

LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE
CURSO DE GRADUAÇÃO EM DIREITO

GUILHERME EDUARDO ARAÚJO DA NÓBREGA COUTINHO

**O REGIME JURÍDICO DA RESPONSABILIDADE CIVIL DOS AGENTES DE
TRATAMENTO DE DADOS NA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD
(LEI Nº 13.709/2018)**

NATAL/RN

2022

GUILHERME EDUARDO ARAÚJO DA NÓBREGA COUTINHO

**O REGIME JURÍDICO DA RESPONSABILIDADE CIVIL DOS AGENTES DE
TRATAMENTO DE DADOS NA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD
(LEI Nº 13.709/2018)**

Trabalho de Conclusão de Curso (Direito)
apresentado ao Centro Universitário do
Rio Grande do Norte (UNI-RN) como
requisito final para obtenção do título de
Bacharel em Direito

Orientador: Prof. Msc. Leonardo
Medeiros Júnior

NATAL/RN

2022

GUILHERME EDUARDO ARAÚJO DA NÓBREGA COUTINHO

**O REGIME JURÍDICO DA RESPONSABILIDADE CIVIL DOS AGENTES DE
TRATAMENTO DE DADOS NA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD
(LEI Nº 13.709/2018)**

Trabalho de Conclusão de Curso (Direito)
apresentado ao Centro Universitário do
Rio Grande do Norte (UNI-RN) como
requisito final para obtenção do título de
Bacharel em Direito

Aprovado em: ____/____/____

BANCA EXAMINADORA

Prof. Msc. Leonardo Medeiros Júnior
Orientador

Prof. Msc. Abraão Luiz Filgueira Lopes

Prof. Msc. Matusalém Jobson Bezerra Dantas

Às minhas avós, Rita Margarida de Araújo - Vovó Rita (*in memorian*) e Elisabeth da Nóbrega Coutinho - Vovó Beta (*in memorian*), que, caso cá estivessem, neste plano material de passagem efêmera, acalentariam meus temores durante o desenvolvimento do presente trabalho e regozijar-se-iam com a minha alegria ao finaliza-lo.

AGRADECIMENTOS

Aos meus pais Francisco e Luciana, pelos princípios e valores que norteiam minha vivência diária, pelas renúncias e sacrifícios que fizeram nos últimos vinte anos para proporcionar-me a mais zelosa criação, pelo amor e afeto que tornam porto seguro o ambiente familiar, pelo cuidado e preocupação ao longo da realização desta pesquisa.

Aos meus irmãos Nathália e Francisco, pelo incentivo fraternal e pela constante lembrança, nos momentos de imersão na produção deste trabalho, de que nem tudo a ele se resumia.

A minha família, em nome de meus avós Júlio, Elisabeth (*in memorian*), Luciano e Rita (*in memorian*), pelo ensinamento que a gratidão é a maior das virtudes e o mais nobre dos sentimentos.

A Lais, pelo companheirismo, apoio e compreensão incondicionais nos últimos quatro anos e, em especial, durante a escrita deste trabalho.

No âmbito acadêmico, Ao professor Leonardo, pela pronta aceitação diante do convite em orientar esta pesquisa e por ter, ao longo deste semestre, fornecido subsídios para seu desenvolvimento e conclusão.

A Lucas, pela paciência e atenção nas discussões sobre os elementos deste trabalho.

Aos amigos que o Colégio Salesiano Dom Bosco, direta e indiretamente, me deu, pela estima e encorajamento ao longo da jornada, conferindo-me a convicção necessária à finalização deste trabalho, e por não terem admitido que eu esquecesse do quanto a vida é melhor ao lado dos amigos.

Aos amigos do Centro Universitário do Rio Grande do Norte, por terem compartilhado ao longo do curso as angústias e alegrias intrínsecas a formação acadêmica e à escrita do trabalho de curso, pelas contribuições e convivência diária.

Aos amigos do curso de História da Universidade Federal do Rio Grande do Norte, por possibilitarem os indispensáveis alheamentos a este trabalho, viabilizadores de um retorno mais produtivo à presente pesquisa.

Aos que integraram, até 2008, a 3ª Vara Cível da Comarca de Mossoró/RN, por terem sido minhas primeiras referências no âmbito jurídico e, até hoje, se fazerem presentes na minha formação.

A todos que não foram diretamente citados, mas que contribuíram para a consecução deste trabalho de curso.

Fazer o que seja é inútil.
Não fazer nada é inútil.
Mas entre fazer e não fazer
mais vale o inútil do fazer.
Mas não, fazer para esquecer
que é inútil: nunca o esquecer.
Mas fazer o inútil sabendo
que ele é inútil e que seu sentido
não será sequer pressentido,
fazer: porque ele é mais difícil
do que não fazer, e difícil-
mente se poderá dizer
com mais desdém, ou então dizer
mais direto ao leitor Ninguém
que o feito o foi para ninguém.

João Cabral de Melo Neto

RESUMO

A pesquisa tem por finalidade analisar o regime jurídico de responsabilidade civil dos agentes de tratamento de dados pessoais, previsto entre os arts. 42 e 44 da Lei Geral de Proteção de Dados – LGPD. Isso porque não há, no texto legal, menção expressa à modalidade de responsabilização do violador de suas disposições normativas. Procedeu-se à análise do referido instrumento regulador específico (Lei nº 13.709/2018) e das normas que lhe são correlatas, assim como à investigação da doutrina que trata sobre responsabilidade civil e LGPD. Tratou-se acerca dos conceitos necessários para a compreensão do microssistema de proteção de dados pessoais no ordenamento jurídico brasileiro, tais como os conceitos de “dados”, “informação”, “tratamento de dados”, “titular de dados” e “agentes de tratamento”. Discutiu-se a modalidade de responsabilidade civil imputável aos agentes de tratamento de dados no contexto de efetivação do direito fundamental à proteção de dados, se objetiva, decorrente do risco da atividade empenhada, se subjetiva, centrado no elemento da culpa, ou, ainda, se constituída a partir de um regime diferenciado, calcado, por exemplo, na prevenção. Através do método dedutivo, concluiu-se que não há uniformidade no âmbito doutrinário acerca do regime de responsabilidade civil imputável aos agentes de tratamento de dados. Ademais, verificou-se que o tema ainda não foi apreciado no Superior Tribunal de Justiça e no Supremo Tribunal Federal, o que ocasiona insegurança jurídica para os destinatários da legislação.

Palavras-chave: Lei Geral de Proteção de dados. Dados pessoais. Agentes de tratamento. Responsabilidade Civil. Regime jurídico de responsabilização.

ABSTRACT

The purpose of the research is to analyze the legal regime of civil liability of agents processing personal data, provided for in articles 42 and 44 of the General Data Protection Act – GDPR. This is because, in the legal text, there is no express mention of the mode of accountability of the violator of its normative provisions. An analysis of the aforementioned specific regulatory instrument (Law no. 13.709/2018) and the norms related to it was carried out, as well as an investigation of the doctrine that deals with civil liability and the GDPR. The article dealt with the concepts necessary for understanding the personal data protection microsystem in the Brazilian legal system, such as the concepts of "data", "information", "data processing", "data holder" and "data agents". The type of civil liability attributable to data processing agents in the context of the realization of the fundamental right to data protection was discussed, whether objective, arising from the risk of the committed activity, or subjective, centered on the element of guilt, or, even, constituted from a differentiated regime, based, for example, on prevention. Through the deductive method, it was concluded that there is no uniformity in the doctrinal scope regarding the civil liability regime attributable to data processing agents. In addition, it was found that the issue has not yet been considered by the Superior Court of Justice and the Federal Supreme Court, which causes legal uncertainty for the recipients of the legislation.

Keywords: General Data Protection Act. Personal data. Treatment agents. Civil responsibility. Legal regime of accountability.

SUMÁRIO

1. INTRODUÇÃO.....	9
2. DA PRIVACIDADE AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS.....	13
3. PANORAMA HISTÓRICO: A TRAJETÓRIA DA PROTEÇÃO DE DADOS NO MUNDO E NO BRASIL	17
3.1 NO MUNDO	17
3.2 NO BRASIL.....	24
4. A LEI Nº 13.709/2018: LEI GERAL DE PROTEÇÃO DE DADOS – LGPD. 29	
4.1 OBJETIVOS, FUNDAMENTOS E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD.....	29
4.2 DADOS NA LGDP	31
4.3 TRATAMENTO DE DADOS.....	35
4.4 TITULAR DE DADOS.....	36
4.5 AGENTES DE TRATAMENTO: CONTROLADOR E OPERADOR.....	39
5. BASES LEGAIS: HIPÓTESES AUTORIZATIVAS DO TRATAMENTO DE DADOS PESSOAIS.....	45
6. REGIME JURÍDICO DE RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS NA LGPD.....	55
6.1 RESPONSABILIDADE CIVIL.....	56
6.2 DA REGULAMENTAÇÃO DA RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS NA LGPD.....	57
6.3 CORRENTES DOUTRINÁRIAS DE INTERPRETAÇÃO QUANTO AO FUNDAMENTO DA RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS NA LGPD.....	59
6.3.1 Responsabilidade Objetiva	60
6.3.2 Responsabilidade Subjetiva	64
6.3.3 Responsabilidade a partir de regime diferenciado (aversão à culpa, ao risco e concepções dualistas)	70
7. CONSIDERAÇÕES FINAIS.....	75
REFERÊNCIAS.....	79

1. INTRODUÇÃO

A Revolução Técnico-Científica-Informacional, cujo início remete à segunda metade do século XX, demarca um vertiginoso desenvolvimento do processo produtivo, das relações interpessoais e do campo científico a partir dos avanços tecnológicos em diversas áreas, destacadamente nos campos da eletrônica, informática e robótica.

Desde então, o fenômeno da globalização está relacionado a integração mundial a partir do estabelecimento de redes e canais de comunicação com fluxos informacionais dinâmicos e de longo alcance, atingindo um número cada vez mais amplo de pessoas a partir da democratização do acesso aos meios digitais e às novas tecnologias, culminando na constituição da denominada “Sociedade da Informação”, na qual a fonte de produtividade e exercício de poder consubstanciam-se na produção, processamento e propagação de dados e informações.

No sentido de disseminação do aparato tecnológico, a Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2019, realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), demonstrou que 82,7% dos domicílios brasileiros possuem acesso à internet, sobrevivendo crescimento da conexão aos meios digitais em todas as regiões do País, na mesma medida em que, por outro lado, foram elevadas as taxas de vazamento de dados de titularidade de cidadãos brasileiros (GOV.BR, 2021). É o que demonstra pesquisa divulgada em 2021 pelo Massachusetts Institute of Technology (MIT), conduzida pelo pesquisador brasileiro Nelson Novaes Neto, na qual constatou-se que mais 205 milhões de dados pertencentes a brasileiros foram vazados, apenas de forma criminosa, em 2019, o que representa um aumento de 493% em relação aos dados violados no ano pretérito (BORGES et al, 2021).

Nesse contexto, faz-se mister a discussão acerca da proteção de dados pessoais e da responsabilização dos agentes encarregados por seu tratamento no ordenamento jurídico brasileiro.

Todavia, quanto à temática, vagaroso foi o processo de incorporação de instrumento regulador específico à legislação pátria, concretizado apenas com a elaboração da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709, de 14 de agosto de 2018), cuja vigência plena iniciou em 1º de agosto de 2021, 1.082 dias após a publicação da Lei no Diário Oficial da União, em 15 de agosto de 2019.

A despeito da morosidade do Poder Legislativo em instituir regulamentação própria à proteção de dados, a LGPD constituiu-se como elemento central de um marco regulatório sistematizador da proteção de dados pessoais no território nacional, inclusive no meio digital, com a finalidade de salvaguardar os direitos fundamentais de proteção de dados pessoais, de liberdade, de privacidade e de autodeterminação informativa, anteriormente adstritos, explícita ou implicitamente, a abordagem constitucional ou a leis esparsas.

Ainda assim, a LGPD, ao tratar sobre a responsabilidade dos agentes de tratamento de dados e o ressarcimento de danos causados aos titulares de dados, conteúdo disciplinado entre artigos 42 e 45 da Lei, constantes na seção III (“Da responsabilidade e do Ressarcimento de Danos”) do capítulo VI (“DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS”), ficou silente quanto ao regime de responsabilidade dos agentes de tratamento de dados nas hipóteses de violação aos seus dispositivos legais.

Desta forma, é ininteligível o critério adotado para responsabilização do agente de tratamento de dados violador das disposições normativas da LGPD; se objetivo, decorrente do risco inerente à atividade de tratamento de dados, se subjetivo, centrado no elemento da culpa, ou, ainda, se calcada em outro pressuposto que destoe das modalidades clássicas de responsabilidade civil, a exemplo do regime de responsabilidade proativo, assentado na prevenção.

A opção por uma das modalidades de responsabilidade civil impactará diretamente nos titulares que alegarem violação de seus dados e nos agentes de tratamento alegadamente violadores, na medida em que influirá nos elementos direta e indiretamente relacionados à averiguação da responsabilidade dos agentes de tratamento de dados no curso de ação judicial, a exemplo da distribuição do encargo probatório, diferenciada em cada regime de responsabilidade.

Nesse aspecto, a previsão de responsabilidade civil na LGPD provoca interpretações distintas no meio doutrinário, uma vez que não há menção expressa ao regime de responsabilidade civil dos agentes de tratamento de dados, de forma que os teóricos, com o intento de solver a problemática e consolidar uma modalidade de responsabilidade civil à hipótese, subjetiva, objetiva ou diferenciada, buscam desvendá-lhe a hermenêutica respectiva.

De igual maneira, não fora, até o momento, sedimentado entendimento na jurisprudência acerca da responsabilidade civil no contexto dos casos regulamentados

pela LGPD, com escopo de fundamentar a imputação da obrigação de ressarcir os danos causados aos titulares respectivos, de maneira que pertinente o debate acerca do regime de responsabilidade civil imputável aos agentes de tratamento de dados no âmbito de incidência da LGPD a fim de efetivar o direito fundamental à proteção de dados (art. 5º, LXXIX, CRFB/1988), pelo que se justifica a realização desta pesquisa.

Diante do contexto supramencionado, o objetivo do presente trabalho reside em analisar as modalidades de responsabilidade civil, objetiva, subjetiva, e espécies diversas, potencialmente aplicáveis aos agentes de tratamento de dados na LGPD quando, violando à legislação de proteção de dados pessoais, em razão do exercício de atividade de tratamento de dados pessoais, causarem dano de ordem patrimonial, moral, individual ou coletivo a outrem. Não há, entretanto, pretensão de formular solução definitiva para problemática, uma vez que, conforme descrito acima e detalhado oportunamente, variadas e distintas são as perspectivas legitimadas pelos estudiosos do tema, considerando-se precipitado o peremptório deslinde da problemática na conjuntura hodierna, dada a inovação trazida pelo dispositivo normativo em comento, bem como a atualidade das discussões que o sucederam.

Os objetivos específicos consubstanciam-se em: *i)* Analisar, a partir do fenômeno histórico, os fatores que impulsionaram o processo de constitucionalização da proteção de dados enquanto direito fundamental e de elaboração dos sistemas legislativos de proteção de dados no Brasil e no mundo; *ii)* Perquirir, no âmbito da LGPD, o modo como delineados conceitos jurídicos essenciais à pesquisa (dados, proteção de dados pessoais, titular de dados pessoais, agentes de tratamento de dados, bases legais); *iii)* Evidenciar a forma como a responsabilidade civil dos agentes de tratamento de dados foi abordada na LGPD, de modo a explicitar a omissão legislativa abarcada na redação dos dispositivos; *iv)* Examinar as correntes doutrinárias estruturadas acerca do regime de responsabilidade civil dos agentes de tratamento de dados na LGPD;

O presente trabalho utiliza-se do método dedutivo, partindo do direito fundamental à Proteção de Dados e da LGPD, para analisar as modalidades de responsabilidade civil potencialmente definidoras do regime jurídico de responsabilidade civil aplicável aos agentes de tratamento de dados no âmbito da LGPD, contemplando os métodos de procedimento analítico e comparativo.

Para tanto, vale-se de pesquisa bibliográfica, a partir de investigação doutrinária, análise dos dispositivos da LGPD (Lei nº 13.709, de 2018) e das normas correlatas a regulamentação da responsabilidade civil dos agentes de tratamento de dados, a exemplo

do Código Civil de 2002 (Lei nº 10.406, de 2002) e do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).

2. DA PRIVACIDADE AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

A tutela da privacidade constitui-se como marco inaugural da defesa contra a ingerência indesejada de outrem na esfera pessoal do sujeito de direito, conferindo “ao indivíduo a possibilidade de conduzir sua própria vida da maneira que julgar mais conveniente, sem intromissão da curiosidade alheia” (NOVELINO, 2016, p.337), o que está intrinsecamente relacionado ao constitucionalismo moderno, depreendido entre o final do século XVIII e a metade do século XX, a partir da consagração, nas constituições liberais, dos direitos fundamentais de primeira geração, associados, sobretudo, ao valor da liberdade (NOVELINO, 2016).

A proteção de dados pessoais, por sua vez, denota um desdobramento contemporâneo do direito à privacidade, tendo em vista que a proteção de dados pessoais visa, em suma, a proposição do “tema da privacidade, porém, modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão.” (DONEDA, 2020, p. 144).

