

# LEI GERAL DE PROTEÇÃO DE DADOS: respeito à privacidade e à responsabilidade civil dos agentes de tratamento de dados pessoais no Brasil

MENDES, Mikaelly Gonçalves<sup>a</sup>; MACEDO, Suélem<sup>b</sup>



<sup>a</sup> Discente do curso de Bacharelado em Direito - UNIFAGOC

<sup>b</sup> Doutora em Administração Pública – Professora do Curso de Direito – UNIFAGOC

mikaellygm19@gmail.com  
suelem.macedo@unifagoc.edu.br

## RESUMO

*O objetivo geral do presente estudo consistiu em analisar a responsabilidade civil dos agentes de tratamento de dados no âmbito da Lei Geral de Proteção de Dados (LGPD), apontando os principais posicionamentos adotados. Quanto aos procedimentos metodológicos, adotou-se uma abordagem qualitativa, à luz das normas jurídicas constitucionais e legais brasileiras, bem como apontamentos doutrinários. Para tanto, parte-se de um estudo das principais características da Lei Geral de Proteção de Dados, sendo importante compreender o direito à privacidade como um dos fundamentos da proteção dos dados pessoais. Os resultados apontam que a Lei Geral de Proteção de Dados adotou o sistema de responsabilidade civil subjetiva. No entanto, ainda é possível que o agente de tratamento possa ser responsabilizado objetivamente quando for comprovada a relação de consumo.*

**Palavras-chave:** Agentes de Tratamento. Direito Digital. Lei Geral de Proteção de Dados. Privacidade. Responsabilidade Civil.

## INTRODUÇÃO

O uso da internet se faz cada vez mais presente na vida das pessoas, causando importantes transformações no cotidiano. Cursar uma faculdade, pagar uma conta, fazer compras e justificar a ausência às urnas, tudo isso é possível se estiver conectado, a qualquer hora, em qualquer lugar. Devido a esses avanços tecnológicos, foi necessária uma legislação que regulamentasse as atividades de tratamento de dados pessoais, sendo criada a Lei Geral de Proteção de Dados (LGPD). Aprovada em 2018, a Lei 13.709 (BRASIL, 2018), tem como objetivo assegurar o direito à privacidade e à proteção de dados pessoais dos usuários digitais, entrando em vigor em 18 de setembro de 2020, à exceção das sanções administrativas, que passaram a ser exigíveis a partir de 1º agosto de 2021.

O conceito de dado pessoal, nos termos do artigo 5º da LGPD (Brasil, 2018), corresponde a “toda informação que torna a pessoa identificada ou identificável”, tais como: nome, RG, CPF, gênero, telefone e endereço residencial. É comum que, para acessar sites, aplicativos, realizar uma compra no ambiente virtual, seja necessário preencher cadastros informando os dados pessoais. Dessa forma, a LGPD traz em seu texto legal a obrigatoriedade da adequação para todas as pessoas físicas ou jurídicas que utilizam dados pessoais em suas atividades, adotando políticas para garantir a

segurança dos dados pessoais de seus clientes, sendo imprescindível a autorização do usuário para a coleta de suas informações pessoais e adoção de medidas de segurança da informação para evitar incidentes e a exposição de dados pessoais a usos indevidos.

Tal foi a importância da promulgação da LGPD, que o Supremo Tribunal Federal, mesmo durante uma longa *vacatio legis*, mudou seu entendimento sobre a matéria, reconhecendo o direito fundamental autônomo à proteção de dados pessoais (Ações Diretas de Inconstitucionalidade (ADIs) nº. 6387/2020 6388/2020, 6389/2020, 6390/2020 e 6393/2020). Isso ocorreu ao suspender a Medida Provisória nº 954/2020 (Brasil, 2020), que obrigava as operadoras de telefonia a repassarem ao Instituto Brasileiro de Geografia e Estatística (IBGE) os dados identificadores de seus clientes de telefonia fixa e móvel. O julgamento se baseia no fato de que, com o constante desenvolvimento da tecnologia da informação, não há dados neutros. A Ministra Rosa Weber, relatora do caso, afirmou que qualquer dado que permita identificar um indivíduo pode ser usado para a construção de perfis informacionais de grande valor para o Estado e para as empresas privadas, as quais potencialmente ameaçam o direito à autodeterminação informativa.

