Ao passo que, sob um novo modelo de negócio, consumidores não pagam em dinheiro pelos bens de consumo, eles cedem seus dados pessoais em troca de publicidade direcionada. São os anunciantes de conteúdo publicitário que aperfeiçoam o seu arranjo econômico. Dessa forma, tal relação torna-se plurilateral, uma vez que ela envolve, necessariamente, os anunciantes de conteúdo publicitário, para haver retorno financeiro nesse modelo de negócio.

Assim, a partir dos dados do consumidor (usuário), é traçado um perfil comportamental através de algoritmos automáticos e, posteriormente, as empresas conseguem influenciar na escolha de aquisição de produtos e serviços, ou até mesmo produzir segregações de ordem discriminatória que são capazes de afetar os aspectos da construção da livre e autoinformada personalidade do indivíduo (Bioni, 2019), tornando-se imperativa, portanto, a criação de instrumentos que visem a proteção do consumidor no ambiente digital.

Dessa forma, uma ampla parcela dos usuários não possui sequer ciência acerca do tratamento realizado nos seus dados pessoais, desconhecendo a prática de coleta e tratamento de dados em contraprestação ao fornecimento de serviços/produtos. No atual cenário, as informações íntimas dos usuários

encontram-se frequentemente disponíveis e acessíveis nas redes, erigindo uma economia algorítmica de padrões estatísticos.

Nesse sentido, apesar da LGPD ter representado um verdadeiro marco regulatório na matéria da proteção de dados no Brasil, ela necessita ser analisada no contexto da economia política em que se inseriu: a da comercialização dos dados pessoais em uma prática de vigilância dos titulares de dados (consumidores).

Desse modo, observa-se certa ambiguidade na referida Lei, uma vez que apesar de se propor à proteção dos dados pessoais, ela permite, juridicamente, a criação e expansão de um mercado de dados no Brasil. Isto porque o referido diploma legal admite a entrega de dados, com a livre contratação sobre a cessão de tais dados a partir do consentimento do consumidor (usuário), sem contudo, identificar os limites do consentimento do titular, não abarcando formas específicas de consentimento juridicamente eficazes, trazendo a normativa do consentimento de maneira generalizada (Fornasier; Knebel, 2021).

Apesar da necessidade de regulação dos algoritmos automatizados no mundo virtual, a LGPD, enquanto norma mais avançada no que tange a proteção de dados pessoais no Brasil, se desincumbiu da previsão de métodos e procedimentos adequados para garantir a utilização eficiente dos algoritmos, com vistas a coibir as práticas preconceituosas e violações a direitos fundamentais.

Deste modo, pensa-se que os limites do consentimento previstos na LGPD por si só, não garantem a proteção ao direito à privacidade do consumidor, uma vez que o referido diploma legal possibilita a entrega de dados de forma consentida, o que pode ser utilizado e comercializado por empresas, para os mais diversos fins, sem que, no entanto, o usuário (consumidor) tenha ciência real do produto que seus dados pessoais se tornaram.

O ordenamento jurídico pátrio deve criar mecanismos de atualização legislativa visando acompanhar as mudanças

tecnológicas, afim de se atingir a maior objetividade possível na represália às ofensas contra a privacidade do titular de dados (Fernandes, 2017). Deste modo, é preciso que haja um esforço conjunto entre os Governos, empresas e cidadãos, no sentido de adotar medidas que visem ampliar essa proteção aos dados do usuário frente à mercantilização dos dados.

Além do fortalecimento das regulamentações dessa temática, é preciso aprimorar os mecanismos de controle e monitoramento das atividades que envolvam o tratamento de dados, encorajando a minimização de dados (coleta apenas dos dados estritamente necessários ao propósito), estimulando a concorrência no mercado de dados, exigindo-se uma maior transparência das empresas e impondo multas significativas para os que violarem a regulamentação. Ademais, é necessário garantir investimentos para o desenvolvimento de novas tecnologias de privacidade e aprimoramento da cibersegurança, bem como para a promoção de educação digital para a população e a conscientização sobre privacidade, para que o usuário possa, de fato, exercer a autodeterminação informacional.