A afirmação dos dados pessoais enquanto bem jurídico de elevado potencial econômico, sendo concebido, conforme assinalado por Mendlowicz e Ribeiro (2020), como o “novo petróleo”, isto é, um recurso de elevado potencial econômico, fomentador da economia digital, evidencia a atividade de tratamento de dados, empreendida em massa na conjectura contemporânea, como iminentemente invasiva à esfera pessoal, ensejando a formulação e desenvolvimento de mecanismos normativos de proteção de dados pertinentes aos desafios da era digital, as quais implicam em reformas legislativas que obstem a exploração de dados como mero instrumento mercadológico.

Nesse ínterim, a proteção de dados, segundo Quintiliano (2022a), era tida, até a vigência da Emenda Constitucional nº 115, em 11 de fevereiro de 2022, como princípio constitucional implícito, decorrente dos direitos fundamentais à privacidade (art. 5º, X, CRFB/1988), à intimidade (art. 5º, X, CRFB/1988), ao sigilo de dados (art. 5º, XII, CRFB/1988) e à Dignidade da Pessoa Humana (Art. 1º, III, CRFB/1988).

A alteração formulada pela referida Emenda Constitucional nº 115, culminou, contudo, na constitucionalização do direito à proteção de dados, o qual passou a integrar o rol de direitos e garantias fundamentais constantes no artigo 5º da Constituição da República Federativa do Brasil de 1988 (CRFB/1988):

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a

inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...)

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Quintiliano (2022a) entende que desnecessária fora a inclusão do direito à proteção de dados no rol de direitos fundamentais do artigo 5º da CRFB/1988, uma vez que, como retromencionado, constituía-se como princípio constitucional implícito, decorrente de direitos fundamentais reconhecidos não apenas pela CRFB/1988 mas também por tratados internacionais, tais quais a Convenção Americana de Direito Humanos, usualmente denominada Pacto de San José da Costa Rica, de 1969, e a Declaração Universal dos Direitos Humanos, de 1948.

Salienta o autor que o direito à privacidade transcende a proteção à vida íntima do indivíduo, albergando, também os seus dados pessoais, uma vez que estes exprimem abrangente projeção da personalidade humana. Acrescenta que a constitucionalização do direito à proteção de dados decorre do clamor de parcela da sociedade civil, a qual crê ganho efetivo a partir de sua inserção expressa no texto constitucional. Não obstante, ao reforçar que o direito à proteção de dados era princípio implícito na CRFB/1998, assegurado por uma gama de direitos fundamentais, Quintiliano (2022a) não vislumbra expressivo ganho de proteção jurídica em seu reconhecimento expresso, excepcionando o ganho semântico, dada a integração ao texto constitucional. Exprime que outros direitos fundamentais acrescentados à CRFB/1988 por meio de emendas constitucionais, como o direito à alimentação (art. 6º), verificaram minguadas alterações efetivas após incorporação ao texto constitucional, ainda que reconhecidos em tratados internacionais.

Assente, todavia, que a constitucionalização de determinados direitos viabiliza a composição de uma esfera de compromisso interinstitucional, conferindo-lhes maior relevância e primado no âmbito normativo, o que não se configura na hipótese da proteção de dados, pois, no Brasil, subsiste avançada legislação que densifica o princípio.

Chaves (2022), por sua vez, denota que no contexto contemporâneo de informatização da sociedade e desenvolvimento tecnológico, nos quais os dados pessoais são operados como ativo comercial e reserva de valor, a constitucionalização do direito à proteção de dados representa um marco histórico apto a fomentar um desenvolvimento econômico e tecnológico circunscrito aos ditames constitucionais e legais.

A autora enuncia que a proteção de dados, ao ser alçada ao patamar constitucional, não poderá sofrer retrocessos ou restrições pelas autoridades

governamentais, as quais deverão assegurar a efetividade do direito, tendo em vista que, como destaca Novelino (2016), os direitos fundamentais tem por características a inalienabilidade, configurando-se como direitos inegociáveis, intransferíveis e indisponíveis; e a irrenunciabilidade, isto é, não admitem a abdicação ao seu núcleo substancial em abstrato.

A CRFB/1988, segundo Chaves (2022), intentou preservar os direitos fundamentais à privacidade (art. 5º, X, CRFB/1988), à intimidade (art. 5º, X, CRFB/1988), ao sigilo de dados (art. 5º, XII, CRFB/1988). A garantia de direitos fundamentais decorre, contudo, de um contexto histórico-cultural de uma sociedade, objetivando-se a dignidade do indivíduo, capacitando-o a desenvolver-se plenamente em meio aos seus semelhantes. Novelino (2016), ao abordar os atributos inerentes aos direitos fundamentais, explicita que a historicidade é qualidade a eles imanente, dados o surgimento e desenvolvimento dos direitos fundamentais conforme um contexto histórico, o que afasta, juntamente a eventualidade de modificação em suas formas e conteúdos no curso da história, a concepção jusnaturalista imputada a esses direitos.

Nesse aspecto, Chaves (2022) exprime que os direitos constitucionais preexistentes não se mostravam hábeis a englobar a conjuntura digital hodierna, uma vez que a realidade social experimentada em 1988, ano de promulgação da CRFB/1988, em muito diverge da verificada atualmente. A autora manifesta que a sociedade contemporânea interrelaciona-se indissociavelmente por meio das tecnologias da comunicação, de modo que as interações são pautadas na troca de informações, coleta de dados ou análise de perfis e hábitos. À vista disso, conclui Chaves (2022) que o status de direito fundamental conferido ao direito à proteção de dados acarreta benefícios a todos os cidadãos brasileiros, atribuindo maior relevância e solidificação ao tema.

Doneda (2020), ao formular, em momento anterior ao ingresso do direito à proteção de dados pessoais no rol de direitos fundamentais do artigo 5º da CRFB/1988, questionamento acerca da possibilidade de consideração da existência de tutela constitucional (implícita) da proteção de dados pessoais a partir da preexistente tutela constitucional da privacidade, já considerava:

Se derivarmos a proteção de dados pessoais diretamente da privacidade, tal qual espécie e subespécie, poderíamos sustentar existir uma extensão da tutela da privacidade à proteção de dados pessoais, sendo esta última uma espécie de mão longa da primeira. Tal operação, se bastaria para abarcar a disciplina sob a égide constitucional, acaba por simplificar demasiadamente os fundamentos da tutela de dados pessoais, o que pode eventualmente limitar o seu alcance. (DONEDA, 2020, p. 267).

O autor denota, ainda, que eventual incorporação do direito à proteção de dados no rol de direitos fundamentais da CRFB/1988, de fato ocorrida, proporcionaria a isonomia essencial à proteção das liberdades individuais entre o direito à proteção de dados e uma gama de outros direitos que possuem repercussão direta sobre os dados pessoais, tais quais o direito à privacidade, o direito à informação e a transparência.

Assim, a garantia constitucional do direito à proteção de dados, nos termos da norma específica, fomentou o debate sobre a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), regulamentadora do tratamento de dados pessoais, inclusive nos meios digitais, e sobre os elementos que lhe são correlatos, tendo em vista que as disposições da LGPD incidem em diversas áreas do conhecimento jurídico.

3. PANORAMA HISTÓRICO: A TRAJETÓRIA DA PROTEÇÃO DE DADOS NO MUNDO E NO BRASIL

3.1 NO MUNDO

O direito à proteção de dados, enquanto implícito no direito à privacidade, já encontrava guarida no artigo 12 da Declaração Universal dos Direitos Humanos, de 1948, ainda que de forma velada e genérica. Considera-se, de igual maneira, que a Convenção Americana de Direito Humanos, usualmente denominada Pacto de San José da Costa Rica, de 1969, em seu artigo 11, ponto 2, consagrou expressamente o direito à privacidade, o que implica, conseqüentemente, no reconhecimento subjacente do direito à proteção de dados (QUINTILIANO, 2022b). Remetendo-se ao passado, sem, contudo, precisar uma data concreta, Almeida e Lugati (2020, p.3) definem que as discussões acerca do que contemporaneamente é conhecido privacidade originaram-se a partir do momento no qual as tecnologias “se tornaram invasivas, dando margem à divulgação de informações da esfera privada do indivíduo.”

Dessa feita, enquanto os debates sobre os limites da ingerência de outrem na vida privada dos sujeitos de direito eram potencializados e consolidados em tratados internacionais e legislações nacionais, não se vislumbrava, até a década de 1970, o direito à proteção de dados como um direito autônomo, mas como consectário do direito à privacidade (DONEDA, 2021).

Nesse aspecto, Doneda (2021), ao explanar e distinguir os precedentes e fundamentos para a emergência e sedimentação do direito à proteção de dados como um direito autônomo e fundamental de caráter global, destaca os itinerários trilhados nos Estados Unidos da América e na Europa.

Alude, inicialmente, que os Estados Unidos da América detêm em seu ordenamento jurídico consolidada tradição no que concerne ao direito à privacidade, do qual derivam alguns dos mais representativos institutos atinentes à proteção de dados (DONEDA, 2021).

A gênese desta tradição remonta ao ano de 1890, com a publicação do artigo “*The right to privacy*”, de Samuel Warren e Louis Brandeis, o qual constatou, a partir de um compilado de precedentes sobre privacidade, que o assunto já ocupava, de forma dissociada, as cortes do país, erigindo-se, a partir disso, a tese denominada *right to be let alone* – o direito a ser deixado só (DONEDA, 2021).

O autor assevera que a relevância do artigo na contemporaneidade, ainda que passados mais de cento e trinta anos de sua publicação original, decorre da constatação, em excerto do artigo, de vínculo da tutela da privacidade ao progresso tecnológico (DONEDA, 2021).

Denota-se, nesse sentido, que o progresso viabiliza novas maneiras de veiculação e obtenção de informações sobre pessoas, “sendo o vetor principal que proporcionou a demanda pela elaboração de um direito à privacidade, que veio a se consolidar em diversos ordenamentos jurídicos desde então.” (DONEDA, 2021, p. 24).

Dessa forma, Doneda (2021), expressa que ao longo da primeira metade do século XX, constituiu-se, na jurisprudência estadunidense, um moroso, porém ininterrupto, assentamento do direito à privacidade, o qual era pautado, segundo Almeida e Lugati (2020, p. 4) por um cunho fortemente individualista e pela concepção que constitui-se como direito negativo, de tal maneira que o direito à privacidade “estaria sendo garantido desde que o Estado se abstinhasse de adentrar na esfera individual de cada um”, perspectiva vinculada à primeira geração de direitos fundamentais, originária da Revolução Francesa, depreendia entre 1789 e 1799, a qual aclamava o direito à liberdade.

Na década de 1960, contudo, adveio concreta inquietação devido a eclosão e desenvolvimento do processamento automatizado de dados pessoais e bancos de dados informatizados nos Estados Unidos da América (DONEDA, 2021). Isso porque, no período, o autor destaca que:

a tecnologia, que começava a ser determinante para a definição dos limites do direito à privacidade, passasse a ser a informática. Com a informática, veio também a mudança nos próprios postulados da matéria, com a concentração do seu objeto cada vez maior nos dados pessoais em si do que no caráter subjetivo das considerações quanto à violação da privacidade. (DONEDA, 2021, p. 25).

O estopim para que os riscos à liberdade e privacidade advindos do processamento informatizado de dados fossem debatidos no congresso dos Estados Unidos da América e, posteriormente, em todo o mundo, fora o *National Data Center*, um projeto de construção de base de dados centralizada no país, que não progrediu em razão da verificação da ausência de mecanismos regulatórios aptos a assegurar os direitos dos cidadãos hodiernamente referenciados, no que tange ao direito à proteção de dados pessoais, como titulares de dados pessoais (DONEDA, 2021). Almeida e Lugati (2020, p.4), nesse sentido, atestam que, com o advento do tratamento informatizado de dados e o enfoque a ele conferido, o entendimento sobre a abrangência do direito à

privacidade fora remodelado para abarcar a proteção de dados, o que não se mostrou suficiente, tendo em vista que no curso da década de 1970 surgiram as primeiras decisões judiciais e legislações que conferem à proteção de dados o *status* de direito autônomo, considerando que “dados pessoais são uma projeção da personalidade do indivíduo e por isso são hábeis a receber tutela jurídica.”

Doneda (2021, p.26), menciona, nessa perspectiva, que o *National Data Center* não fora o único caso motivador do debate sobre a proteção de dados pessoais, complementando que:

A herança mais sistemática desse período é o relatório compilado em 1973 pelo Departamento de Saúde, Educação e Bem-Estar (*Department of Health, Education and Welfare – HEW*), denominado *Records, Computers and the Rights of Citizens. Report of the Secretary’s Advisory Committee on Automated Personal Data Systems*, no qual se propõe a observância dos *Fair Information Practice Principles*, algo como “princípios para o tratamento leal da informação” que, além de sugerir fortemente a adoção de uma normativa federal para a proteção de dados nos Estados Unidos, enunciou alguns dos princípios que, até hoje, formam a espinha dorsal da grande maioria dos marcos regulatórios de proteção de dados, como os princípios da finalidade, livre acesso, transparência, segurança e qualidade/correção.

A partir desses casos paradigmáticos, o interesse pela tutela da privacidade e, além disso, pela proteção dos dados pessoais, expandiu-se e democratizou-se, ensejando crescente disposição da população em ter seus dados pessoais efetivamente preservados frente ao avanço tecnológico que viabilizava o tratamento de dados pessoais em massa, fosse pelo Estado, fosse por entidades privadas (ALMEIDA; LUGATI, 2020)

Os Estados Unidos da América estabeleceram, assim, sobretudo através da formulação de precedentes jurisprudenciais e da atuação institucional do Poder Executivo, as bases para a estruturação de um sistema jurídico de proteção de dados pessoais.

É, contudo, no território europeu que surgem, de fato, os primeiros marcos regulatórios ensejadores do desenvolvimento da proteção de dados pessoais como modelo normativo autônomo, demarcando-se que as deliberações legislativas e os precedentes jurisprudenciais que constituem a disciplina jurídica da proteção de dados como tal vem sendo edificadas há, pelo menos, cinco décadas (DONEDA, 2020), frisando-se que, em sendo um desdobramento contemporâneo do direito à privacidade, além de essencialmente vinculada à direitos individuais, a estruturação autônoma da proteção de dados pessoais principiou-se com a constituição do processamento automatizado de dados como um fator de risco, por si só, ao indivíduo (DONEDA, 2021).

Nesse aspecto, o autor utiliza o recurso doutrinário da classificação por gerações para desvelar o desenvolvimento das legislações de proteção de dados.

A primeira geração de leis cujo objeto era a proteção de dados pessoais, trazendo reflexos dos Estados Modernos à segunda metade do século XX, conforme preconizado por Almeida e Lugati (2020), acautelava os direitos dos titulares de dados em face do Estado, que assumia a condição de administrador dos dados de seus cidadãos, evidenciando a condição tecnológica e a visão dos juristas à época, acreditando-se que a coleta ilimitada de dados pessoais, efetivada em larga escala quase que exclusivamente pelo Estado em centros de tratamento de dados, ameaçava direitos e garantias fundamentais (DONEDA, 2020). O Estado, fora, assim, preponderantemente, os destinatários das primeiras regulamentações que tutelavam o direito à proteção de dados pessoais (ALMEIDA; LUGATI, 2020).

O elo inaugural das legislações precursoras no que concerne à proteção de dados pessoais foi a Lei de Proteção de Dados do *Land* alemão de Hesse, de 1970, seguida pela Estatuto para bancos de dados de 1973 – *Data Legen 289*, ou *Datalag*, primeira lei nacional de proteção de dados, editado na Suécia e, no âmbito dos Estados Unidos da América, o *Privacy Act*, de 1974, diametralmente relacionado ao caso do *National Data Center*, estendendo-se, conforme assinalado por Almeida e Lugati (2020, p.5), até a “*Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977.”

Essa geração de leis, pautada em autorizações conferidas pelo titular de dados para o tratamento de seus dados pessoais, tornou-se obsoleta, uma vez que, associado ao progresso tecnológico, o tratamento de dados pessoais perpassa à esfera de domínio governamental e passa a ser exercido também por entes privados (ALMEIDA; LUGATI, 2020)

Concebe-se, assim, a segunda geração de leis de proteção de dados subsequente, surgida ao final metade da década de 1970, pautada pela insatisfação dos cidadãos com o uso indevido de seus dados pessoais por terceiros e pela ausência de instrumentos para exercer a defesa de seus interesses em face do Estado e de entes privados. Nessa senda, a legislação instituiu um sistema apto ao fornecimento de instrumentos para a identificação, pelo titular, do uso indevido de suas informações pessoais e proposição de sua tutela (DONEDA, 2020).

A *Informatique et Libertés*, lei francesa de proteção de dados, promulgada em 1978, é o principal expoente desta geração (DONEDA, 2020).

Os avanços tecnológicos, todavia, condicionam a pós-modernidade à um constante ciclo de rompimentos e estabelecimentos de paradigmas, de forma que percebeu-se, no último quarto do século XX, que “o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social” (DONEDA, 2020, p. 167).

Desse modo, a terceira geração de leis de proteção de dados é demarcada pela compreensão por parte dos Poderes Legislativo e Judiciário e pelos próprios cidadãos, de que a proteção de dados é um procedimento complexo, o qual envolve, além da tutela de dados pessoais, a participação ativa dos indivíduos em seus contextos sociais e a efetividade conferida ao sistema de proteção de dados pessoais (DONEDA, 2020), centralizando no cidadão o sistema legal de proteção de dados a partir de sua atuação ativa enquanto titular de dados pessoais.