Além disso, o voto condutor destacou que a Medida Provisória possuía vícios, como a inobservância do princípio da eficácia, a ausência de medidas de segurança adequadas e o excesso no recolhimento de dados, os quais foram agravados pela preservação do quadro normativo-institucional, proveniente da demora da criação da Autoridade Nacional de Proteção de Dados (ANPD). Apesar de sua importância central para a implantação bem-sucedida do novo regime jurídico, a ANPD somente foi criada em 2019, pela Lei 13.853 de julho de 2019 (Brasil, 2019).

A Lei 13.709/2018 (BRASIL, 2018), em seu artigo 5º, inciso X, define o tratamento como toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. O referido tratamento de dados é realizado pelo operador em nome do controlador, os quais são obrigados a reparar dano patrimonial, moral, individual ou coletivo, que for causado a outrem em razão do exercício de atividade de tratamento de dados pessoais, em violação à legislação de proteção de dados pessoais, conforme disposto no artigo 42 da referida Lei.

Ocorre, porém, que ainda não há um consenso na literatura acerca da aplicabilidade da responsabilidade subjetiva ou objetiva dos agentes no âmbito da LGPD. Parte da doutrina defende que o desenho das normas de responsabilidade civil na LGPD apresenta falhas e omissões que precisam ser corrigidas pelo intérprete para estabelecer um regime coerente e eficaz. É necessário considerar os elementos da LGPD e de outras normas brasileiras, especialmente as constitucionais, para construir soluções interpretativas adequadas. Embora o artigo 42 da Lei 13.709/2018 (Brasil, 2018) não mencione explicitamente a culpa, não utiliza a expressão “independentemente de culpa”, como apresentado em outras normas como o Código Civil e o Código de Defesa do Consumidor, o que sugere uma preferência por um regime de responsabilidade subjetiva (Schreiber, 2020).

Entretanto, para os autores que defendem a responsabilidade civil objetiva, tem-se como argumento principal que a atividade de tratamento de dados apresenta

um risco inerente, uma vez que há potencial significativo de danos em caso de violação dos direitos dos titulares. Em suma, o tratamento de dados pessoais seria considerado uma atividade de risco devido ao fato de que tais direitos dos titulares são personalíssimos e fundamentais (Mendes; Doneda, 2018).

Desse modo, frente à problemática apresentada, o presente estudo busca responder ao seguinte questionamento: qual a responsabilidade civil dos agentes de tratamento de dados pessoais no Brasil? Diante do exposto, este trabalho tem como objetivo geral analisar a responsabilidade civil dos agentes de tratamento de dados no âmbito da Lei Geral de Proteção de Dados (LGPD).

Especificamente, esta pesquisa pretende: (a) analisar o direito à privacidade como fundamento da Lei Geral de Proteção de Dados; (b) compreender os aspectos relevantes sobre a Lei Geral de Proteção de Dados; (c) discutir a responsabilidade civil dos agentes de tratamento no âmbito da Lei Geral de Proteção de Dados.

Em termos de justificativa, o presente estudo visa contribuir para esse debate, apontando os principais posicionamentos adotados e as consequências dessas interpretações para os titulares e agentes de tratamento. Trata-se de uma lei que de modo sistemático coordena a proteção de dados pessoais, definindo normas e procedimentos fundamentais, trazendo grande impacto na vida das pessoas, das empresas e dos entes dos setores público e privado, de modo geral.

Para o desenvolvimento do estudo, a abordagem metodológica utilizada é a pesquisa qualitativa de cunho descritivo, baseada em revisão de literatura. Os procedimentos de coleta dos dados serão realizados por meio de técnicas de pesquisa bibliográfica e documental, visto que é efetuada uma análise da legislação vigente, com base na doutrina, e normas aplicáveis, com o intuito de relacionar os dados para a interpretação (Gil, 2002).

Este artigo encontra-se dividido em cinco seções, começando por esta introdução. A segunda seção aborda as características gerais da LGPD. A terceira trata sobre o respeito à privacidade como fundamento da proteção de dados pessoais. Na quarta seção, é discutida a responsabilidade civil dos agentes de tratamento na Lei Geral de Proteção de Dados e, por fim, são apresentadas as considerações finais.