## 5 CONSIDERAÇÕES FINAIS

A instituição da LGPD (Lei Geral de Proteção de Dados) no Brasil reconheceu a importância da obtenção do consentimento informado e inequívoco dos titulares de dados para o processamento de seus dados pessoais. No entanto, ainda que o consentimento tenha assumido uma posição de destaque na legislação supracitada, por meio do qual o titular de dados pode exercer a autodeterminação informacional, este instrumento, unicamente, não garante a proteção da privacidade do titular de dados. A existência de termos e condições complexos e as práticas frequentemente obscuras de coleta e uso de dados criam uma conjuntura em que os indivíduos podem consentir inadvertidamente com práticas que comprometem sua privacidade.

Além disso, o surgimento do capitalismo de vigilância e a mercantilização de dados pessoais ocasionou uma assimetria de poder entre os indivíduos e os controladores de dados. Muitos serviços ofertados de maneira "gratuita" em troca de dados pessoais, transformam os indivíduos em produto. O consentimento dado em tais transações pode não ser verdadeiramente voluntário devido à falta de conhecimento técnico e de alternativas viáveis ao desigual poder de barganha.

A LGPD, visando enfrentar esses desafios, impôs requisitos de transparência, princípios de minimização de dados e direitos para os titulares de dados acessarem e controlarem seus dados. Entretanto, a aplicação desse regulamento ainda está em evolução, havendo a necessidade de constante monitoramento e adaptação para acompanhar as tecnologias emergentes e práticas de mercado, visando encontrar um equilíbrio entre o tratamento de dados e a privacidade dos titulares, ou seja, o verdadeiro desafio da LGPD e regulamentos análogos em todo o mundo reside em sua capacidade de permanecer como uma ferramenta eficaz, capaz de salvaguardar a privacidade e os direitos dos titulares de dados em um mundo orientado por dados.

Por fim, reconhece-se que, embora o consentimento continue sendo crucial para a proteção de dados, ele deve ser complementado por outras medidas. Reforçar a conscientização sobre privacidade, promover a educação digital, estimular a concorrência no mercado de dados e aprimorar a supervisão regulatória são medidas essenciais para garantir que o direito de privacidade dos indivíduos seja mantido diante da crescente comercialização de dados. REFERÊNCIAS

ALCANTARA, L. K. *Big data internet das coisas: tecnologia e inovação no Direito Digital*. São Paulo: Martins Fontes, 2018.

ALMEIDA, J. E.; GERVÁSIO, A. L. M.; AMÉRICO, L. B. *Hipervulnerabilidade dos consumidores na era do*

- marketing 4.0. *Revista de Direito*, Viçosa, v. 14, n. 2, p. 1-21, 2020.
- ANDRADE, D. C. M.; BARRETO, R. H. A. A ausência da atividade fiscalizadora na Lei Geral de Proteção de Dados e sua ineficácia. *Redes: Revista Eletrônica Direito e Sociedade*, Canoas, v. 8, n. 2, p. 61-73, 2020.
- ANGELO, E. S. Lei Geral de Proteção à Dados Pessoais como elemento da Agenda 2030: cesso à informação e desenvolvimento de competência crítica. *Revista ABC: Biblioteconomia em Santa Catarina*, Florianópolis, v. 26, n. 3, p. 1-14, 2021.
- BIONI, B. R. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.
- BIONI, B. R. *Proteção de dados pessoais: a função e os limites do consentimento*. 3 ed. Rio de Janeiro: Forense, 2021.
- BRASIL. *Lei n° 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 04 fev. 2023.
- \_\_\_\_\_. *Emenda Constitucional n° 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](https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm). Acesso em: 14 set. 2019.
- CASTELLS, M. *A sociedade em rede*. São Paulo: Paz e Terra, 2016.
- DONEDA, D. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: *Revista dos Tribunais*, 2019.
- D'ÁVILA, A. V. G.; SILVA, B. F.; ARAÚJO, T. V. *LGPD: muito além da lei: uma análise do direito em conjunto*