O protagonismo desta geração, todavia, é conferido a um julgado da Corte Constitucional Alemã (*Bundesverfassungsgericht*), referência no âmbito da proteção de dados ainda nos dias atuais, que consagrou a expressão autodeterminação informativa para “designar o direito dos indivíduos de “decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados” (DONEDA, 2020, p. 160, *apud* PANEBIANCO, 2000, p. 187.)

A despeito da centralização do sistema de proteção de dados no cidadão, as leis de terceira geração não estendem a tutela da proteção de dados pessoais à toda coletividade, de modo que, abrangendo apenas uma parcela de indivíduos, tornaram-se, insuficientes, demandando, desta maneira, o surgimento de novel geração de normas destinadas à proteção de dados pessoais, prevacente nos dias atuais, buscando-se priorizar todos os titulares de dados pessoais em face de terceiros aptos à manejar os dados aludidos (ALMEIDA; LUGATI, 2020)

A quarta geração de leis de proteção de dados, manifestada contemporaneamente na disciplina jurídica de mais de cento e quarenta países (DONEDA, 2021), rompe o paradigma do direito à autodeterminação informativa ao buscar suprir as desvantagens do enfoque individual preexistente.

Assume-se, dessa forma, que, a garantia legal de proteção dos dados pessoais a partir do reconhecimento do direito à autodeterminação informativa pautado e centralizado na capacidade de escolha individual do cidadão é ineficiente em face da amplitude e velocidade com que os dados são tratamento atualmente (DONEDA, 2020). Assim, diante do manifesto desequilíbrio na relação entre os cidadãos titulares de dados pessoais e as

entidades responsáveis pela coleta e processamento dos dados respectivos, é inócuo alicerçar a tutela dos dados pessoais unicamente no direito à autodeterminação informativa do cidadão (DONEDA, 2020).

Intenta-se nos regramentos contemporâneos de proteção de dados, ao reconhecer o desequilíbrio existente entre os polos em uma relação de tratamento de dados e a inexequibilidade de nortear o sistema legal de proteção de dados exclusivamente na decisão individual do titular dos dados pessoais quanto aos limites da utilização de seus dados, o fortalecimento do indivíduo frente aos entes que realizam o tratamento de dados a partir da institucionalização de instrumentos normativos que estabeleçam e destaquem o padrão coletivo de proteção (DONEDA, 2020).

Outro postulado das leis de quarta geração reside na paradoxal atenuação do papel da decisão individual na autodeterminação informativa, partindo-se, conforme assevera Doneda (2020, p. 169) do pressuposto de que “determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, à qual não pode ser conferida exclusivamente a uma decisão individual.”

O marco inicial desta quarta geração deu-se com a Diretiva 95/46/CE, de 1995, no âmbito da União Europeia, válida para todo o espaço jurídico europeu (DONEDA, 2021). Almeida e Lugati (2020), nesta perspectiva, exprimem que essa diretiva é paradigmática na medida em que estrutura o modelo europeu de proteção de dados.

Nesse aspecto, dentre as inovações preceituadas pela Diretiva 95/46/CE, tem-se a introdução de deveres aos *data controllers*, isto é, os agentes responsáveis pelo tratamento de dados pessoais, a adoção de princípios que permeiam todo o processo de tratamento de dados, desde a coleta até à eliminação dos dados, assim como a definição do conceito de consentimento enquanto conceito fundamental para a proteção de dados pessoais (ALMEIDA; LUGATI, 2020).

A Diretiva 95/46/CE destinava-se, contudo, aos Estados-Membros da União Europeia, não vinculando os próprios órgãos da União Europeia, a qual possui, segundo Quintiliano (2022b), natureza jurídica de confederação, ainda que detenha diversas características federativas.

Verifica-se, nesse aspecto, que:

Toda sociedade política estatal, dotada de órgãos com poderes que expressam a soberania concedida ou compartilhada, há a necessidade da consagração de direitos que limitem este poder face ao povo donde o mesmo poder emana. Tal limitação é feita pela previsão de direitos e garantias aos cidadãos frente aos

poderes estatais, instrumento conhecido como a declaração de direitos. (QUINTILIANO, 2022b, online).

O autor exprime que apenas no ano 2000, com a promulgação da Carta de Direitos Fundamentais, houve o reconhecimento de direitos fundamentais limitadores dos poderes da entidade na União Europeia (QUINTILIANO, 2022b), dentre os quais o direito à proteção de dados, consagrado no artigo 8º da Carta.

Não obstante, a princípio, o documento não gozava de normatividade, passando a ser vinculativo como direito primário da União Europeia em 2009, com a vigência do Tratado de Lisboa (QUINTILIANO, 2022b).

Dessa forma, foi apenas ao fim da primeira década do século XXI que os Estados-Membros e a própria União Europeia enquanto organização, passaram a assegurar a proteção de dados como direito fundamental.

A diretiva 95/46/CE “veio a ser substituída em 2016 pelo Regulamento Geral de Proteção de Dados (RGPD ou, no acrônimo anglófono pelo qual é mais conhecido, GDPR)”, norma considerada paradigma no âmbito da proteção de dados que exerceu influência direta na redação final da LGPD (DONEDA, 2021, p. 28).

A GDPR, entretanto, manteve os princípios da Diretiva revogada e conferiu enfoque ao consentimento enquanto manifestação de vontade do titular para legitimar o tratamento de seus dados pessoais na mesma medida em que consagrou o princípio da autodeterminação informativa e assegurou, também, a participação do titular no curso de todo o procedimento de tratamento de seus dados pessoais e a necessidade de que esteja evidenciada a finalidade a qual se destina o tratamento de dados no caso concreto (ALMEIDA; LUGATI, 2020).

Depreende-se, portanto, que os Estados Unidos da América e a Europa enveredaram por rotas distintas no que concerne ao desenvolvimento de sistemas legislativos de proteção de dados, o que evidencia as distinções sociais, culturais e jurídicas subsistente entre as localidades (DONEDA, 2021). Sinteticamente, enquanto no modelo estadunidense a proteção de dados encontra disciplina difusa e casuística, no modelo europeu subsiste a regulamentação ampla e detalhada da proteção de dados pessoais (GUEDES; TEPEDINO; TERRA, 2022).

Vislumbra-se, contudo, um fenômeno de convergência e integração entre diversos países com o propósito de estruturar uma cooperação internacional sobre a matéria diante dos desafios advindos do tratamento de dados que transpõe as fronteiras nacionais, pelo qual compõem-se ecossistemas cada vez mais complexos e que

demandam harmonia no diálogo entre fontes legislativas de cada país, notabilizando-se, nesse aspecto, a universalização do direito à proteção de dados e as consequências disto provenientes, uma vez que toda a temática da privacidade passou a se estruturar em função dos dados pessoais (DONEDA, 2020).

3.2 NO BRASIL

A tutela da proteção de dados no Brasil, segundo Quintiliano (2022b), quando comparada aos desdobramentos institucionais das experiências jurídicas dos Estados Unidos da América e da Europa no tema, desenvolveu-se tardiamente.

O autor expõe, nessa perspectiva, que, em toda história constitucional do Brasil, somente na CRFB/1988 houve menção à proteção de dados, ainda que não reconhecida como direito autônomo, mas implicitamente decorrente dos direitos à privacidade (artigo 5º, X) e à inviolabilidade do sigilo de dados (artigo 5º, XII) (QUINTILIANO, 2022b). No mesmo sentido, Almeida e Lugati (2020) aduzem que, além dos retromencionados direito à privacidade (artigo 5º, X) e à inviolabilidade de dados (artigo 5º, XII), a proteção de dados pessoais era tacitamente assegurada na CRFB/1988 a partir da à liberdade de expressão (art. 5º, IX), pelo direito à informação (art. 5º, XIV), o habeas data (art. 5º, LXXII) e a interceptação das comunicações telefônicas, telegráficas ou de dados (art. 5º, LXXII).

Ressalta-se, neste viés, que a constitucionalização do direito à proteção de dados, denotando sua propriedade de direito fundamental autônomo, ocorreu, conforme tratado no capítulo anterior, com a Emenda Constitucional nº 115, de 2022, trinta e quatro anos após a promulgação da CRFB/1988, pelo que passou a integrar o rol de direitos fundamentais inscrito no artigo 5º da CRFB/1988 (inciso LXXIX).

Outrossim, compassado fora o trâmite legislativo para regulamentação infraconstitucional da proteção de dados em território nacional, ocorrido apenas no ano de 2018 com a LGPD, trinta anos após promulgação da CRFB/1988.

Nessa senda, Doneda (2021) explicita que a introdução da expressão “proteção de dados pessoais” no vocabulário jurídico brasileiro é recente, ocorrida essencialmente devido aos debates ensejadores da formulação da LGPD. Assevera, ademais, que os fenômenos inerentes à proteção de dados pessoais não são estranhos à práxis jurídica brasileira, uma vez que preexistentes, mas manifestados sob vinculação a disciplinas jurídicas diversas, ocorrida, por exemplo, com o direito do consumidor, ou com as

questões atinentes à privacidade, direito do qual a proteção de dados foi, por muito tempo, considerada decorrente e dependente, motivação pela qual reduziu-se, no Brasil, ao longo da segunda metade do século XX, a demanda pela consideração da proteção de dados como direito autônomo (DONEDA, 2021).

Esses fatores elucidam as causas pelas quais não subsistiu a composição e desenvolvimento de sistemática jurídica de proteção de dados no Brasil em paralelo aos marcos regulatórios verificados em outras nações no mesmo período, ainda que patente a semelhante conjectura fática.

Isso porque, compara Doneda (2021), tal qual ocorrido com o caso “*National Data Center*” nos Estados Unidos da América, tratou-se, no Brasil, durante a década de 1970, sobre a criação de uma base de dados centralizada para cadastro único de cidadãos, no qual seriam processados seus dados pessoais a partir de um projeto denominado RENAPE (Registro Nacional de Pessoas Naturais), o qual previa a criação de órgão nacional para integração do Registro Civil de Pessoas Naturais e a Identificação Civil. O projeto, assim como o *National Data Center*, não fora bem sucedido, sendo arquivado em 1978, não tendo, contudo, o condão de instigar amplamente a discussão social e política sobre proteção de dados pessoais (DONEDA, 2021).

No âmbito legislativo, Doneda (2021, p. 30) destaca a pioneira proposição sobre proteção de dados pessoais, o Projeto de Lei 2.796 de 1980, de autoria da Deputada Cristina Tavares, que “assegura aos cidadãos acesso às suas informações constantes de bancos de dados e dá outras providências”. O projeto foi arquivado ao final da legislatura, sustentando-se, contudo, em consonância aos anseios de redemocratização no Brasil durante a década de 1980, a pretensão de maior concretude aos direitos relacionados a proteção de dados, o que culminou na inserção da ação de *habeas data* na Constituição de 1988 (DONEDA, 2021).

Na CRFB/1988, o autor leciona que:

o *habeas data*, ao cabo, assumiu a forma de uma ação constitucional, e não propriamente a de direito material, apesar de esse caráter poder ser dessumido de suas características. Assim, de forma algo oblíqua, essa opção legislativa acabou por suscitar a alguns intérpretes a oportunidade de ressaltar a efetiva existência de um direito material de acesso e retificação com relação aos dados pessoais, ainda que não expresso na literalidade da lei (DONEDA, 2021, p. 32)

O autor manifesta que, mesmo com a regulamentação pela Lei nº 9.507/1997, a ação constitucional de *Habeas Data*, por si só, era inócua ao enfrentamento dos desafios

de tratamento de dados pessoais impostos pelos fenômenos da globalização e informatização no contexto da sociedade da informação (DONEDA, 2021).

Nesse aspecto, assim como Quintiliano (2022b), Doneda (2021) expõe que não houve, com a promulgação da CRFB/1988, a identificação do direito a proteção de dados de pessoais enquanto direito autônomo, o que contrariou entendimento majoritário à época.

No que tange à legislação infraconstitucional após a promulgação da CRFB/1988, constatou-se um gradativo avanço na proteção de dados pessoais, mesmo que esta não fosse objeto central da regulamentação.

A Lei nº 8.078/1990, cognominada Código de Defesa do Consumidor, concentrou inúmeras demandas atinentes a proteção de dados pessoais em relações de consumo na medida em que estabeleceu “vetores e princípios de proteção ao consumidor adaptáveis a várias situações, bem como um sistema de tutela concreta com base no Sistema Nacional de Defesa do Consumidor” (DONEDA, 2021, p. 33). Ainda no âmbito consumerista, o artigo 43 CDC preceitua a proteção conferida ao titular de dados pessoais frente à bancos de dados e cadastro pela qual exigem-se “cadastros e dados claros, objetivos e verdadeiros, com linguagem facilmente compreendida” (ALMEIDA; LUGATI, 2020, p,10), demandando-se, ainda, que o consumidor “seja comunicado sobre a abertura de cadastros, ficha, registro e dados pessoais e de consumo” (ALMEIDA; LUGATI, 2020, p,10).

As autoras, citando Andrade e Moura (2010), ressaltam, todavia, que à época a norma de proteção ao consumidor tendia à regulamentação de banco de dados e não à efetiva tutela jurídica da proteção de dados com enfoque no consentimento do titular de dados pessoais, o que só fora efetivamente tratado na LGPD (ALMEIDA; LUGATI, 2020).

A Lei nº 12.414/2011, denominada Lei do Cadastro Positivo, fomentada por debates acerca do registro de dados sobre operações financeiras do consumidor, constituiu, segundo Doneda (2021), o primeiro regramento jurídico no Brasil idealizado a partir da sistemática comum à tradição de dados pessoais, já consolidada em outros países. Nesse âmbito, Almeida e Lugati (2020) complementam que há, na Lei do Cadastro Positivo, exigência de que o titular de dados expresse seu consentimento para que a atividade de tratamento de seus dados seja operacionalizada e concretizada, o que não era vislumbrado no CDC, o qual previa apenas mera notificação ao consumidor

Outras regulamentações antecedentes à LGPD que abordavam a tutela da proteção de dados, a exemplo da Lei de Acesso à Informação (Lei 12.527/2011) e do

Marco Civil da Internet (Lei 12.965/2014), passaram, conforme assinalado por Almeida e Lugati (202) sobre conceitos fundamentais à LGPD, tal qual o supramencionado “consentimento”. Inobstante, inseriram-se no mesmo contexto da Lei do Cadastro Positivo, integrando um limbo jurídico encerrado com a vigência da LGPD, instituidora da sistematização do tratamento de dados pessoais no Brasil, da qual constitui-se como elemento central (DONEDA, 2021).

No que se refere a elaboração e tramitação da LGPD, o autor indica que sua gênese encontra-se em discussões e negociações do Mercado Comum do Sul (MERCOSUL) visando o estabelecimento de regulamentação unificada sobre tratamento de dados pessoais para os países integrantes do bloco. (DONEDA, 2021).

A despeito da ausência de deliberação para que a proposta fosse convertida em norma do Mercosul, percebe-se que as tratativas do Mercosul semearam em solo brasileiro o interesse pela regulamentação da proteção de dados pessoais:

Assim, o texto que serviu de base para um debate público e que é o primeiro antecedente direto do que hoje é a Lei Geral de Proteção de Dados, foi tornado público pelo Ministério da Justiça em 30 de novembro de 2010. O referido debate público foi promovido pelo Ministério da Justiça e realizado inteiramente pela Internet, contando com a colaboração da Fundação Getúlio Vargas – Direito Rio e do Observatório da Internet, do Comitê Gestor da Internet do Brasil. (DONEDA, 2021, p. 35)

Encerradas as discussões no debate público, o Ministério da Justiça estruturou e revisou, entre 2011 e 2015, o Anteprojeto da Lei de Proteção de Dados, submetido a novo debate público em 2015, sendo, então, consolidado pelo Ministério da Justiça, que o enviou à Casa Civil da Presidência da República, responsável pelo encaminhamento do anteprojeto ao Congresso Nacional, em 13 de maio de 2016, tendo sido protocolado na Câmara dos Deputados como PL 5.275/2016 (DONEDA, 2021).

No período em que o texto fora enviado ao Congresso Nacional, a discussão acerca proteção de dados pessoais já havia sido disseminada pelo País, de maneira que subsistiam outros projetos de lei sobre o tema em tramitação (DONEDA, 2021). Nessa senda, destaca-se o Projeto de Lei 4.060/2012, de autoria do deputado Milton Monti (PR/SP), ensejador, em 2016, da criação de Comissão Especial para sua discussão, envolvendo audiências públicas e participação de diversos setores da sociedade, sendo “aprovado, em 29 de maio de 2018, pelo Plenário da Câmara dos Deputados, por unanimidade, o parecer da referida Comissão Especial e a matéria seguiu para o Senado Federal, identificada como o PLC 53/2018.” (DONEDA, 2021, p. 36).

No Senado Federal, autor aponta que:

o PL aprovado pela Câmara (PLC 53/2018) passou a tramitar em conjunto com o PLS 181/2014, PLS 131/2014 e PLS 330/2013, tendo sido a estes apensado e enviado à Comissão de Assuntos Econômicos (CAE), sob relatoria do senador Ricardo Ferraço (PSDB/ES) que, 14 de junho de 2018, apresentou relatório a favor do PLC 53/2018 com emendas e pela prejudicialidade dos demais, que foi aprovado pela Comissão em 3 de julho de 2018. (DONEDA, 2021, p.36).