## **CARACTERÍSTICAS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS**

Desde 2018, a União Europeia tem em vigor o seu regulamento, conhecido como Regulamento Geral de Proteção de Dados (GDPR). Esse regulamento foi um impulso para o Brasil na criação da Lei Geral de Proteção de Dados (LGPD), que foi promulgada como Lei nº 13.709 (Brasil, 2018) e, em 2020, entrou em vigor (Agência Senado, 2020). A LGPD tem como objetivo aprimorar a administração de dados pessoais por parte de órgãos públicos, instituições e empresas, estabelecendo normas indispensáveis para garantir a sustentabilidade na era digital. Diante das diretrizes impostas pela LGPD, como a imposição de multas, as organizações e instituições tiveram que se adequar, tendo em vista a obrigatoriedade das normativas para a efetivação de tratamento de dados, que possui como objetivo regulamentar a utilização e o tratamento de dados pessoais.

O fundamento da proteção conferida pela LGPD (Brasil, 2018) consiste na pessoa natural, cujos dados são tutelados a depender de serem ou não sensíveis. O artigo 5º, inciso I a III da Lei 13.709 (Brasil, 2018) caracteriza os tipos de dados,

considerando dado pessoal como as informações relacionadas à pessoa natural identificada ou identificável; dado pessoal sensível como os dados 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, bem como os dados anonimizados, que se referem aos dados relativos a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios de finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção e a não discriminação, além da responsabilização e prestação de contas, bem como cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas, como previsto pelo artigo 6º, I ao X, da Lei 13.709 (Brasil, 2018). Logo, a análise de risco e a segurança da informação são aspectos que devem ser levados em consideração pelas organizações para que sejam respeitados os requisitos determinados pela lei em questão.

Outra fundamental característica da nova legislação consiste no significativo fomento ao aspecto preventivo, estabelecendo procedimentos mandatários para os controladores e operadores de dados pessoais, tais como, deveres atinentes à implementação de severas políticas de segurança para proteção dos dados de acessos não autorizados, conforme prevê o artigo 46 da LGPD (Brasil, 2018). Trata-se de uma perspectiva promissora, uma vez que as características inerentes ao ambiente digital – como a rápida evolução tecnológica, a capacidade de disseminação de informações e a dificuldade de controlar o fluxo de dados – juntamente com a expansão da coleta e do processamento de dados, apresentam desafios à abordagem repressiva, especialmente quando baseados no modelo comando-controle. O engajamento espontâneo dos titulares dos deveres e a prevenção na tutela do direito fundamental aos dados pessoais afiguram-se essenciais e, não à toa, no que diz respeito a este último aspecto, cuida-se de princípio plasmado no art. 7º, VIII, da LGPD (Brasil, 2018) (Frazão; Oliva; Abilio, 2019).

O tratamento de dados pessoais é realizado pelo controlador, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados. As hipóteses para realização do tratamento de dados pessoais estão elencadas no artigo 7º da Lei 13.709/2018 (Brasil, 2018):

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular; II – para o cumprimento de obrigação legal ou regulatória pelo controlador; III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de

23 de setembro de 1996 (Lei de Arbitragem) ; VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII – para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (Brasil, 2018).

São requisitos substanciais os que digam respeito à qualidade do consentimento. Conhecimento e compreensão por aquele de quem se requer o consentimento são elementos essenciais para a sua configuração. Daí o sentido de que se trate de uma manifestação de vontade livre – significa dizer, isenta de pressões ou ameaças diretas ou indiretas que contaminem a decisão do consumidor, consoante o artigo 8º, §3º da LGPD (BRASIL, 2018). Exige-se também que seja uma manifestação de vontade informada, ou seja, só é reconhecido como eficaz o consentimento quando aquele que manifesta vontade teve as condições plenas de compreender o conteúdo da sua decisão e de que modo ela repercute em relação aos seus interesses pressupostos. O consentimento daquele que decide a partir de informações incorretas ou incompletas não é reconhecido como tal, de modo a tornar ilícitas, no âmbito do tratamento dos dados pessoais, quaisquer operações que venham a se basear nele (Miragem, 2019).

O direito de revogar o consentimento está intrinsecamente ligado à autonomia do titular dos dados. O titular tem o direito de consentir com o processamento dos seus dados e pode modificar sua decisão, revogando o consentimento. A lei estabelece que o exercício desse direito de revogação deve ser realizado de forma gratuita e facilitada, conforme previsto no artigo 8º, parágrafo 5º, da LGPD (Brasil, 2018). No mínimo, deve-se exigir que seja disponibilizado o mesmo meio utilizado pelo controlador para obter o consentimento, e a revogação tem efeito a partir do momento em que é manifestada (*ex nunc*). A revogação relaciona-se também com o direito de informação do titular dos dados sobre a possibilidade e as consequências da revogação, inclusive sobre a eventualidade de ela não impedir a continuidade do tratamento nas hipóteses que a lei estabelece (Miragem, 2019).