- com a segurança da informação. São Paulo: Amazon, 2021.
- FERNANDES, D. A. Dados pessoais: uma nova commodity, ligados aos direitos à intimidade a dignidade da pessoa humana. *Revista Jurídica*, Curitiba, v. 4, n. 49, p. 360-392, 2017.
- FERREIRA, I. A. C.; ARAÚJO, D. F. O. A Lei Geral de Proteção de Dados e suas repercussões no e-commerce de empresas privadas. *Novos Direitos*, v. 10, n. 1, p. 54-83, 2020.
- FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (Coord.). *Lei geral de proteção de dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.
- FORNASIER, M. O.; KNEBEL, N. M. P. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. *Revista Direito e Práxis*, Rio de Janeiro, v. 12, n. 2, p. 1002-1033, 2021.
- GUIMARÃES FILHO, P. A.; FERNEDA, A. S.; FERRAZ, M. O. K. A proteção de dados e a defesa do consumidor: autonomia privada frente à privacidade. *Meritum*, v. 15, n. 2, p. 38-52, 2020.
- HAN, B. *Infocracia: digitalização e a crise da democracia*. Petrópolis: Editora Vozes, 2022.
- LUGATI, L. N.; ALMEIDA, J. E. Da evolução as legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *Revista de Direito*, Viçosa, v. 12, n. 2, p. 1-33, 2020.
- MARCONI, M. A.; LAKATOS, E. M. *Técnicas de Pesquisa*. 5 ed. São Paulo, Atlas, 2002.
- MEIRELLES, F. S. *Pesquisa do uso da TI – Tecnologia da Informação nas Empresas*. 34 ed. Rio de Janeiro: FGV,

2023. Disponível em: [https://easp.fgv.br/sites/easp.fgv.br/files/u68/pesti-fgvicia-2023\\_0.pdf](https://easp.fgv.br/sites/easp.fgv.br/files/u68/pesti-fgvicia-2023_0.pdf). Acesso em 14 set. 2023.
- MORELLATO, A. C. B.; SANTOS, A. F. P. Capitalismo de vigilância e a Lei Geral de Proteção de Dados: perspectivas sobre consentimento, legítimo interesse e anonimização. *RBSD – Revista Brasileira de Sociologia do Direito*, v. 8, n. 2, p. 184-211, maio/ago. 2021.
- PEREIRA, M. M. F.; MEDEIROS, V. F. A importância do papel regulatório da ANPD na Sociedade Informacional sob a perspectiva da análise econômica do Direito. *Revista de Direito, Economia e Desenvolvimento Sustentável*, v. 9, n. 1, p. 16–33, jan/Jul. 2023.
- RIGON FILHO, A.; NEPOMUCENO, A. S. Tutela da privacidade a internet: papel o consumidor. In: BOREGGIO, A. (Org.). *Temas atuais de direito do consumidor*. Salvador: Studio Sala de Aula, 2021.
- SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2018.
- TEPEDINO, G.; TEFFÉ, C. S. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil – RBD Civil*. V. 25, p. 83-116, jul./set., Belo Horizonte, 2020.
- YANDRA, B. F. F.; SILVA, A. C. A.; SANTOS, J. G. Lei Geral de Proteção de Dados e a tutela dos dados pessoais e crianças e adolescentes: a efetividade do consentimento dos pais ou responsáveis legais. *Internet & Sociedade*, v. 1, n. 1, p. 230-249, 2020.
- ZUBOFF, S. *A era do capitalismo da vigilância: A luta por um futuro humano na nova fronteira do poder*. Rio de Janeiro: Editora Intrínseca, 2021.
- 34ª edição da Pesquisa Anual do FGVcia sobre o Mercado Brasileiro de TI e Uso nas Empresas, *Coordenação: Prof. Fernando S. Meirelles*, 2023. Disponível em: <https://easp.fgv.br/producao-intelectual/pesquisa-anual-uso-ti>.



Acesso em: 10 jun. 2023.