O projeto foi aprovado por unanimidade pelo plenário do Senado Federal, após aprovação de requerimento de urgência, em 5 de junho de 2018, pelo que seguiu para sanção presidencial para ser promulgada, com vetos, em 14 de agosto de 2018:

Posteriormente, foi editada a Medida Provisória 869/2018, que veio a se tornar a Lei 13.853/2019 que, além de modificar a LGPD em diversos pontos, finalmente definiu as características da ANPD e do seu Conselho, de acordo com os arts. 55-A a 55-L da LGPD. Outra das modificações foi a extensão de sua *vacatio legis*, que passou de fevereiro de 2020 para agosto de 2020, com exceção dos referidos artigos sobre a ANPD e Conselho Nacional de Proteção de Dados e da Privacidade, cuja vigência é imediata.

Mais recentemente, a Lei 14.010, de 10 de junho de 2020, especificou que os arts. 52, 53 e 54 da LGPD (referentes às sanções administrativas) entrarão em vigor em 1.º de agosto de 2021 (...) (DONEDA, 2021, p. 36).

Quintiliano (2022b, online) conclui, assim, que a LGPD foi resultado das confluências advindas do “Projeto de Lei 4.060/2012, de iniciativa parlamentar, com o Projeto de Lei 5.276/2016, apresentado pela Presidência da República, que gozou de relativa proeminência no texto final aprovado.”

4. A LEI Nº 13.709/2018: LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

O desenvolvimento das sociedades ao longo do curso da história está intrinsecamente relacionado a um elemento central estruturador, variável em cada período histórico, que constitui e fomenta os modos de produção, as relações interpessoais e a organização social.

Nesse sentido, Bioni (2021) destaca que na contemporaneidade, devido a evolução tecnológica hodierna, o elemento que impulsiona a organização da sociedade é a informação, constituindo-se como componente essencial ao desenvolvimento da economia, assim como instrumento regente dos relacionamentos sociais, envoltos no fluxo informacional gerado pelos mecanismos de processamento e transmissão de informações em larga escala e velocidade.

A partir do estabelecimento de um novo paradigma no que concerne a estruturação das relações sociais, no qual a informação assume papel de protagonismo, são apresentados inéditos desafios à ciência jurídica, a qual, por essência, deve adequar-se ao contexto vigente, formulando soluções às problemáticas jurídicas surgidas no meio social.

Dentre os desafios advindos da nova organização social na era digital, destaca-se a proteção de dados pessoais, que, no Brasil, recebeu tratamento constitucional, estando expressamente prevista no rol de direitos e garantias fundamentais do artigo 5º da CRFB/1988, insculpida no inciso LXXXIX, o qual assegura, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais, a todos.

A lei referida pelo dispositivo constitucional é a de nº 13.709/2018, nominalmente tratada por “Lei Geral de Proteção de Dados (LGPD)”, a qual, visando a proteção de direitos fundamentais, dispõe sobre o tratamento de dados pessoais, inclusive no meio digital, constituindo-se como marco regulatório da temática de proteção de dados no Brasil, disciplinando, dentre outros elementos, a responsabilidade dos agentes de tratamento de dados no caso de violação às disposições da LGPD, sem, contudo, definir o regime jurídico específico, o que constitui objeto de análise do presente trabalho.

4.1 OBJETIVOS, FUNDAMENTOS E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

A Lei nº 13.709/2018, cognominada na ementa do próprio diploma normativo como “Lei Geral de Proteção de Dados” (LGPD), segundo Maimone (2022), tem por escopo a regulamentação do tratamento de dados pessoais no intuito de protegê-los, o que é factível mediante garantia do respeito aos direitos fundamentais expressamente mencionados no artigo 1º do diploma normativo, quais sejam os direitos: i) à privacidade, ii) à liberdade, iii) ao livre desenvolvimento da personalidade; iv) assim como ao direito fundamental à proteção de dados pessoais, inclusive no meio digital, cuja previsão não está manifesta no artigo referido, uma vez que, a época da promulgação da Lei, não figurava no rol de direitos e garantias fundamentais do artigo 5º da CRFB/1988.

Demonstrado o escopo da norma, Cots e Oliveira (2019) aduzem que é relevante destacar a nitidez na distinção entre objetivos, fundamentos e princípios jurídicos em um instrumento normativo, o que é delineado na própria LGPD, uma vez esta lei tratou de cada conceito de forma harmoniosa, assegurando coesão e adequação à sua aplicação.

Dessa forma, além do objetivo previsto no artigo 1º, os fundamentos da LGPD são definidos de forma direta em 7 (sete) incisos de seu artigo 2º:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

De igual maneira, os princípios que regem as atividades de proteção de dados são enunciados no artigo 6º do Instrumento Normativo, prevendo, além do princípio da boa-fé, o qual está inserido no *caput* do artigo retromencionado, 10 (dez) princípios correlacionados, os quais devem ser, imprescindivelmente, seguidos pelos agente de tratamento de dados: (i) finalidade; (ii) adequação; (iii) necessidade; (iv) livre acesso; (v)

qualidade dos dados; (vi) transparência; (vii) segurança; (viii) prevenção; (ix) não discriminação; e (x) responsabilização e prestação de contas.

4.2 DADOS NA LGDP

Denota-se, em se tratando da proteção de dados pessoais em meio à Sociedade da Informação, a distinção entre dois termos usualmente tidos por sinônimos, inclusive na redação de dispositivos legais, tal qual ocorre na Lei de Acesso a Informação (Lei nº 12.527/2011) e na própria Lei Geral de Proteção de Dados, cujas acepções são circunstancialmente sobrepostas: informação e dados.

Doneda (2020) destaca, nesse sentido, que ambos tencionam retratar um fato, captando determinado aspecto de uma dada realidade, subsistindo, no entanto, peculiaridades no emprego de cada um dos termos.

O “dado” apresenta “conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida” (DONEDA, 2020, p. 139), uma espécie de pré-informação, pretérita ao procedimento de recebimento, interpretação e refino do conteúdo fático.

A “informação”, por sua vez, segundo o autor:

alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza. (DONEDA, 2020, p.139)

Não obstante, denota que, em geral, a doutrina e a própria legislação não delineiam distinções entre os termos em disceptação (DONEDA, 2020).

Nesse aspecto, a LGPD, ao abordar conceitos fundamentais aos seus fins, explicita a definição de “dados pessoais”, sem distingui-la do sentido do termo “informação”, constando do dispositivo legal: “Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;”.

A legislação brasileira, nessa senda, não trata de qualquer tipo de dado, mas unicamente de “dados pessoais”, os quais devem ser vinculados, necessariamente, a pessoa natural identificada ou identificável.

A LGPD, adota, portanto, no que refere aos dados pessoais, consoante depreendido do inciso I do artigo 5º da LGPD, um conceito expansionista, pelo qual estarão amparados pela lei a informação concernente à pessoa diretamente identificada,

assim como a informação que tem o potencial de tornar a pessoa identificável (VAINZOF, 2020).

A distinção entre dados gerais, fora da esfera de abrangência da LGPD, e dados pessoais, objeto por excelência da LGPD, consoante Doneda (2020), reside no fato de que estes dispõem de um vínculo objetivo com o indivíduo, transparecendo aspectos que lhe dizem respeito, de forma que é uma característica fundamental do dado pessoal o componente da identidade de uma pessoa natural (VAINZOF, 2020).

A identidade, nesse aspecto, transcende à especulação filosófica ensejadora da formulação de pressupostos teóricos complexos, consubstanciando-se, além dos traços de personalidade que distinguem um indivíduo de seu ser semelhante, conferindo-lhe autorreconhecimento, na reunião de diversos comportamentos, padrões, fatos e atributos utilizados como forma de comunicação automática (DONEDA, 2020).

Os dados pessoais, em meio ao contexto contemporâneo, encontram-se, assim, inseridos em diversas nuances do cotidiano, desde tarefas simples, como acesso a contas de *email*, registro de acesso a conexões de internet, no aparecimento automático de uma barra de notificações acerca da utilização de *cookies* em domínios na internet; até documentos imprescindíveis a vida em sociedade, tal qual o Registro Geral – RG e o Cadastro de Pessoa Física – CPF.

A disciplina jurídica da LGPD não abarca, portanto, dados ou informações corporativas em sua essência, sejam essas sigilosas, sejam confidenciais, sejam públicas, sejam privadas, a exemplo do que ocorre, conforme exemplifica Vainzof (2020) com balanços financeiros, planejamentos estratégicos, fórmulas, protótipos, sistemas em desenvolvimento ou qualquer tipo de documento corporativo, os quais só serão objeto de proteção da LGPD caso contenham dados pessoais.

De igual maneira, os dados anonimizados (LGPD, artigo 5º, inciso III), isto é, dados cujo titular não possa ser identificado, e os dados que sofreram anonimização (LGPD, artigo 5º, inciso XI), qual seja, a perda, por meios técnicos, da capacidade de associação, direta ou indireta, de um dado a um indivíduo, não são considerados, em regra, dados pessoais pela LGPD, conforme preceituado no artigo 12 do diploma normativo, mantendo-se ausentes, portanto, da esfera de abrangência das regras relativas à proteção de dados pessoais.

Doneda (2020) destaca ainda, em se tratando do desenvolvimento conceitual de dados pessoais, a possibilidade de agrupamento de informações pessoais em subcategorias, relacionadas a determinados aspectos da vida de uma pessoa.

A setorização dos dados pessoais, segundo o autor, acarreta variadas consequências, mencionando exemplificativamente a conveniência da individualização da abordagem atribuída à cada subcategoria de dados pessoais consoante suas especificidades.

A legislação de proteção de dados pátria adota a subcategorização ao discorrer sobre de dados pessoais, na medida em que a abordagem de dados pessoais efetivada LGPD comporta o estabelecimento de uma categoria específica cuja tutela é diferenciada: os dados sensíveis, conceito positivado no inciso II do artigo 5º do dispositivo normativo:

Art. 5º Para os fins desta Lei, considera-se:

(...)

II - 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;

Os dados pessoais acima elencados são definidos como sensíveis, tendo em vista que, caso sejam conhecidos e submetidos a tratamento, as informações deles provenientes são potencialmente de maior risco do que outros tipos de informações, dada a possibilidade de sua utilização de forma discriminatória ou lesiva (DONEDA, 2020). Complementa Vainzof (2020, p. 85) que os dados pessoais sensíveis “poderão implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais dos titulares.”

A observação pragmática acerca da dissimilitude entre os efeitos provenientes do tratamento de dados pessoais gerais e de dados pessoais sensíveis consubstanciou-se como motivação para a criação desta categoria específica e o seu consequente apartamento dos dados pessoais gerais (DONEDA, 2020). A triagem, em si, dos dados pessoais considerados sensíveis (origem racial ou étnica, convicção religiosa, opinião política, relativos à saúde, genético ou biométrico, para citar alguns exemplos) decorre da verificação de que, em determinada configuração social, a “circulação de determinadas espécies de informação apresentariam um elevado potencial lesivo aos seus titulares” (VAINZOF, 2020, p. 85).

Assim, considerando o potencial mais danoso do manuseio de dados pessoais sensíveis, a LGPD imputou a esses tutela jurídica particularizada, erigindo estrutura legal protecionista de maior envergadura ao delimitar as imposições normativas para o

tratamento respectivo dos dados pessoais sensíveis, afigurando uma base legal diferenciada e limitada (VAINZOF, 2020).

A distinção no tratamento de dados pessoais sensíveis está expressa no *caput* e inciso I do artigo 11 da norma de proteção de dados, segundo os quais somente ocorrerá o tratamento de dados pessoais sensíveis na hipótese de consentimento (livre, inequívoco e informado, conforme inciso XII do artigo 5º da LGPD), de forma específica e destacada, do titular ou de seu representante para finalidade específica, ou, conforme inciso II do artigo 11 da LGPD, poderá ocorrer o tratamento de dados pessoais sem consentimento do titular nas hipóteses das alíneas que o sucedem.

Inexiste, comparativamente, via de regra, a necessidade de consentimento do titular para tratamento de dados pessoais cujo acesso é público ou que tenham se tornado manifestamente públicos pelo titular, conforme disciplina dos §§3º e 4º do artigo 7º da LGPD. Outrossim, à integralidade dos dados pessoais não classificados como sensíveis, subsiste também a perspectiva de tratamento posterior para finalidades diversas da originariamente pretendidas, desde que verificados os propósitos legítimos e específicos para o inédito tratamento, assim como observados os direitos do titular, os princípios e fundamentos da LGPD.

A setorização e conseqüente tutela jurídica diferenciada dos dados pessoais sensíveis na LGPD atendem, conforme explicita Doneda (2020), à demanda advinda de um tipo de dado mais suscetível de utilização discriminatória após o seu tratamento, o que implica na hipervulnerabilização do titular. Não obstante, reforça o autor que o emprego lesivo de informações decorrentes de dados pessoais sensíveis é potencialmente maior, mas não a única fonte da qual podem jorrar situações discriminatórias, uma vez que podem advir a partir do manuseio de dados pessoais gerais, ou, ainda resultar configurado o uso de dados pessoais sensíveis com finalidade legítima e lícita, consonante aos ditames legais. (DONEDA, 2020).

Vainzof (2020), nessa perspectiva, exemplifica que a coleta de hábitos de consumo, por si, não implica no tratamento de dados pessoais sensíveis. Sobrevindo, contudo, no exemplo do autor, inferência acerca de qualquer dado pessoal reputado sensível, nos termos da legislação, no curso do processo de coleta de hábitos de consumo, ainda que a inferência mostre-se equivocada, incidirão as regras relativas ao tratamento de dados pessoais sensíveis, situações que devem ser analisadas com prudência e precisão pelo controladores, considerando a preponderância do tratamento

de dados pessoais em larga escala e de forma automatizada, evitando que as ocorrências nos moldes do exposto adiante sejam reiteradas:

(...) em 2012, por meio do hábito de consumo de uma cliente, cruzando padrões de comportamento de compra, como cremes e loções sem perfume, suplementos de cálcio, magnésio e zinco, uma loja de departamentos norte-americana chegou à conclusão de que ela estaria grávida, até mesmo antes que seu pai.

(...)
Inclusive, uma pesquisa da Universidade de Cambridge demonstrou que “curtidas” em redes sociais podem gerar um retrato fidedigno dos gostos e preferências dos seus usuários por meio do qual poderiam ser extraídas inferências, com exatidão, da porcentagem dos homossexuais e heterossexuais, brancos e negros e eventuais ligações partidárias, republicana ou democrata. (VAINZOF, 2020, p. 86-87)

Nesse ínterim, ao concluir sua exposição acerca de dados sensíveis, Vainzof (2020) reputa que a elaboração da própria LGPD fora impulsionada pelo escândalo concernente à utilização indevida de dados pessoais que teve repercussão mundial envolvendo a empresa de análise de dados políticos *Cambridge Analytica*.

No caso, a imputação à empresa incidia, em suma, sobre a cooptação, direta e indireta, de informações relativas a aproximadamente cinquenta milhões de usuários da rede social “*Facebook*” a partir de um aplicativo que realizava testes de personalidade no qual os usuários assentiam na coleta de seus dados para fins acadêmicos (BBC, 2018). O veículo de imprensa britânico assevera que a *Cambridge Analytica*, aproveitando-se de hiatos na política institucional da plataforma do *Facebook* sobre coleta de dados de terceiros, obteve não apenas acesso aos dados de quem que realizava o teste de personalidade, mas também, sem nenhuma autorização, aos dados daqueles que estavam vinculados como “amigos” da pessoa que havia efetivado o teste de personalidade, identificando, a partir disso, as personalidades dos eleitores para envio de conteúdos aptos a influenciar seus comportamentos (BBC, 2018).

4.3 TRATAMENTO DE DADOS

Consta do inciso X do artigo 5º da LGDP:

Art. 5º Para os fins desta Lei, considera-se:

(...)

X - tratamento: 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)

Vislumbra-se que a legislação de proteção de dados pessoais pátria objetivou destrinchar conceitos que lhes são correlatos nos incisos do artigo 5º, especificando, dentre eles, a definição do termo “tratamento” (de dados pessoais).

Depreende-se que a LGPD adotou uma acepção abrangente no que tange ao tratamento de dados pessoais, dada a consideração de que concebe-se como tratamento toda operação realizada com dados pessoais, englobando a integralidade das hipóteses de manuseio de dados, desde a coleta até sua eliminação, sem ter em conta o meio despendido para a consecução da atividade (VAINZOF, 2020).

Nesse aspecto, Soler (2021) enfatiza a relevância da compreensão de que, a despeito da constante imersão no âmbito digital em meio a sociedade da informação, o tratamento de dados pessoais ocorre tanto no ambiente físico, quanto no ambiente online. Assim, a LGPD e as respectivas normas concernentes ao tratamento de dados pessoais também abrangem situações cotidianas que destoam do imaginário relativo à atividade de tratamento de dados, a exemplo da circulação de papeis, preenchimentos de formulários, troca de cartões pessoalmente e permissões de uso (SOLER, 2021).

A percepção da amplitude conceitual do termo “tratamento” adotado na LGPD torna-se imprescindível ao agente de tratamento de dados pela necessidade de manutenção dos registros de suas operações (VAINZOF, 2020).