O titular deverá ter direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizados de forma clara, adequada e ostensiva, entre outras características previstas em regulamentação, para o atendimento do princípio do livre acesso, como dispõe o artigo 9º, I ao VII, da Lei 13.709 (Brasil, 2018).

A seção IV da LGPD (Brasil, 2018) discorre sobre o término do tratamento de dados, o qual é possível nas seguintes hipóteses: quando for verificado que a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; fim do período de tratamento; comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou por meio de determinação da

autoridade nacional, quando houver violação ao disposto na referida Lei. Após o término do tratamento, os dados pessoais serão eliminados, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as finalidades permitidas pela LGPD.

Dessa forma, percebe-se que a Lei Geral de Proteção de Dados é uma legislação que reforça o respeito à privacidade como um direito fundamental e estabelece regras claras para o tratamento adequado dos dados pessoais, buscando equilibrar a proteção dos direitos individuais com a necessidade de avanços tecnológicos e inovações, garantindo a privacidade dos cidadãos em um ambiente digital cada vez mais complexo.

## **RESPEITO À PRIVACIDADE COMO FUNDAMENTO DA PROTEÇÃO DE DADOS PESSOAIS**

Consoante declara o artigo 2º, I, da Lei 13.709 (Brasil, 2018), o respeito à privacidade é um dos fundamentos essenciais da proteção de dados pessoais. A privacidade refere-se ao direito de uma pessoa controlar o acesso e o uso de informações que lhe dizem respeito, como a sua vida pessoal, familiar e íntima. Na era digital, em que cada vez mais informações pessoais são coletadas, armazenadas e processadas, o respeito à privacidade torna-se ainda mais crucial. Dessa forma, para garantir que as informações pessoais de um indivíduo sejam tratadas de forma adequada, segura e transparente, é necessário que seja respeitado o direito das pessoas de controlarem seus próprios dados e decidirem como tais dados serão utilizados, com quem serão compartilhados e por quanto tempo serão aceitos.

A Constituição Federal de 1988 (Brasil, 1988), em seu artigo 5º, inciso X, declara que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. Isso significa que todos têm o direito de serem respeitados em sua esfera pessoal e familiar, sendo protegidos contra qualquer forma de divulgação ou invasão não autorizada de sua vida privada.

A partir de 1990, foram criados os primeiros instrumentos legais que abrangiam a proteção de dados pessoais. Em 1990, criou-se o Código de Defesa do Consumidor, pela Lei 8.078 (Brasil, 1990), que prevê o direito do consumidor de acessar as informações sobre ele existentes em cadastros, registros, fichas de dados pessoais e de consumo arquivados, além de permitir a ciência do consumidor no caso de abertura de cadastros contendo dados pessoais. Em 1996 foi criada a Lei 9.296 de Interceptação Telefônica e Telemática (Brasil, 1996), que permite o uso de tais interceptações de comunicação apenas em casos específicos e mediante autorização judicial. O Habeas Data, instituído pela Lei 9.507 (Brasil, 1997), regulou o rito de acesso de registros ou banco de dados, tornando-se um direito constitucional com a finalidade de garantir o acesso às pessoas físicas ou jurídicas, bem como promover a retificação de seus dados que estejam registrados em banco de dados de órgãos públicos ou instituições similares.

A Lei nº. 10.406/2002 (Brasil, 2002), que institui o Código Civil, possui um capítulo que versa sobre os direitos da personalidade, o qual fornece instrumentos que visam reprimir a violação da vida privada das pessoas, tendo a privacidade como um direito subjetivo do ser humano. Como forma de coibir a violação da vida privada, foi

criada a Lei nº. 12.527 (Brasil, 2011), chamada Lei de Acesso à Informação, que define a informação pessoal como aquela relacionada à pessoa natural identificada ou identificável, determinando aos órgãos e entidades do poder público a proteção da informação sigilosa e pessoal, observando a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. A Lei de Acesso à Informação também ressalta alguns princípios que são celebrados na LGPD, como o princípio da transparência, vida privada e respeito à intimidade.