Ao controlador, em específico, faz-se mister a avaliação de adequação de sua atividade à uma das bases legais que ensejam e justificam a realização de tratamento de dados previstas no rol do artigo 7º da LGPD:

o que implica dizer que um simples dado pessoal arquivado, mesmo que não seja processado, precisará ter um fundamento previsto na Lei para estar sob a responsabilidade do agente. Se o controlador não encontrar um embasamento jurídico para manter o dado pessoal consigo (ou com o operador), deverá eliminá-lo. (VAINZOF, 2020, p. 108)

Explicita, ainda, Soler (2021) que, considerando o constante desenvolvimento tecnológico originador de novas formas de atividades relativas ao tratamento de dados pessoais, a redação conferida ao inciso X do artigo 5º da LGPD caracterizou interessante escolha do legislador, optando este por um conceito abrangente em detrimento à idealização e posituação de cada atividade passível de inserção na concepção de tratamento de dados pessoais.

4.4 TITULAR DE DADOS

A LGPD, conforme Lima e Ramiro (2020), ao estabelecer normas específicas, compreendendo, assim, princípios e regras, decorrentes do sistema de proteção de dados pessoais, constitui-se como microssistema legislativo. Neste sentido, verifica-se que a LGPD é inserida como elemento legislativo de integração do sistema protetivo de dados pessoais, coordenando-o na medida em que centraliza a temática e, sem prejuízo do diálogo com outras fontes legais associadas à proteção de dados pessoais, como o Código de Defesa do Consumidor (Lei nº 8.078/90) e a Lei de Acesso à Informação (Lei nº 12.527/2011), estabelece obrigações e assegura direitos (LIMA; RAMIRO, 2020).

Nessa perspectiva, Vainzof (2020) aduz que o titular dos dados pessoais é o núcleo central da existência da LGPD, uma vez que eventuais violações aos dispositivos normativos da LGPD concernentes à proteção de dados pessoais atingem diretamente a esfera de direitos da pessoa natural a eles vinculados, isto é, ao titular de dados pessoais.

Assim, define-se como titular dos dados pessoais, consoante disposto no inciso V, do artigo 5º, da LGPD, a pessoa natural cujos dados pessoais são objeto de tratamento.

No que tange à formação de personalidade da pessoa natural, o Código Civil de 2002 (CC/2002) preceitua em seu artigo 2º que esta tem início com o nascimento com vida. Nesse aspecto, “assim que qualquer pessoa nasce e respira (nasce com vida), automaticamente já conta com os direitos tutelados pela LGPD.” (VAINZOF, 2020, p.95).

Não obstante, ainda no artigo 2º do CC/2002, há expressa previsão de que os direitos do nascituro serão resguardados desde o momento da concepção. Vainzof (2020) expõe que julgamentos paradigmas do STJ e do STF denotam que há de se reconhecer os direitos de personalidade do nascituro, dos quais o mais destacado é o direito à vida, inexistindo indissociável vinculação entre o nascimento com vida e o conceito de pessoa, de personalidade jurídica e de titularização de direitos.

Consequentemente, segundo Vainzof (2020, p. 95):

Quando da identificação, no ultrassom do nascituro, da sua imagem, peso, tamanho, batimento cardíaco, tipo sanguíneo, potenciais doenças, sexo, nome da mãe, entre inúmeros outros dados pessoais do próprio feto (não são dados pessoais somente da mãe, direitos ou indiretos), acenamos que esse nascituro teria, no mínimo, expectativa de direito sobre seus dados pessoais, em razão da sua personalidade jurídica formal, desde a sua concepção, e da sua personalidade jurídica material, relacionada aos direitos patrimoniais, que se adquire com o nascimento com vida

Conclui-se, assim, que:

No Brasil, a tutela dos direitos existentes na LGPD se inicia com o feto, no mínimo diante da expectativa de direito sobre seus dados pessoais, em razão da sua personalidade jurídica formal, desde a sua concepção, e da sua personalidade jurídica material, relacionada aos direitos patrimoniais, adquirida com o nascimento com vida, e terminaria com o falecimento. (VAINZOF, 2020, p.96)

Dessa maneira, no que se refere à efetiva tutela dos direitos do titular de dados pessoais, a LGPD dedica o Capítulo III em sua integralidade ao tópico, elencando-os entre os artigos 17 e 22 da norma, sem, contudo, olvidar que os direitos do titular de dados não são taxativamente listados no rol de artigos retromencionado (LIMA; RAMIRO, 2020).

As autoras, inobstante, transcrevem os direitos inerentes aos titulares de dados pessoais constantes no Capítulo III da LGPD:

i) o direito de obter a confirmação da existência de tratamento; ii) direito de acesso aos dados; iii) direito de correção dos dados incompletos, inexatos ou desatualizados; iv) direito à anonimização dos dados pessoais; v) direito ao bloqueio ou eliminação dos dados desnecessários, excessivos ou decorrentes de tratamento ilícito; vi) direito à portabilidade dos dados pessoais; vii) direito à informação sobre o compartilhamento de seus dados pessoais pelo controlador; viii) informações sobre não fornecimento do consentimento e quais as consequências da negativa; ix) direito à revogação do consentimento; x) direito à revisão das decisões tomadas com base em tratamento automatizado de dados pessoais, dentre outros. (LIMA; RAMIRO; 2020, p. 249)

A fonte da qual decorrem todos estes direitos é a autodeterminação informacional, disciplinada na LGPD como um dentre os fundamentos da proteção de dados pessoais (artigo 2º, II), conceituado como o “direito de controlar as informações que lhe digam respeito.” (LIMA; RAMIRO; 2020, p. 250).

A autodeterminação informacional supera, contudo, a mera possibilidade de controle das informações relativas ao titular de dados pessoais, abrangendo, de acordo como Lima e Ramiro (2020, apud RODOTÁ, 1991, p.525) o direito de procurar, receber e difundir informações.

Assim, considerando-se o direito à proteção de dados pessoais, inclusive nos meios digitais, como direito fundamental constitucionalmente assegurado (CRFB/1988, artigo 5º, LXXIX) e instrumentalizado por norma específica, cognominada LGPD; e compondo-se o titular de dados pessoais como o núcleo de existência da referida norma (CAIO LIMA, 2020), compreende-se que a sistemática legal de proteção de dados pessoais no Brasil perpassa o ideário de assegurar formalmente o controle, pelo titular de dados pessoais, de suas informações, constituindo mecanismos operacionalizadores da

concreta tutela das informações pelo titular de direitos pessoais respectivos, viabilizando o pleno gozo do exercício dos direitos que lhes são conferidos pela legislação (LIMA;RAMIRO, 2020).

4.5 AGENTES DE TRATAMENTO: CONTROLADOR E OPERADOR

A expressão “agentes de tratamento” revela conceito aglutinador, disciplinado no inciso IX do artigo 5º da LGPD, criado para indicar na referida legislação o conjunto de responsabilidades e obrigações as quais estão sujeitos o “controlador” e o “operador”, pessoas naturais ou jurídicas, de direito público ou privado, responsáveis pelo exercício de atividades relacionadas ao tratamento de dados.

Determinam-se os agentes de tratamento a partir de seu caráter institucional, de forma que funcionários, servidores públicos e equipes de trabalho de uma organização, enquanto conservarem a subordinação que lhes é característica por atuarem sob o poder diretivo do agente de tratamento, não são considerados controladores ou operadores, o que, por consequência, também obsta a qualificação como agente de tratamento de dados (ANPD, 2021).

A definição conceitual das espécies pertencentes ao gênero “agentes de tratamento” é dada pela própria LGPD, a qual assenta que o controlador é, consoante previsão do inciso VI do artigo 5º, da LGPD, a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018).

Infere-se do conceito legal cunhado para definir o controlador que, a despeito deste conservar capacidade para o realizar o tratamento de dados, seu traço distintivo consubstancia-se no poder de decisão que lhe é conferido. Nesse aspecto, o controlador deve possuir influência e autoridade sobre as mais relevantes decisões do tratamento de dados, concernentes aos “elementos essenciais para o cumprimento da finalidade de tratamento” (ANPD, 2021, p. 10), sendo desnecessário que todas as decisões sejam tomadas pelo controlador, o qual detém a faculdade de, mediante fornecimento de instruções, conferir a um terceiro, o operador, a realização de um tratamento de dados em seu nome (LGPD, art. 5º, VIII; art. 39).

Nesse contexto, conforme assevera Vainzof (2020), a LGPD impõe sobre o controlador maiores encargos jurídicos, pois é responsável pela tomada das principais decisões relativas ao tratamento de dados pessoais, desde o projeto, passando pelas

etapas de coleta e processamento, até o descarte dos dados, o que abarca, conforme exposto por Cíntia Lima (2020), a determinação das motivações e finalidades de uma operação de tratamento de dados compete ao controlador, além de considerações sobre o tempo de duração e a natureza dos dados objeto de tratamento (ANPD, 2021).

Ademais, a delimitação legal e conceitual do agente de tratamento denominado controlador mostra-se elementar em função da repercussão prática do termo, dada a atribuição de obrigações específicas ao controlador. Assim, dentre as obrigações que competem ao controlador, Cíntia Lima (2020, p.290) elenca como substanciais:

- a) elaborar relatório de impacto de proteção de dados pessoais quando determinado pela ANPD (art. 38 LGPD); b) manter registro das operações de tratamento de dados (art. 37 LGPD); c) dever de notificação sobre qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados pessoais (art. 48 LGPD); d) adotar medidas de segurança, técnicas e administrativas para a proteção de dados pessoais (art. 46 LGPD); e) formular regras de boas práticas e de governança (art. 50 LGPD); f) dever de informar (transparência) e de respeitar os demais direitos dos titulares estabelecidos no art. 17 e seguintes da LGPD; e g) dever de sigilo.

Nesse aspecto, a identificação e individualização do agente definido legalmente como controlador, segundo Cíntia Lima (2020, *apud* SALOM, 2013, p.69), é essencial à determinação do responsável pelos danos causados ao titular de dados pessoais ou a terceiros em decorrência de tratamento de dados pessoais.

O controlador, preponderantemente, será uma pessoa jurídica, de direito público interno ou de direito privado, nos termos delimitados pelos artigos 41 e 44 do CC/2002. Tal hipótese será manifestada quando a entidades públicas ou sociedades empresariais couber a definição sobre tomada de decisões, incluindo a motivação e a finalidade, de uma operação de tratamento de dados pessoais, compreendendo coleta, processamento, armazenamento e compartilhamento ou eliminação das informações que integram o banco de dados gerido no âmbito da organização. Disso decorre o entendimento que profissionais (pessoas naturais) subordinados a uma pessoa jurídica ou como membro de seus órgãos não serão controladores. (ANPD, 2021).

Reforça-se, contudo, que pessoais naturais poderão ser controladoras nas hipóteses em que for responsável pelas decisões concernentes ao tratamento de dados pessoais, agindo de forma independente, isto é, em nome e interesse próprio, não havendo que se falar em subordinação, pois encontram-se desvinculadas de pessoa jurídica (ANPD, 2021). A Autoridade Nacional de Proteção de Dados (ANPD) exemplifica que isso ocorre “com os empresários individuais, os profissionais liberais (como

advogados, contadores e médicos) e os responsáveis pelas serventias extrajudiciais” (ANPD, 2021, p. 10).

O operador, por seu turno, é definido, nos termos do inciso VII do artigo 5º da LGPD, como a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (BRASIL, 2018). Na mesma perspectiva, o artigo 39 da LGPD prevê que o operador “deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria” (BRASIL, 2018).

O operador é o encarregado direto pelo tratamento de dados, estando sua ação condicionada, no entanto, às determinações do controlador ou à previsão legal, conforme Vainzopf (2020). Assim, a principal distinção entre o operador e o controlador reside no poder de decisão conferido a esse enquanto aquele tem sua atuação adstrita aos limites das finalidades preestabelecidas pelo controlador (ANPD, 2021). Ao operador, em sua margem de ação, cabe a definição sobre elementos não essenciais ao tratamento de dados, como medidas técnicas (ANPD, 2021).

A regulamentação de proteção de dados pátria também confere uma série de obrigações ao operador, ainda que consideradas exíguas em face das incumbências do controlador, destacando-se, consoante a ANPD (2021, p. 16), as necessidades de “(i) seguir as instruções do controlador; (ii) firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com suboperador.”

Ademais, a despeito de a LGPD não positivar a indispensabilidade de avença contratual sobre o tratamento de dados entre os agentes de tratamento (controlador e operador) responsáveis pela operação, entende-se a pactuação de contrato como uma boa prática de tratamento de dados (ANPD, 2021). Isso porque definições e cláusulas contratuais delineiam de modo mais satisfatório a imposição de limites à atuação do operador, a fixação de parâmetros objetivos para a alocação de responsabilidades entre as partes e a redução de riscos e incertezas decorrentes da operação (ANPD, 2021).

São matérias passíveis de estipulação contratual: “o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos e obrigações e responsabilidades relacionados ao cumprimento da LGPD” (ANPD, 2021, p.16).

Nesse aspecto, o operador poderá ser responsabilizado por sua conduta na hipótese em que exceder, no tratamento de dados, os limites impostos pelas instruções do controlador (ANPD, 2021).

Assim como ocorrido com o controlador, o operador usualmente será uma pessoa jurídica, não subsistindo, entretanto, óbices à caracterização de uma pessoa natural como operadora, desde que contratada para prestar serviços de tratamento de dados com finalidade específica (ANPD, 2021).

Reitera-se que “o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.” (ANPD, 2021, p. 17). Dessa forma, assim como não é possível considerar profissionais subordinados a uma pessoa jurídica como controladores, denota-se que “empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores” (ANPD, 2021, p.17).

Exemplificativamente:

Uma empresa decide enviar propagandas aos seus clientes com a finalidade de alavancar as vendas de determinado produto. Para isso, contrata agência de publicidade, que elaborará a campanha de marketing com fotos de pessoas utilizando o produto. A empresa informa todos os critérios para a campanha, tais como o público-alvo e estabelece os critérios de como deve ser a aparência física dos modelos fotográficos. A agência de publicidade trata dados pessoais para prestar o serviço para a empresa, ao selecionar modelos fotográficos e armazenar as fotos desses titulares. Após a conclusão do serviço pela agência, o funcionário da empresa envia as propagandas aos clientes.

Neste exemplo a empresa atua como controlador, ao determinar o tratamento de dados e definir os seus elementos essenciais. A agência de publicidade atua como operadora ao tratar dados conforme a finalidade do tratamento definida pelo controlador. E o funcionário, ao enviar os e-mails para os clientes, atua sob o poder diretivo da empresa e não se caracteriza como agente de tratamento. (ANPD, 2021, p. 6)

Complementando-se o exemplo, indica-se que os funcionários (pessoas naturais) da agência de publicidade (pessoa jurídica) atuam sob seu poder diretivo, sendo, portanto, subordinados ao empregador – agência de publicidade, de forma que não são caracterizados como operadores, distanciando-se, assim, do conceito de agente de tratamento de dados.

No âmbito das cadeias mais complexas de tratamento de dados pessoais, desponta, ainda, a figura do “suboperador”, definido como “aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador” (ANPD, 2021, p. 19).

O termo em análise inexistente na LGPD, a qual definiu, formalmente, como agentes de tratamento de dados (artigo 5º, IX) o controlador (artigo 5º, VI) e o operador (artigo 5º, VII). Inobstante, a ausência de disciplina jurídica específica na LGPD sobre o suboperador não o torna ilegal ou impossibilita sua existência e a consequente distribuição de funções, responsabilidades e competências para consecução de seus objetivos na realização de tratamento de dados pessoais, “principalmente porque pode desempenhar a função de operador em subordinação a outro operador” (ANPD, 2021, p.19).

Nessa perspectiva, o suboperador só possui relação direta com o operador, inexistindo vínculo imediato com o controlador (ANPD, 2021). Impende-se destacar que, para efeitos da LGPD, tanto o operador quanto o suboperador podem desempenhar a função de operador e responder por eventuais falhas que cometerem. Assim, no que concerne às responsabilidades frente às atividades para as quais foi contratado para executar, o suboperador pode ser equiparado ao operador perante a LGPD (ANPD, 2021).

Há, por exemplo, uma conjectura envolvendo controlador, operador e suboperador quando:

A empresa ALPHA deseja contratar uma pesquisa de mercado para alavancar suas vendas. Para isso, contrata a empresa de pesquisas BRAVO, que envia os resultados para a empresa ALPHA.

Com a autorização da empresa ALPHA, a empresa BRAVO contrata os serviços de armazenamento em nuvem da empresa CHARLIE.

A empresa ALPHA pode ser considerada controladora pois verifica-se que foram cumpridos os seguintes requisitos: i) a empresa A teve poder decisório em relação ao tratamento de dados; ii) os elementos essenciais do tratamento foram definidos pela empresa A: finalidade, titulares (por exemplo mulheres da faixa etária de 20 a 30 anos, residentes em Brasília/DF), tipos de dados (por exemplo nome, idade, endereço, preferência alimentar) etc.

Ainda que possa decidir quanto às técnicas a ser empregadas no processo de tratamento de dados para gerar os resultados da pesquisa, a empresa de pesquisas BRAVO realiza os tratamentos de dados de acordo com a finalidade e as instruções determinadas pela empresa ALPHA, atuando, portanto, como operadora.

A empresa CHARLIE atua conforme diretrizes da empresa BRAVO e seria, portanto, suboperadora. É recomendável que BRAVO obtenha autorização formal de ALPHA para a subcontratação de CHARLIE (ANPD, 2021, p. 20-21).