Após um caso de muita repercussão sobre violação à privacidade, foi criada a Lei nº. 12.737 (Brasil, 2012), denominada Lei Carolina Dieckman, a qual tornou crime a prática de invasão de dispositivos de informática, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Entretanto, o Marco Civil da Internet foi o primeiro grande passo da nossa legislação com relação ao direito digital. A Lei nº. 12.965 (Brasil, 2014) estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, representando um importante marco na regulamentação da internet no país.

O objetivo principal do Marco Civil da Internet é garantir a liberdade de expressão, a privacidade dos usuários, a neutralidade da rede e a responsabilidade dos diversos agentes envolvidos no ambiente digital. A lei foi elaborada com a participação da sociedade civil e busca equilibrar os interesses dos usuários, das empresas e do Estado, criando um ambiente online mais seguro e transparente. A LGPD aprimorou diversas normas visando potencializar os efeitos do Marco Civil da internet, com regras mais específicas sobre o tratamento de dados pessoais, cobrindo algumas lacunas deixadas pela Lei 12.965 (Brasil, 2014), regulamentando, principalmente, a coleta e a forma de utilização dos dados pessoais dos usuários. Além disso, a LGPD definiu padrões a serem seguidos para que as relações desenvolvidas na internet respeitassem o princípio da privacidade.

De acordo com Moraes (2002, p. 60), “o direito à vida privada, à intimidade, à honra, à imagem dentre outros, aparecem como consequência imediata da consagração da dignidade da pessoa humana como fundamento da República Federativa do Brasil”. Isso ocorre porque esse direito é um princípio estrutural, estabelecido no art. 1º, inciso III, da Constituição Federal (Brasil, 1988), e abrange a proteção dos direitos fundamentais, irradiando seus efeitos a todas as cláusulas constitucionais, inclusive o direito à privacidade, que é inerente à individualidade do ser humano. Diante dessa questão, é relevante mencionar o conceito apresentado por José Afonso da Silva (2009, p. 206), que entende o direito à privacidade como “conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito”.

Nesse sentido, fica evidente que o direito à privacidade assegura a proteção dos dados pessoais relacionados ao seu titular, que possui a liberdade de decidir mantê-los sob sua posse ou, se preferir, divulgá-los, estabelecendo limites e condições, sempre em conformidade com as provisões legais do sistema jurídico ao qual está subordinado. Por sua vez, a responsabilidade civil dos agentes de tratamento de dados pessoais diz respeito à obrigação desses agentes de agirem de forma adequada e responsável ao lidar com os dados pessoais dos indivíduos. Isso envolve o

cumprimento dos princípios e requisitos alcançados nas leis de proteção de dados, como a LGPD, bem como a adoção de medidas técnicas e organizacionais para proteger os dados contra acessos não autorizados, perdas ou violação de segurança.

## **A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO NA LGPD**

Considerando que a legislação vigente não se mostrava adequada para enfrentar os desafios emergentes do cenário atual, a LGPD foi criada para estabelecer um regime de responsabilidade civil específico para lidar com situações envolvendo danos decorrentes do tratamento de dados pessoais. A Lei Geral de Proteção de Dados Pessoais possui uma seção dedicada à responsabilização, abordando critérios para reparação de danos e circunstâncias que caracterizam um tratamento irregular. No entanto, ao contrário do Código de Defesa do Consumidor, a LGPD não especifica claramente um regime de responsabilidade civil que exija a comprovação de culpa para a concessão de indenização.

Enquanto o Código de Defesa do Consumidor estabelece a responsabilidade objetiva do fornecedor de serviços, tornando-o involuntariamente responsável por danos causados ao consumidor, independentemente de culpa, a LGPD não adota uma abordagem tão explícita. A lei não define se a responsabilidade dos agentes de tratamento por cometer violações de dados é objetiva (sem necessidade de comprovar culpa) ou subjetiva (havendo necessidade de comprovar culpa ou negligência).