A autorização formal, genérica ou específica, a que se refere o exemplo é conferida pelo controlador em cláusula contratual de instrumento firmado entre os agentes de tratamento de dados ou após solicitação do operador. A medida, conforme a ANPD (2021), tem por escopo impossibilitar que responsabilidades usualmente exclusivas do controlador sejam atribuídas ao operador em função da contratação do suboperador, uma

vez que, ausente autorização do controlador para contratação de suboperador, perdura a possibilidade de que o operador tenha efetivado o tratamento de dados descumprindo as instruções passadas pelo controlador.

5. BASES LEGAIS: HIPÓTESES AUTORIZATIVAS DO TRATAMENTO DE DADOS PESSOAIS

A expressão “bases legais” consubstancia-se como terminologia cunhada pela doutrina para referenciar as hipóteses insculpidas na LGPD para fundamentar a realização do tratamento de dados pessoais (art. 7º, incisos I - X) e de dados pessoais sensíveis (art. 11, incisos I e II) (SOLER, 2021), estas já explicitadas em seção pretérita ao discorrer-se sobre distinção entre dados pessoais sensíveis e dados pessoais.

Teffé e Viola (2021), ao abordar as hipóteses legais de tratamento de dados pessoais, constatam que a LGPD atribuiu valor e importância a todo dado pessoal, motivação pela qual adotou-se um conceito abrangente para o termo, sendo definido como dado pessoal a informação relacionada a pessoa natural identificada ou identificável (art. 5º, inciso I).

Nessa perspectiva, diante da cautela e prudência que o tema implica, estabeleceu-se como regra geral (art. 1º da LGPD) que todo aquele que empreenda a atividade de tratamento de dados pessoais, independentemente de sua personalidade jurídica, deverá ter uma base legal para respaldar os tratamentos de dados pessoais que venha a realizar (TEFFÉ; VIOLA, 2021). Exceptuam-se, contudo, da necessidade de identificação de uma base legal apropriada os casos que amoldam-se as hipóteses de exclusão de aplicação da lei constantes no artigo 4º da LGPD (TEFFÉ; VIOLA, 2021).

Assim, ressalvadas as hipóteses excepcionais do art. 4º da LGPD, para que o tratamento de dados pessoais revista-se de licitude e legitimidade, faz-se necessária sua conformação à pelo menos uma das hipóteses constantes do rol inscrito no art. 7º da LGPD, o qual, assim como o rol do art. 11, relativo às hipóteses de tratamento de dados pessoais sensíveis, reputa-se taxativo, inexistindo embaraço a cumulação de bases legais (TEFFÉ; VIOLA, 2021), isto é, que o tratamento de dados empenhado pelo agente esteja fundamentado em mais de uma hipótese do rol respectivo.

Caio Lima (2020) consigna que a LGPD (art. 7º, incisos I - X) positivou dez bases legais visando a legitimação do tratamento de dados, exprimindo-se que a ausência de embasamento do tratamento de dados em uma das hipóteses legais implica na obrigatória eliminação do dado, o que, se não observado, acarretará na irregularidade do tratamento de dados e na eventual responsabilização do agente responsável caso cause danos ao titular.

A primeira base legal inscrita no rol do art. 7º da LGPD consubstancia-se no fornecimento do consentimento do titular para que o tratamento de dados revista-se de legalidade e legitimidade. O consentimento do titular é, segundo Caio Lima (2020), a principal base legal, ainda que não seja “a única hipótese legal para o tratamento de dados nem hierarquicamente superior às demais contidas no rol do Art. 7º ou 11 da lei” (TEFFÉ; VIOLA, p. 134, 2021). Soler (2021) denota que subsiste no âmbito doutrinário o entendimento de que é a base legal mais segura, uma vez que, conforme apontam Teffé e Viola (2021), o consentimento do titular obteve tutela destacada na LGPD.

Nesse aspecto, os autores denotam que uma investigação pormenorizada dos princípios da LGPD, “que têm grande parte de seu centro gravitacional baseado no ser humano – revela a preocupação do legislador com a participação do indivíduo no fluxo de suas informações.” (TEFFÉ, VIOLA, 2021, p.134), sinalizando-se que:

O maior cuidado com o consentimento do titular mostra-se de grande relevância no cenário tecnológico atual, no qual se verifica a coleta em massa de dados pessoais, a mercantilização desses dados por parte de uma série de sujeitos e situações de pouca transparência e informação no que tange ao tratamento de dados pessoais de usuários de serviços online. Nesse sentido, defende-se que a interpretação do consentimento deverá ocorrer de forma restritiva, não podendo o agente estender a autorização concedida a ele para o tratamento de dados para outros meios além daqueles pactuados, para momento posterior ou para finalidade diversa.

O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele promove a personalidade, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações. (TEFFÉ; VIOLA, 2021, p. 134).

Nos termos da LGPD, o consentimento é assinalado como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (art. 5º, inciso XII).

Na acepção legislativa, o vocábulo “livre” denota a possibilidade de escolha, pautada no aceite ou na recusa, conferida ao titular de dados pessoais concernente a utilização de seu bem, sem interferências que sejam capazes de eivar seu consentimento, vedando-se, assim, de forma expressa o tratamento de dados pessoais mediante vício de consentimento (TEFFÉ; VIOLA, 2021).

No mesmo sentido, Soler (2021) denota que a disciplina legal inviabilizada que o consentimento seja assinalado como uma presunção, devendo ser concedido por escrito, com cláusula destacada, ou por outro meio específico que evidencie efetiva manifestação

de vontade do titular, consoante preceitua o art. 8º da LGPD, de maneira que o consentimento será livre na medida em que o titular expresse precisamente a aceitação sobre os tipos de dados que serão tratados em cada operação a ser realizada por um agente de tratamento de dados.

Nesse sentido, Caio Lima (2020) entende que é inválido o consentimento manifestado no formato “tudo ou nada”, uma vez que patente o vício de consentimento nesta modalidade. Isso porque, em havendo coleta de dados para distintas finalidades, ao titular deve ser conferida a oportunidade de assentir ou negar de forma individualizada a finalidade específica a qual se destina o tratamento de dados.

A “manifestação informada” a que se refere o inciso II do art. 5º da LGPD exprime a imprescindibilidade da disposição de informações necessárias e suficientes para que o titular compreenda e avalie a forma e o ciclo de tratamento de seus dados pessoais (TEFFÉ; VIOLA, 2021). O consentimento informado será manifestado quando, em momento anterior ao tratamento de dados, houver o fornecimento de “informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados” (TEFFÉ; VIOLA, 2021), reduzindo, no que possível, a disparidade técnica e informacional entre o titular de dados pessoais e os agentes de tratamento dos respectivos dados.

Nessa perspectiva, em consonância aos princípios da finalidade, transparência e adequação, o art. 9º da LGPD expressa que devem ser apresentadas ao titular de dados, de forma clara e ostensiva, as informações relativas à:

- a) finalidades específicas do tratamento;
- b) forma e duração do tratamento, guardados os segredos comercial e industrial;
- c) identificação e informações de contato do controlador;
- d) informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- e) responsabilidades dos agentes que realizarão o tratamento; e
- f) direitos do titular, aí se incluindo menção à possibilidade de confirmação de tratamento dos dados, acesso, atualização, retificação, anonimização, eliminação, além de outros dispostos nos artigos 17 a 22 da Lei. (CAIO LIMA, 2020, p. 203)

O autor alude que, desde que respeitada uma linguagem clara, direta, objetiva e em língua portuguesa, não subsistem limitações quanto à modalidade de obtenção de consentimento. Dessa feita, há viabilidade de consecução do consentimento de variadas formas: por escrito, áudio, vídeo, dentre outros (CAIO LIMA, 2020).

Por fim, a manifestação de vontade deve ser “inequívoca”, isto é, não ambígua, indubitável e de forma clara (TEFFÉ; VIOLA, 2021).

Acrescentam os autores que, atentando-se aos princípios da responsabilização e prestação de contas, é ônus do controlador produzir provas de que o consentimento foi obtido de acordo com os ditames legais, demonstrando, assim, a inexistência de vício apto à eiva-lo (TEFFÉ; VIOLA, 2021).

Considera-se, ainda, segundo Teffé e Viola (2021), que a finalidade da coleta de dados, independentemente da base legal utilizada, deverá ser previamente conhecida.

Nesse sentido, Caio Lima (2020) discorre que as bases legais constantes nos incisos II à X do art. 7º da LGPD são autônomas ao consentimento, isto é, a opção de fundamentar o tratamento em uma destas hipóteses não depende do consentimento do titular de dados para que seja reputada válida, ainda que, conforme retromencionado, não se vislumbrem óbices à cumulação de bases legais.

A segunda base legal para o tratamento de dados pessoais reside no cumprimento de obrigação legal ou regulatória pelo controlador, o que ocorre nas hipóteses em que o controlador fundamenta o tratamento de dados pessoais em determinação legal, seja proveniente do Poder Legislativo por meio de lei federal, estadual ou municipal, a exemplo de deveres oriundo da lei anticorrupção ou de obrigações trabalhistas (TEFFÉ; VIOLA, 2021), seja por meio de medidas do Poder Executivo, como decretos e resoluções (CAIO LIMA, 2020).

A terceira hipótese decorre do tratamento de dados pessoais pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD, regulador do tratamento de dados pessoais pelo Poder Público. Nessa perspectiva, Teffé e Viola (2021, p. 147), entendem que “As políticas em questão podem envolver, por exemplo, a implementação de saneamento básico, de auxílios a cidadãos em situação de vulnerabilidade ou de projetos voltados à educação de crianças e adolescentes”.

A quarta base legal para tratamento de dados pessoais advém da realização de estudos por órgãos de pesquisas, os quais são definidos pela própria LGPD, assegurado, sempre que possível a anonimização dos dados pessoais, situação considerada mais protetiva para o titular de dados pessoais, uma vez que, conforme preceituam Teffé e Viola (2021), o dado anonimizado assegura que o titular não possa ser identificado, sucedendo-se uma desvinculação entre o dado e titular respectivo, de forma que o dado deixa de ser pessoal, o que ocorre, exemplificativamente, em pesquisa para apuração de

intenção de votos em uma eleição na qual as informações são distribuídas em categorias predefinidas, tal qual região geográfica, faixa etária, sexo, sem que seja possível identificar, contudo, os cidadãos que participaram do estudo.

A quinta base legal autorizativa do tratamento de dados decorre da necessidade de legitimação da execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido deste. Nessa hipótese, há pedido do titular para o tratamento de seus dados pessoais visando a execução de obrigações contratualmente firmadas ou em procedimentos preliminares à formalização do contrato (CAIO LIMA, 2020).

Teffé e Viola (2021) exprimem que esta base legal assemelha-se, em certa medida, à hipótese de tratamento de dados a partir do fornecimento de consentimento pelo autor. Destacam, entretanto, que cristalina distinção subsiste entre ambas na medida em que o controlador dos dados estará resguardado pela LGPD enquanto durar a execução do contrato, não podendo, assim, o titular de dados revogar seu consentimento no período aludido, oportunizando a manutenção dos dados pelo controlador. Assim, não há necessidade de consentimento, nos termos definidos pela LGPD e tratados previamente, pelo titular para que o agente de tratamento de dados realize a operação respectiva, necessária à contratação, desde que o titular seja parte ou esteja em tratativas para um contrato (TEFFÉ; VIOLA, 2021).

O acontecimento desta base legal dar-se-á, por exemplo:

a) nas situações em que o titular adquira produtos ou serviços para entregá-los será preciso conhecer o nome completo, o endereço e outras informações de contato do consumidor; e b) levantamentos realizados por instituições financeiras em relação a determinada pessoa, anteriormente à concessão de crédito a ela. (TEFFÉ; VIOLA, 2021, p. 149).

A sexta hipótese para o tratamento de dados pessoais destina-se ao exercício regular de direitos em processo judicial, administrativo ou arbitral. Esta base legal, consoante Caio Lima (2020), decorre de direitos constitucionalmente assegurados à inafastabilidade do Poder Judiciário (artigo 5º, inciso XXXV, CRFB/1988) e ao contraditório e ampla defesa (artigo 5º, inciso LV, CRFB/1988).

Nesse sentido, para Teffé e Viola (2021, p. 149), “O exercício regular de direitos compreende ações do cidadão comum autorizadas pela existência de direito definido em lei e condicionadas à regularidade do exercício desse direito”. Nesses casos, é vedada a conduta abusiva ou desempenho funcional de certa posição jurídica pela parte,

entendendo a doutrina que o tratamento e armazenamento de dados pessoais nesta base legal está condicionado à utilidade destes dados como elementos para o exercício de direito em demandas, quando evidente real necessidade e para essa finalidade (TEFFÉ; VIOLA, 2021).

Nesse contexto, apontam Teffé e Viola (2021, p. 149):

Entende-se que não seria razoável que uma parte ficasse privada de legitimamente se defender, tendo que depender do consentimento da parte adversa para apresentar determinadas provas ou informações para a defesa de seus interesses. Protege-se, assim, a ampla defesa e o contraditório.

Assim, os autores exprimem que esta hipótese, de base ampla, visa assegurar o direito de produção de provas de uma parte em face da outra no curso de processos em geral (judicial, administrativo ou arbitral) a partir do uso de dados pessoais (TEFFÉ; VIOLA, 2021).

A sétima hipótese concerne ao tratamento de dados pessoais para a proteção da vida ou da incolumidade física do titular ou de terceiro. Caio Lima (2020) aduz que trata-se de base legal restritiva, uma vez que essas questões relacionam-se a circunstâncias graves em que a vida ou integridade física do titular de dados ou de terceiro é posta em risco.

Exemplificativamente, há a utilização desta base legal para:

obtenção de dados de geolocalização de celulares visando a encontrar pessoas desaparecidas em desastres e escombros ou que possam ter sido sequestradas ou estar perdidas. Outra aplicação dessa base poderia ser para o tratamento de dados importantes para se conter o avanço de epidemias, como o recente caso do Covid-19. (TEFFÉ; VIOLA, 2021, p. 150).

A oitava base legal conduz à tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Soler (2021) salienta que esta é uma dentre as reduzidas hipóteses nas quais a lei direciona o tratamento de dados à agentes específicos, quais sejam, os retromencionados profissionais de saúde, abarcando médicos, enfermeiros, farmacêuticos, educadores físicos, fisioterapeutas, nutricionistas, biomédicos, dentre outros; serviços de saúde, isto é, “estabelecimentos destinados a promover a saúde do indivíduo, protegê-lo de doenças e agravos, prevenir e limitar os danos a ele causados e reabilitá-lo quando sua capacidade física, psíquica ou social for afetada” (ANVISA, online); ou autoridade sanitária, compreendendo as entidades integrantes do SNVS (Sistema Nacional de Vigilância Sanitária), a exemplo da ANVISA (Agência Nacional de Vigilância

Sanitária), Laboratórios Centrais de Saúde Pública (LACENS); Instituto Nacional de Controle de Qualidade em Saúde (INCQS); Fundação Oswaldo Cruz (FIOCRUZ) (CAIO LIMA, 2020).

A saúde, na condição de direito fundamental (art. 196, CRFB/1988), recebeu tutela específica na lei, uma vez que:

O cuidado com a mencionada base deve existir entre outras razões porque, a partir da solicitação de exames ou da análise de dados de saúde, é possível inferir inclusive situações sensíveis sobre determinada pessoa e, se utilizados de maneira inadequada, podem dar ensejo a discriminações ilegítimas ou abusivas (Art. 6.º, IX). Em relação à autoridade sanitária, recorda-se a Lei 9.782/1999, que define o Sistema Nacional de Vigilância Sanitária e cria a Agência Nacional de Vigilância Sanitária. (TEFFÉ; VIOLA, 2021, p. 151)

A nona e penúltima hipótese chancela o tratamento de dados pessoais quando necessário ao atendimento de interesses legítimos do controlador ou de terceiro, excepcionado o caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Soler (2021) aponta que a base legal em referência é abrangente e dotada de elevado grau de subjetividade, uma vez que não há definição legal na LGPD sobre as causas que poderiam revestir-se de “interesses legítimos”, ou mesmo a indicação de finalidade específica para esta hipótese de tratamento de dados, tal qual manifestado nas demais bases legais.

A autora define, entretanto, que depreende-se da interpretação literal do artigo que o legítimo interesse não pode ser sobreposto aos direitos fundamentais dos titulares (SOLER, 2021). Nessa perspectiva, Teffé e Viola (2021, p. 141) constatam que “quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse”, dada a relevância da expectativa do titular de dados frente à flexibilidade da base legal.

Os autores, diante da omissão legislativa concernente a conceituação da expressão “interesse legítimo”, definem-na como resultado ou benefício nítido e específico esperado pelo controlador, ou por terceiro, a partir de uma determinada operação de tratamento de dados pessoais cuja finalidade seja ética e lícita, sendo inservível, para fins de configuração de legítimo interesse, a afirmação de “existência de interesses comerciais vagos ou genéricos” (TEFFÉ; VIOLA, 2021 p.141).