A concepção de culpa está intrinsecamente associada à noção de responsabilidade, motivo pelo qual, em geral, ninguém pode ser alvo de censura ou juízo de reprovação sem ter negligenciado o dever de agir com cautela. Isso leva à conclusão de que a culpa é, conforme a perspectiva clássica, o elemento central da responsabilidade civil subjetiva. O Código Civil (Brasil, 2002), em seu artigo 186, mantém a culpa como base da responsabilidade subjetiva. Aqui, o termo “culpa” é utilizado em um sentido abrangente, englobando não apenas a culpa propriamente dita, mas também o dolo. Relevantes estudos surgiram, posteriormente, na Itália, Bélgica e, sobretudo, na França, defendendo uma responsabilidade objetiva, desvinculada da culpa, fundamentada na chamada teoria do risco. Essa abordagem foi igualmente adotada em certos casos pela legislação brasileira, e agora foi amplamente incorporada pelo Código Civil (Brasil, 2002), particularmente no parágrafo único do artigo 927, no artigo 931 e em outros dispositivos (Cavaliere Filho, 2012).

A legislação de proteção de dados estabelece um conjunto de princípios e diretrizes com o objetivo de promover um ambiente de responsabilidade preventiva. Isso significa que busca antecipar a ocorrência de danos na coleta e processamento de informações, especialmente diante dos desafios inerentes a uma sociedade cada vez mais orientada para a classificação de dados (Frazão, 2019). Entretanto, exige-se um sistema de responsabilidade civil capaz de garantir a proteção adequada da vítima e a completa reparação do dano.

O tema sobre responsabilidade e ressarcimento de danos atribuídos aos agentes responsáveis pelo tratamento de dados foi incluído na Seção III do Capítulo VI da Lei 13.709/2019 (Brasil, 2019). A introdução do artigo 42 estabelece a obrigação de indenização por danos patrimoniais, morais, individuais ou coletivos, aplicada aos responsáveis pelo controle e pela operação, quando ocorrerem violações à Lei Geral de Proteção de Dados (LGPD) durante as atividades de processamento de dados.



Assim como o Código de Defesa do Consumidor – Lei 8.078 (Brasil, 1990), a LGPD (Brasil, 2018) estabeleceu a solidariedade entre os agentes de tratamento que causarem lesão (art. 42, § 1º, I e II) e permitiu a inversão do ônus da prova por critério judicial (art. 42, § 2º) para equilibrar a relação entre controladores, operadores e titulares de dados pessoais.

A teoria da responsabilidade objetiva, conhecida como teoria do risco, opera de maneira independente da conduta do agente responsável pelo prejuízo. Nesse contexto, a focalização está na constatação do dano e na conexão causal com a ação do agente; uma vez estabelecida essa ligação, emerge a obrigação de efetuar a reparação (Rodrigues, 2002). A teoria do risco ganhou proeminência como reação à inadequação da responsabilidade subjetiva para abranger todas as situações de compensação. Isso se deve ao fato de que, em muitos cenários, a vítima não conseguia substanciar os elementos da responsabilidade civil, o que resultava em danos não ressarcidos (Pereira, 2018).

Como resposta a esse desafio, emergiu a doutrina objetiva, alicerçada na interrelação fundamental entre dano e autoria. Partindo desse pressuposto, os defensores da aplicação da responsabilidade objetiva no contexto da LGPD (Brasil, 2018) sustentam que o artigo 42 desse regulamento reflete a associação entre a obrigação de reparar danos e a realização do tratamento de informações pessoais.

De acordo com Tasso (2020), o dispositivo em questão não exclui nem prevê o elemento culpa e, em suas conclusões, enfatiza que apenas dois critérios objetivos são utilizados para fundamentar a responsabilidade: o exercício da atividade de tratamento de dados e a violação da legislação de proteção de dados (Tasso, 2020).

No artigo seguinte, a LGPD (Brasil, 2018) aborda as situações excepcionais da responsabilidade dos responsáveis pelo tratamento de dados, nas quais eles podem se isentar de responsabilidade mediante comprovação de que: i) não efetuaram o tratamento dos dados pessoais; ii) se realizaram o tratamento, este não violou as normas de proteção de dados pessoais; ou iii) o dano foi causado por terceiros ou pelo próprio titular dos dados (art. 43, incisos I a III, da Lei 13.709).