A nebulosidade conferida ao conceito pela ausência de redação legislativa delimitadora da amplitude de sua incidência é refletiva na multiplicidade de situações nas quais o legítimo interesse pode ser manifestado:

a) o tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controle de fraudes ou para garantir a segurança da rede e da informação nos sistemas informáticos de determinada instituição; b) fornecimento de imagens de câmeras de segurança para fins de seguro; c) segurança e melhoria de produtos e serviços; d) tratamentos de dados de empregados para programas de retenção de talentos e iniciativas de bem-estar; e) no caso de uso de dados por uma empresa para fazer ofertas mais adequadas e personalizadas a seus clientes, usando apenas os dados estritamente necessários para tal; f) envio de e-mail com descontos específicos para os produtos buscados por determinado usuário ou com indicações de compras, tomando como base seu histórico de compras; g) lembrar ao usuário que ele deixou itens no carrinho online, mas não finalizou a compra; e h) reunião de informações sobre determinado candidato em processos seletivos (TEFFÉ; VIOLA, 2021, p.142).

Assim, diante da ausência de conceito legal sobre a terminologia em análise e de parâmetros expressamente delimitados na lei para sua utilização, considera-se que o Poder Judiciário terá destacada responsabilidade na atribuição de significado a expressão “interesses legítimos” no caso concreto (TEFFÉ; VIOLA, 2021).

Dessa forma, segundo Soler (2021), visando concretizar parâmetros interpretativos para a análise de ocorrência do requisito do legítimo interesse, articulou-se no âmbito doutrinário, seguindo o modelo europeu de proteção de dados, o desenvolvimento do *Legitimate Interests Assessment* (LIA), isto é, um teste de ponderação. Teffé e Viola (2021) asseveram que intenta-se, ao adotar o teste de ponderação, sopesar os direitos inerentes aos titulares de dados e aos agentes de tratamento de dados, examinando-se, no decurso do LIA, a efetiva existência de um interesse legítimo do responsável pelo tratamento de dados e a proteção aos direitos e liberdades fundamentais dos titulares, respeitando-se suas legítimas expectativas.

O teste de ponderação para Soler (2021, p. 21) compreende três análises:

1. Teste de Finalidade – identificação de quem é o legítimo interesse;
2. Teste de Necessidade – validação se de fato é necessário esse tratamento de dados para que seja atingido o interesse pretendido;
3. Teste de Balanceamento – equalização do tratamento com os direitos do titular.

A autora expressa que a adoção de um teste de ponderação não materializa uma inovação jurídica, pois revela apenas a proposição de uma fórmula utilizada como parâmetro para averiguar e justificar a presença do legítimo interesse no caso concreto, legitimando o tratamento de dados por essa base legal (SOLER, 2021).

Teffé e Viola (2021, p. 242), por sua vez, manifestam que a análise para averiguação do preenchimento dos requisitos asseguradores da ocorrência do legítimo interesse compreende quatro fases:

- (i) a avaliação dos interesses legítimos; (ii) o impacto sobre o titular do dado; (iii) o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e (iv) salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado

Os autores assentam, nesse sentido, que constam em rol exemplificativo no art. 10 da LGPD parâmetros para autorizar e fundamentar a utilização do legítimo interesse como base legal para tratamento de dados pessoais que dispensa a anuência do titular (TEFFÉ; VIOLA, 2021).

Assim, conclui-se que os dispositivos atinentes ao legítimo interesse na LGPD (art. 7º, IX; art. 10) indicam a adaptação parcial do teste de ponderação à legislação de proteção de dados brasileira, viabilizando-se a avaliação de existência do legítimo interesse no caso concreto (TEFFÉ; VIOLA, 2021).

A décima e última base legal de dados concerne à proteção de crédito.

Soler (2021) enfatiza que a LGPD, novamente, positivou um termo de conteúdo amplo sem conferir-lhe conceito legal, o que implica, por sua própria natureza, na extensão de aplicação desta hipótese de tratamento de dados à toda cadeia de crédito. Teffé e Viola (2021) aduzem que a adoção dessa base legal visa, a partir dos tratamentos realizados, ampliação e facilitação da concessão de crédito, a melhoria nas análises de risco e o impulsionamento do mercado de consumo.

Há, portanto, nesta hipótese, conforme Teffé e Viola (2021, p. 152) a necessidade de manutenção de “constante diálogo com normas como o CDC (Código de Defesa do Consumidor) (Lei 8.078/1990), a Lei do Cadastro Positivo (Lei 12.414/2011) e portarias do Ministério da Justiça”.

Isso porque, consoante Soler (2021), ao abarcar a integralidade da cadeia de crédito, o inciso X do art. 10 da LGPD possibilita o tratamento de dados com fundamento na proteção ao crédito por instituições financeiras, empresas de cobrança e birôs de crédito, isto é, empresas cuja finalidade perfaz-se na análise e estudo do *score* de crédito.

Nessa senda, torna-se imprescindível a consolidação desta base legal a partir do diálogo de fontes, integrando-a às normas relativas à proteção do consumidor e ao

cadastro positivo, profícua ao estabelecimento de uma rede ampla de salvaguarda aos direitos do titular de dados integrante de relação consumerista.

6. REGIME JURÍDICO DE RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS NA LGPD

A problemática que circunda o regime jurídico de responsabilidade civil dos agentes de tratamento de dados reside no fato de que foi dedicada seção na íntegra à responsabilidade e ressarcimento de danos na LGPD, sem, contudo, haver menção expressa ao regime jurídico ao qual estão suscetíveis os agentes de tratamento que, no exercício de suas atividades, causarem danos a outrem.

Assim, a LGPD, ao tratar sobre a responsabilidade e o ressarcimento de danos, disciplinados entre arts. 42 e 45 da Lei, constantes na seção III (“Da responsabilidade e do Ressarcimento de Danos”) do capítulo VI (“DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS”), ficou silente quanto ao regime de responsabilidade dos agentes de tratamento de dados nas hipóteses de violação aos seus dispositivos legais.

Dessa forma, não existe, no âmbito da LGPD, nitidez quanto à aplicabilidade da responsabilidade subjetiva, levando em consideração a “culpa genérica” (dolo, decorrente de conduta voluntária ou culpa, decorrente de imprudência, negligência ou imperícia), ou objetiva, excluindo-se o elemento da culpa, considerando, portanto, a atividade de tratamento de dados como atividade que, por sua natureza, implica risco aos direitos de outrem. Guedes, Tepedino e Terra (2022) destacam que a ausência de indicação expressa da espécie de responsabilidade civil aplicável aos agentes de tratamento de dados no âmbito da LGPD é uma das principais críticas tecidas pela doutrina à lei.

Bruno (2020), na mesma perspectiva, denota que, em se tratando de diretrizes para ordenar a responsabilização dos agentes de tratamento de dados pessoais, é fundamental o estabelecimento de critérios nítidos e hialinos no intento de assegurar a atenuação da manifesta disparidade existente entre o titular de dados pessoais e o agente responsável pelo respectivo tratamento em uma relação de tratamento de dados pessoais.

Enfatiza-se que a fixação concreta do regime jurídico de responsabilidade civil dos agentes de tratamento de dados, de forma objetiva, subjetiva ou diferenciada, não está circunscrita aos argumentos erigidos no âmbito teórico, uma vez que conserva diversas repercussões práticas, constituindo-se como elemento hábil a impulsionar o modo como serão desenvolvidas as atividades de tratamento de dados pessoais consoante disposições normativas da LGPD, influir no comportamento das partes

integrantes de relação de tratamento de dados pessoais (agentes de tratamento e titulares de dados pessoais) e instituir ônus processuais.

6.1 RESPONSABILIDADE CIVIL

A responsabilidade civil é um instituto clássico do direito, consistente na:

Efetivação da reparabilidade abstrata do dano em relação a um sujeito passivo da relação jurídica que se forma. Reparação e sujeito passivo compõem o binômio da responsabilidade civil, que então se enuncia como o princípio que subordina a reparação à sua incidência na pessoa do causador do dano.

Não importa se o fundamento é a culpa, ou se é independente desta. Em qualquer circunstância, onde houver a subordinação de um sujeito passivo à determinação de um dever de ressarcimento, aí estará a responsabilidade civil (SILVA, TEPEDINO, 2018, p. 34).

Sintetizando a definição trazida por Caio Mário Pereira da Silva e atualizada por Gustavo Tepedino (2018), Tartuce (2021) reputa que a responsabilidade civil decorre de descumprimento obrigacional, em razão de desobediência à regra estipulada contratualmente, isto é, o inadimplemento contratual, caracterizando a responsabilidade contratual, ou, ainda, pela inobservância de preceito normativo que regula a vida, o que consubstancia a prática de ato ilícito, a qual, fora da esfera de estipulação prévia entre as partes, é denominada responsabilidade extracontratual ou aquiliana.

Nesse sentido, o CC/2002 recepcionou um sistema dualista de responsabilidade, no qual a regra é a responsabilidade subjetiva, baseada na Teoria da Culpa, prevista em seu art. 186, disciplinando, para as hipóteses previstas em lei e para as atividades de risco, regime jurídico de responsabilidade objetiva, fundado na Teoria do Risco, delimitado no art. 927, parágrafo único, do regramento civil.

Assim dispõe o CC/2002 sobre a responsabilidade subjetiva: “Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.” (BRASIL, 2002).

De igual maneira, disciplina a responsabilidade objetiva:

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (BRASIL, 2002)

À modalidade subjetiva de responsabilidade civil, regra no ordenamento jurídico brasileiro, segundo Tartuce (2021), ainda que não subsista consenso na doutrina em relação à definição dos critérios, quatro são os pressupostos necessários a caracterização do dever de indenizar: (I) conduta humana; (II) culpa genérica ou *lato sensu*; (III) nexo de causalidade; (IV) dano ou prejuízo.

Por sua vez, na modalidade objetiva, assentada na Teoria do Risco da Atividade, a responsabilização do agente, em razão de hipóteses especificadas em lei ou quando a atividade usualmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem, ocorrerá independentemente de culpa, de modo que necessários à sua configuração três requisitos: (I) conduta humana; (II) nexo de causalidade; (III) dano ou prejuízo.

6.2 DA REGULAMENTAÇÃO DA RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS NA LGPD

O art. 42 da LGPD regula a responsabilidade dos agentes de tratamento de dados pessoais, evidenciando a possibilidade de reparabilidade, tanto pelo controlador, quanto pelo operador, quando este causarem a outrem, em função do exercício da atividade de tratamento de dados pessoais e em violação aos preceitos normativos da LGPD, danos de ordem patrimonial, moral, individual ou coletivo (BRUNO, 2020).

O inciso I do §1º do art. 42 da LGPD determina a equiparação do operador ao controlador de dados pessoais para fins de responsabilidade civil em razão do tratamento de dados pessoais nas hipóteses em que descumprir a legislação de proteção de dados ou deixar de observar as instruções do controlador para a operação de tratamento de dados, ressaltando-se que o operador será igualmente equiparado ao controlador quando divisar que as instruções deste são ilícitas e, ainda assim, prosseguir com o tratamento de dados pessoais (CÍNTIA LIMA, 2020). Nas circunstâncias em que equiparado for ao controlador, o operador responderá solidariamente com este pelos danos causados, causa pela qual é fundamental que o operador compreenda a legislação de dados pessoais para que, além de cumprir as determinações do controlador, fique circunscrito aos ditames legais no exercício de suas atribuições, conforme preceitua Cíntia Lima (2020).

O inciso II do §1º do art. 42, por sua vez, estabelece a responsabilidade solidária entre controladores envolvidos em atividade de tratamento de dados, fator benéfico para o

titular de dados pessoais em consequência da complexidade usual da cadeia de agentes vinculados a operação de tratamento de dados pessoais, sendo demasiado custoso imputar ao titular de dados pessoais o ônus de identificar o agente fomentador do dano causado a si em razão de descumprimento da LGPD (BRUNO, 2020).

Os §§ 2º, 3º e 4º do art. 42 não se dedicam diretamente ao estabelecimento de pressupostos para responsabilização civil dos agentes de tratamento de dados pessoais, ainda que essenciais à análise sistemática da responsabilidade civil no âmbito da LGPD. O §2º trata do direito de regresso, contra os corresponsáveis, daquele que reparar o dano do titular, enquanto o §3º trata da tutela coletiva de direitos e o §4º dispõe sobre distribuição do encargo probatório (BRUNO, 2020).

Andrade e Magro (2022) reputam que o óbice ensejador das discordâncias acadêmicas e da conseqüente formulação de distintas correntes doutrinárias para especificar o regime de responsabilidade jurídica ao qual estão suscetíveis os agentes de tratamento de dados pessoais na LGPD advêm essencialmente da insuficiência redacional do art. 42 da norma de proteção de dados, considerado elementar à sistemática de responsabilização e ressarcimento na LGPD. Os autores exprimem que a interpretação gramatical do dispositivo normativo, por si só, é inservível ao assentamento de um regime de responsabilidade civil dos agentes de tratamento de dados à míngua de fundamentos aptos a denotar a independência da culpa, consagrando a responsabilidade objetiva, ou a imprescindibilidade de perquirir a conduta do agente, legitimando a responsabilidade subjetiva (ANDRADE; MAGRO, 2022).

Essa problemática decorre, segundo Andrade e Magro (2022), dos erros de projeto que vitimaram a LGPD, ainda que decorrente da conjugação de projetos de lei consideravelmente longevos, destacando-se vícios de inconstitucionalidade do processo seletivo responsáveis pela retirada do pretense regime especial de responsabilidade civil no âmbito da legislação de proteção de dados.

O art. 43 da LGPD sedimenta as “hipóteses excludentes de responsabilidade dos agentes de tratamento de dados pessoais envolvidos em um evento danoso.” (BRUNO, 2020, p. 368).

A primeira hipótese, segundo o autor, concerne à prova de que o agente não realizou o tratamento de dados pessoais que lhe é atribuído, o que, a despeito da obviedade da afirmação, mostra-se relevante devido ao caráter complexo da atividade de dados pessoais, expressa na responsabilidade solidária dos agentes envolvidos em uma atividade de de tratamento de dados pessoais (LGPD, art. 42, §1º, II) (BRUNO, 2020).

A segunda possibilidade, relaciona-se, segundo Bruno (2020) à exclusão da ilicitude do ato, o que afasta o dever de indenizar diante da prova de que não houve violação à LGPD quando do exercício do tratamento de dados que lhe é atribuído.

A terceira hipótese, por fim, exclui a responsabilidade do agente de tratamento de dados pessoais em função da culpa exclusiva da vítima ou de terceiros, situação que rompe o nexo de causalidade entre o ato do agente e o dano suportado pela vítima do evento, elemento essencial à configuração da responsabilidade civil, tanto na modalidade objetiva, quanto na modalidade subjetiva (BRUNO, 2020). Rompido o nexo de causalidade, não subsiste a responsabilidade ensejadora do dever de indenizar.

O art. 44 da LGPD conceitua o “tratamento irregular de dados pessoais”, o que ocorrerá “quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes”.

A primeira possibilidade de tratamento irregular perfaz-se na violação dos preceitos legais da LGPD, enquanto a segunda hipótese considera irregular o tratamento de dados pessoais quando, consideradas as circunstâncias relevantes, dentre as quais as previstas nos incisos do art. respectivo, constatar-se que ausente a segurança que dele podia-se esperar (BRUNO, 2020).

Andrade e Magro (2022) discorrem que, ainda que considerada a interpretação do art. 42 da LGPD em conjunto com os subseqüentes arts. 43 e 44, que lhe são complementares, é inexorável a inexecutabilidade da estipulação concreta da modalidade de responsabilidade civil aplicável aos agentes de tratamento de dados pessoais.

O art. 45 da LGPD, em fim, positiva a amálgama dos microssistemas de proteção de dados pessoais e de defesa do consumidor no que tange à responsabilidade civil na hipótese em que a violação dos direitos do titular de dados pessoais devido a irregularidade no tratamento de seus dados opera-se em relação de consumo (BRUNO, 2020).

Nessa hipótese, em circunstância na qual o titular de dados pessoais também é consumidor, nos termos da legislação respectiva, subsiste a viabilidade de invocar o sistema de responsabilização previsto no Código de Proteção e Defesa do Consumidor, e legislação correlata (BRUNO, 2020).

6.3 CORRENTES DOUTRINÁRIAS DE INTERPRETAÇÃO QUANTO AO FUNDAMENTO DA RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS NA LGPD

No âmbito doutrinário, considerando-se a atualidade do tema, o entendimento acerca do regime de responsabilidade dos agentes de tratamento de dados foi ramificado em três linhas de pensamento: (I) considera-se o tratamento de dados uma atividade de risco, de forma que seria aplicável o regime de responsabilidade objetiva; (II) a responsabilidade civil do agente de tratamento de dados somente é configurada quando demonstrada a culpa do ofensor e o dano causado ao titular dos dados; subsistindo, ainda, (III) a consideração de que LGPD inaugurou um regime jurídico diferenciado, *sui generis*, alicerçado, por exemplo, na prevenção, ou dualista, considerando casuisticamente o regime de responsabilidade ao qual o agente de tratamento de dados está suscetível.

6.3.1 Responsabilidade Objetiva

As convicções que alicerçam o entendimento de que o regime jurídico de responsabilidade atribuível aos agentes de tratamento de dados pessoais é de natureza objetiva originam-se da perspectiva de que, com o intento de aplacar efetivamente o risco de vazamentos de dados pessoais, o legislador objetivou restringir ao máximo as hipóteses nas quais o tratamento dos referidos dados é juridicamente permitido, conforme preconizado por Andrade e Magro (2022).