O art. 44 da LGPD (Brasil, 2018) conceitua o tratamento irregular de dados. Assim como o Código de Defesa do Consumidor (CDC), a LGPD definiu que o tratamento de dados será considerado irregular quando contrariar a disciplina legal ou, também, quando não fornecer a segurança legitimamente esperada pelo respectivo titular. A LGPD, em seu artigo 45, destaca, ainda, que as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Após a análise dos artigos 42 a 45 da LGPD (BRASIL, 2018), surgiram duas correntes interpretativas acerca da natureza da responsabilidade civil dos agentes de tratamento de dados pessoais: parte da doutrina, autores como Tasso (2020) e Guedes e Meireles (2019), defende que a responsabilidade civil relacionada ao tratamento de dados pessoais seria subjetiva, enquanto a posição divergente argumenta que a LGPD adotou o sistema de responsabilidade objetiva, baseada no risco, teoria defendida pelos autores Mendes e Doneda (2018). Deve-se o fato à aparente imprecisão normativa quanto ao sistema de responsabilidade civil adotado pela lei protetiva. O embate doutrinário é travado entre posições que afirmam ter a lei estabelecido um

sistema baseado na responsabilidade objetiva ou subjetiva, sendo respeitáveis os posicionamentos em ambos os sentidos (Tasso, 2020).

Ambas as correntes de interpretação possuem uma premissa comum, que é a alegação que a LGPD (Brasil, 2018) apresenta uma séria inexatidão terminológica, tendo em vista que o enunciado do artigo 42 não é suficientemente claro quanto ao regime de responsabilidade civil – subjetiva ou objetiva – adotado pela norma.

Segundo Mendes e Doneda (2018), autores que adotam a linha de responsabilidade civil objetiva, o argumento central reside no fato de que a atividade de tratamento de dados apresenta um risco intrínseco. Isso decorre da potencialidade significativa de danos em caso de violação dos direitos dos titulares, os quais são reconhecidos como direitos personalíssimos e fundamentais. Em resumo, o tratamento de dados pessoais seria considerado uma atividade de risco (Mendes; Doneda, 2018).

Outro argumento utilizado é o de que a responsabilidade não pode ser subjetiva, uma vez que o tratamento de dados pode ser realizado por entidades públicas, as quais estão sujeitas à responsabilidade objetiva. Conforme afirmam Novakoski e Napolini (2020):

Seria contraditório, ainda, que a LGPD permitisse que a responsabilidade civil decorrente de um mesmo fato objetivamente considerado – violação de normas de proteção de dados pessoais – pudesse ter tratamento diferenciado conforme a natureza do agente envolvido, isto é, subjetiva para agentes de direito privado e objetiva para entes de direito público, dado que, não tendo regulado explicitamente a responsabilidade civil destes últimos, a respectiva responsabilidade civil forçosamente observará a teoria do risco administrativo (art. 37, § 6º, CF/88), logo, será objetiva para os atos comissivos e subjetiva para os omissivos. (Novakoski; Napolini, 2020, p. 170).

De acordo com autores como Tasso (2020) e Guedes e Meireles (2019), a LGPD adota a teoria subjetiva da responsabilidade civil. Isso implica que é imprescindível provar a conduta culposa do agente de tratamento quando o dano ocorreu. Essa conduta culposa pode estar fundamentada em dois aspectos: (i) a omissão na adoção de medidas de segurança adequadas para o tratamento dos dados e (ii) o descumprimento das obrigações estabelecidas na lei (Tasso, 2020; Guedes; Meireles, 2019).

As autoras Guedes e Meireles argumentam que o Capítulo VI da LGPD (Brasil, 2018), que aborda as condutas a serem seguidas pelos agentes de tratamento de dados em relação a segurança, sigilo, boas práticas e governança de dados, constitui o fundamento para o reconhecimento da responsabilidade subjetiva (Guedes; Meireles, 2019).

Bioni e Dias (2020) propõem que, mais relevante do que uma análise dualista de responsabilidade, é examinar de forma mais detalhada os elementos normativos que restringiriam ou ampliariam a discussão de culpabilidade para fins de responsabilização. Deve-se, assim, avançar para além da análise binária do regime jurídico de responsabilidade civil da LGPD, julgando-o de natureza objetiva ou subjetiva. Isto porque, não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de

dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. Resultado parece ir no sentido de um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade (Bioni; Dias, 2020).

Desse modo, entende-se que a Lei Geral de Proteção de Dados adotou o sistema de responsabilidade civil subjetiva. Essa escolha é fundamental para fortalecer a cultura de proteção de dados no Brasil, conforme proposto pela própria lei. No entanto, é importante ressaltar que o agente de tratamento ainda pode ser responsabilizado objetivamente quando for comprovada a relação de consumo, de acordo com o Art. 45 da LGPD (Brasil, 2018), o qual estabelece que as violações no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas no CDC.

## CONSIDERAÇÕES FINAIS

O presente estudo, com base na literatura especializada, possibilitou entender que, ainda que a LGPD tenha esculpido um regime de responsabilidade civil subjetiva, não se pode negligenciar que as barreiras para a deflagração do dever de indenizar foram substancialmente diminuídas; em particular, diante da presunção automática legal da culpa do lesante, a qual pode ser somada à inversão do ônus da prova em juízo quanto aos demais pressupostos da responsabilidade civil.

Além disso, em termos de contribuições, é importante considerar uma abordagem flexível em relação à ideia de tratamento irregular, especialmente quando se trata da responsabilidade dos responsáveis pelo processamento de dados pessoais em utilizar as técnicas disponíveis na época do tratamento. Isso inclui evitar um alto grau de negligência em relação ao estado atual das práticas e tecnologias, conforme já discutido na área do direito consumidor, então se tornará extremamente difícil o agente de tratamento de dados afastar a sua culpa.

Em poucas palavras, deve-se avançar para além da constatação se o regime jurídico de responsabilidade civil da LGPD é de natureza objetiva e ou subjetiva. Isso porque não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. Ainda que possa parecer paradoxal, o resultado pode ser um regime jurídico de responsabilidade civil subjetiva com uma espécie de alto grau de objetividade.

A presente pesquisa apresentou limitações, especialmente no que concerne à falta de jurisprudência discorrendo sobre o assunto, visto que a entrada em vigor da referida lei ainda é relativamente recente. Nesse contexto, estudos futuros sobre como os tribunais pátrios têm se posicionado sobre o assunto poderão ser realizados para aprofundar o conhecimento acerca do tema.

## REFERÊNCIAS

- AGÊNCIA SENADO. **Lei Geral de Proteção de Dados entra em vigor. 2020.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>. Acesso em: 20 mar. 2023.
- BIONI, Bruno Ricardo; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, ano 9, n.3, p.1-23, 2023.
- BRASIL. **Constituição. República Federativa do Brasil de 1988.** Brasília, DF: Senado Federal, 1988. Disponível em: [www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 23 maio 2023.
- BRASIL. Lei 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 20 maio 2023.
- BRASIL. Lei 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l9296.htm](https://www.planalto.gov.br/ccivil_03/leis/l9296.htm). Acesso em: 20 maio 2023.
- BRASIL. Lei 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l9507.htm](https://www.planalto.gov.br/ccivil_03/leis/l9507.htm). Acesso em: 20 maio 2023.
- BRASIL. Lei 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/2002/l10406compilada.htm](https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm). Acesso em: 20 maio 2023.
- BRASIL. Lei 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm). Acesso em: 20 maio 2023.
- BRASIL. Lei 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm). Acesso em: 21 maio 2023.
- BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 20 mar. 2023.
- BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 20 mar. 2023.
- BRASIL. Lei 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em:

[https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/l13853.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm). Acesso em: 20 mar. 2023.

BRASIL. Medida Provisória 954, de 17 de abril de 2020. Disponível em [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/mpv/mpv954.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm). Acesso em: 19 abr. 2023.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. Revista e Ampliada. 10. ed. São Paulo: Atlas, 2012.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância na Lei Geral de Proteção de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Viviane da Silveira. Capítulo 10: Compliance de dados pessoais. A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. **Revista dos Tribunais**, 2019.

GIL, A. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Mele Venceslau. Término do tratamento de dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**. São Paulo: Editora RT, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, ano 27, nov.-dez. 2018.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, v. 1009, nov. 2019.

MORAES, Alexandre de. **Direitos humanos fundamentais**. 4. ed. São Paulo: Jurídico, 2002.

NOVAKOSKI, André Luis Mota; NASPOLINI, Smyra Haydêe Dal Farra. Responsabilidade civil na LGPD: problemas e soluções. **Conpedi Law Review**, Florianópolis, v. 6, n. 1, p. 158-174, 2020.

PEREIRA, Caio Mario. **Responsabilidade civil**, 12. ed. Grupo GEN, 2018.

RODRIGUES, Silvio. **Direito civil: responsabilidade civil**, v. 4, 19. ed. São Paulo: Saraiva, 2002.

SCHREIBER, Anderson. **Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais**. Tratado de proteção de dados pessoais. Editora Forense, 2020.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 32. ed. São Paulo: Malheiros, 2009.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, ano 21, nº 53, p. 97-115, jan./mar. 2020.