Os autores, ao cotejarem distintas vertentes doutrinárias acerca da responsabilidade civil dos agentes de tratamento de dados, mencionam o estudo elaborado por Danilo Doneda e Laura Mendes em 2018, considerado precursor da concepção de que o risco intrínseco à atividade de tratamento de dados é o parâmetro prevacente para imputação do dever de indenizar no âmbito da LGPD, o que conduz, portanto, à responsabilização objetiva dos agentes de tratamento de dados (ANDRADE; MAGRO, 2022).

Doneda e Mendes (2018, p. 467), citados por Andrade e Magro (2022), evidenciam que a avaliação acerca da responsabilidade civil dos agentes de tratamento de dados demanda análise sistemática da norma de proteção de dados em sua integralidade, não se cingindo à seção concernente à responsabilidade dos agentes de tratamento de dados.

Assim, a estruturação normativa da LGPD indica que, ao perquirir-se sobre a responsabilização dos agentes de tratamento de dados pessoais, deve-se

considerar que, em regra, o tratamento de dados pessoais está condicionado à observância uma das bases legais exaustivamente elencadas no art. 7º, que o tratamento não deve perpassar a coleta e processamento de dados além do estritamente necessário à consecução de sua finalidade, consoante os princípios da finalidade (art. 6º, I) e da necessidade (art. 6º, III), que o tratamento não deve ser desproporcional ou inadequado à sua finalidade, conforme preceituado pelo princípio da adequação (art. 6º, II), que a norma de proteção de dados adota como conduta padrão a eliminação dos dados quando encerrado o tratamento (art. 16) e que a LGPD, em sua redação normativa, preceitua, em diversas excertos, a imprescindibilidade de que o agente considere o risco presente no tratamento de dados (ANDRADE; MAGRO, 2022 *apud* DONEDA; MENDES, 2018, p. 467).

O cerne desta percepção reside, assim, na convicção de que a atividade de tratamento de dados pessoais apresenta riscos inerentes aos titulares respectivos, conclusão amparada na interpretação sistemática da LGPD, legislação de proteção de dados que, dentre seus fundamentos principais, intenta minguar os referidos riscos, perfazendo tal objetivo ao, conforme asseverado por Doneda e Mendes (2018, p. 467), citados por Andrade e Magro (2022, p. 216), “minimizar as hipóteses de tratamento àqueles que sejam, em um sentido geral, úteis e necessárias” ao titular dos dados pessoais.

Mulholland (2020), outrossim, conclui que, a despeito das inexatidões redacionais da LGPD, adota-se nos arts. 42 e 44 da legislação pátria de proteção de dados fundamento de responsabilidade civil objetiva, de forma que seria prescindível a comprovação, por parte do titular de dados pessoais que alegue ter sofrido danos em decorrência do exercício da atividade de tratamento de dados, da existência de conduta culposa do operador ou controlador, para que constituído o dever de indenizar, sendo suficientes à sua caracterização a demonstração de ato antijurídico decorrente de violação a preceitos normativos da LGPD por parte do agente de tratamento de dados, dano sofrido pelo titular de dados pessoais e o nexo de causalidade entre ambos.

Alicerça sua conclusão na perspectiva de que a atividade de tratamento de dados pessoais implica em riscos inatos aos titulares dos dados pessoais, os quais são intrínsecos e indissociáveis das operações de tratamento de dados e ocasionam danos ao direito fundamental à proteção de dados (art. 5º, LXXIX, CRFB/1988).

Ressalta, ainda, que:

tais danos se caracterizam por serem quantitativamente elevados e qualitativamente graves, ao atingirem direitos difusos, o que, por si só, já justificaria a adoção da responsabilidade civil objetiva, tal como no caso dos danos ambientais e dos danos causados por acidentes de consumo. (MULHOLLAND, 2020, online),

Gondim (2021) denota que a omissão legislativa que resultou na ausência de critérios preestabelecidos para definição da modalidade de responsabilidade civil dos agentes de tratamento de dados resulta, a princípio, na integração desta à regra geral de responsabilização subjetiva positivada no *caput* do art. 927 do CC/2002, dado que para incidência da cláusula geral de responsabilidade objetiva, prevista no parágrafo único do art. 927 do CC/2002, a conduta antijurídica ensejadora de reparabilidade, independentemente de culpa, deve ter expressa previsão legal ou resultar de atividade usualmente desenvolvida pelo autor do dano cujo risco é inerente por sua própria natureza.

Não obstante, a autora considera exercício da atividade de danos pessoais como uma atividade de risco, seja em se tratando de dados pessoais ditos gerais, sejam em se tratando de dados pessoais sensíveis, o que amolda a responsabilidade civil dos agentes de tratamento de dados à modalidade objetiva, prescindindo da culpa, devido à cláusula geral de responsabilidade objetiva, prevista no parágrafo único do art. 927 do CC/2002 (GONDIM, 2021).

Destaca, nesse sentido, que incorporação do risco como cláusula geral deu-se da forma como disposta no parágrafo único do art. 927 do CC/2002 com o intento de viabilizar “pela atividade de interpretação e concreção judicial sua aplicação a novas situações ou riscos que venham a surgir ou se desenvolver com base nos avanços da ciência e da técnica” (GONDIM, 2021, apud BRUNO, 2015, p. 107), o que relaciona-se essencialmente ao desenvolvimento do tratamento de dados pessoais hodiernamente, sobretudo nos meios digitais, sendo, portanto, abrangida pelo regime objetivo de responsabilidade civil.

A autora conclui que, em interpretação sistêmica da norma de proteção de dados, é mais razoável a convicção de que os agentes de tratamento de dados respondem objetivamente pelos danos causados ao titular de dados pessoais no exercício da atividade de tratamento de dados pessoais, uma vez que, além do risco inerente à esta operação, o risco eventualmente causado afronta direito fundamental do titular de dados pessoais e a averiguação de culpa mediante análise de descumprimento de deveres legais constitui óbice à reparação integral do titular dados pessoais (GONDIM, 2021).

Cíntia Lima (2020), por sua vez, entende que a estrutura de excludentes de responsabilidade preconizada no art. 43 da LGPD desvela a problemática originada da ausência de estabelecimento concreto de regime de responsabilidade civil objetivo ou subjetivo na norma de proteção de dados, imputando aos agentes de tratamento de dados responsabilidade objetiva, a qual só será afastada quando provarem:

a) que não realizaram o tratamento dos dados pessoais que lhes é atribuído; b) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou c) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (CÍNTIA LIMA, 2021, p. 292)

Divino e Lima (2020) concebem dupla justificativa para entendimento de que a responsabilidade pelos ilícitos praticados pelos agentes no exercício da atividade de tratamento de dados é objetiva. Sumariamente, consideram, em momento anterior à constitucionalização do direito à proteção de dados, que este é um direito fundamental porquanto intrinsecamente relacionados aos direitos de personalidade. Finalmente, constituem o argumento central na defesa da imputação de responsabilidade objetiva aos agentes de tratamento de dados na medida em que expressam que a própria norma de proteção de dados pessoais delimitou, em rol taxativo, as hipóteses, acima referida, nas quais o operador e o controlador não serão responsabilizados, do qual não consta a verificação da ausência de culpa (negligência, imprudência ou imperícia) “para eventual esquia reparatória ou compensatória” (DIVINO; LIMA, 2020, p. 15).

Andrade e Magro (2022) consideram, ainda, ao exporem as distintas correntes de pensamento sobre responsabilização dos agentes de tratamento de dados pessoais, que faz-se possível a imputação de regime de responsabilidade objetiva ao operador e ao controlador em face da convergência entre a LGPD e o CDC devido à proximidade redacional e sistemática constatada entre as normas.

A opção por uma modalidade objetiva de responsabilidade civil no âmbito da LGPD também atine às relações jurídico-processuais direta e indiretamente, na medida em que influi, por exemplo, nos encargos processuais atribuídos às partes e no modo como os agentes encaram a atividade de tratamento de dados pessoais, atuando com prudência e precaução na consecução de seus interesses em face da necessidade de salvaguarda dos dados dos titulares respectivos diante da perspectiva de responsabilização objetiva na hipótese de eventual falha que implique em violação à LGPD.

Doneda (2020), nessa senda, enuncia que a adoção do modelo objetivo de responsabilidade civil é medida facilitadora do exercício dos direitos inerentes ao titular dados pessoais no curso de ação judicial com a finalidade reparar danos por si suportados devido à irregularidade no tratamento de seus respectivos dados, uma vez, conforme aludido por Andrade e Magro (2022), é flagrante a dificuldade de demonstração do dano na tutela do direito à proteção de dados, reconhecendo-se, neste aspecto, sua hipossuficiência em face do agente de tratamento de dados pessoais:

Um papel auxiliar da responsabilidade civil, no entanto, pode se integrar na disciplina de proteção de dados, principalmente se vier acompanhada da definição de casos específicos de responsabilidade objetiva – vide que a imensa dificuldade na demonstração do dano é um dos maiores problemas enfrentados pela consolidação da tutela da proteção de dados. Assim, uma disciplina de responsabilidade objetiva específica para o setor de tratamento de dados pessoais pode ser um instrumento tanto para a satisfação de interesses lesados como para fomentar uma determinada cultura no tratamento desses dados (DONEDA, 2020, p. 289).

Depreende-se, portanto, que distintas são as teses adotadas para se chegar à conclusão de que o regime jurídico de responsabilidade civil dos agentes de tratamento de dados é objetivo, citando-se, de forma mais recorrente, que a atividade de tratamento de dados pessoais possuir riscos inerentes à sua operação. Outrossim, subsistiram os argumentos de que o direito à proteção de dados constitui-se como direito fundamental, que o rol de excludentes de responsabilidade que não menciona a ausência de culpa como ensejadora da não responsabilização do operador e do controlador, bem como que o regime objetivo atua como meio de facilitação da defesa do titular de dados pessoais.

6.3.2 Responsabilidade Subjetiva

O entendimento de que o regime de responsabilidade civil adotado pela LGPD foi subjetivo, ainda que a norma de proteção de dados não tenha sido explícita quanto à natureza da responsabilidade civil dos agentes de tratamento, resulta de três fundamentos intrínsecos à própria estruturação normativa da LGPD (GUEDES; MEIRELES, 2019). O primeiro alude ao histórico de tramitação legislativa que resultou na LGPD. O segundo concerne à instituição, na LGPD, de *standards* (padrões) de conduta a serem seguidos pelos agentes de tratamento. O terceiro refere-se à excludente de responsabilidade preconizada no inciso II do art. 43 da LGPD (GUEDES; MEIRELES, 2019).

Andrade e Magro (2022, p. 222) denotam, quanto ao primeiro fundamento, que o “ao longo do processo de maturação dos projetos que originaram a LGPD, notadamente o PL nº 5.276, foi-se retirada a única disposição expressa acerca de responsabilidade objetiva em capítulo atinente à transferência internacional de dados”. Guedes e Meireles (2019, p. 123) expressam que no art. 35 do referido capítulo havia “regra geral expressa de responsabilidade solidária e objetiva desses agentes pelos danos causados em virtude do tratamento de dados”.

Nas versões subsequentes do Projeto de Lei até a versão sancionada da LGPD, não subsistiu menção no sentido de adoção, como regra geral, de regime objetivo de responsabilidade civil pelos danos causados por agentes no exercício da atividade de tratamento de dados, de forma que a referencia à responsabilidade civil foi integralmente suprimida do texto legal, o que conduz, em análise histórica, à conclusão de que o legislador, a despeito da omissão legislativa constante na LGPD, optou pelo regime subjetivo de responsabilidade civil na LGPD (GUEDES; MEIRELES, 2019).

Andrade e Magro (2022), no mesmo sentido, explanam que a exclusão do dispositivo que previa responsabilidade objetiva dos agentes de tratamento, associada à omissão legislativa em prever expressamente hipóteses de responsabilidade objetiva, conduzem a presunção de que fora consagrada na LGPD regime de responsabilidade subjetivo, considerando-se que, se a intenção do legislador fosse diversa, incluir-se-ia disposição normativa a ela referente.

Bioni e Dias (2020, p. 4), quanto ao processo de elaboração da LGPD, destacam que os quase dez anos de debates que conduziram à atual redação do diploma normativo de proteção de dados deixaram “pistas hermenêuticas valiosas e possibilidades analíticas a partir dos trabalhos preparatórios da lei”.

Aduzem os autores que houve forte embate para definição do regime jurídico de responsabilização dos agentes de tratamento de dados, tanto no que se refere à seção especificamente destinada a este fim, quanto no que concerne aos elementos que lhe são correlatos e, encontrando-se dispostos em outras seções da LGPD, influem no regime jurídico de responsabilidade dos agentes de tratamento de dados (BIONI; DIAS, 2020).

Assim, enfatiza-se, no curso do trâmite legislativo para desenvolvimento de norma atinente à proteção de dados pessoais, a qual consubstanciou-se na LGPD: “a) o abandono deliberado do regime de responsabilidade civil objetiva; e b) a adoção de técnica legislativa mais prescritiva quanto às excludentes de reponsabilidade civil” (BIONI; DIAS, 2020, p. 5).

O segundo fundamento, central na defesa da adoção da modalidade subjetiva de responsabilidade civil na LGPD, perfaz-se, segundo defesa de Guedes e Meireles (2019), na positivação do capítulo VII da LGPD destinado à “segurança e boas práticas”, o qual é subdividido em duas seções: i) Seção I – Da segurança e do sigilo de dados; ii) Seção II – Das Boas Práticas e da Governança.

A LGPD instituiu, segundo as autoras, nessas seções, uma série de deveres de cuidados que vinculam o agente de tratamento, precisando *standards* (padrões) de conduta a serem compulsoriamente seguidos pelo operador e pelo controlador, notando-se a atenção conferido legislador à conduta dos agentes de tratamento, inclusive ao cumprimento de programas, procedimentos, política internas, padrões técnicos, mecanismos de supervisão, dentre outros (GUEDES; MEIRELES, 2019).

Destaca-se, ainda, no âmbito do estabelecimento de deveres de cuidado ensejadores do cumprimento de padrões de conduta pelos agentes de tratamento, que o art. 6º, X, da LGPD, positiva os princípios da responsabilização e da prestação de contas, pelos quais é essencial a “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.” (BRASIL, 2018). Nessa perspectiva, Guedes e Meireles (2019) afirmam que não há coerência em impor aos agentes de tratamento o dever de adotar mecanismos eficazes ao cumprimento das normas de proteção, comprovando sua diligência ao proceder à prestação de contas ao comprovar a eficácia das medidas adotadas, se, em havendo incidente que ocasione danos ao titular de dados, será responsabilizado independentemente de ter cumprido, na íntegra, os deveres de segurança preconizados na legislação.

De igual maneira, a partir de análise sistemática da lei, não se chega a outra conclusão senão a de que a modalidade apropriada à responsabilização dos agentes de tratamento de dados é subjetiva, uma vez que não há sentido em impor aos agentes de tratamento diversos padrões de conduta, orientativos de sua atuação no exercício do tratamento de dados pessoais, apenas para desconsiderá-los quando da imputação de responsabilidade ao agente, independentemente de terem agido ou não com culpa, de maneira que o regime de responsabilidade objetiva mostra-se incongruente à sistemática da LGPD (GUEDES; MEIRELES, 2019).

Guedes, Tepedino, Terra (2022, p. 293), nesse sentido, aduzem que não se justifica, do ponto de vista lógico, nem do ponto de vista jurídico, a inclusão, pelo legislador, de deveres de cuidado na LGPD se não for para a constituição de um regime

de responsabilidade subjetiva no microsistema legal de proteção de dados, considerando que se a pretensão é de responsabilização dos agentes independentemente de culpa, “seria ocioso criar deveres a serem seguidos, tampouco responsabilizá-los quando tiverem cumprido perfeitamente todos esses deveres”.

Raras são as hipóteses nas quais o legislador estabelece deveres concomitantemente ao estabelecimento de um regime de responsabilidade objetiva, subsistindo, nesses casos, motivação que justifica este proceder:

Na Lei nº 12.846/2013 (Lei Anticorrupção), por exemplo, o legislador trata de responsabilidade civil e também da responsabilidade administrativa com viés sancionador. Nessa lei, o legislador estabelece claramente que a responsabilidade civil é independente de culpa, mas ao mesmo tempo estabelece uma série de deveres. Acontece que, nesse diploma, fica claro que o cumprimento desses deveres será levado em consideração na dosimetria da pena, o que faz sentido para a responsabilidade administrativa sancionadora, mas não para a responsabilidade civil, porque esta não exerce função punitiva, então não cabe falar em pena, mas, sim, em indenização, e indenização se mede pela extensão do dano. (GUEDES, TEPEDINO; TERRA, 2022, p. 293)

A lógica da responsabilidade civil objetiva é, portanto, incompatível ao estabelecimento de deveres de atenção, pois, ao se discutir o cumprimento efetivo de deveres, analisa-se, em última instância, se a conduta do agente foi ou não culposa, de tal modo que, a despeito da omissão legislativa em estabelecer regime de responsabilidade na LGPD, a interpretação sistemática desta culmina na conclusão de que a modalidade de responsabilidade civil adotada no diploma normativo de proteção de dados fora subjetiva (GUEDES; TEPEDINO; TERRA, 2022).

Guedes e Meireles (2019, p. 123) ao procederem também à interpretação sistêmica da norma de proteção de dados, depreendem que a LGPD instituiu um “verdadeiro *standard* de conduta” que conduz à aproximação do regime de responsabilidade subjetiva, fundamentado na noção hodierna de “culpa normativa”, conceito mais objetivado de culpa pelo qual, afastando-se das delimitações da culpa clássica, analisa-se a culpa “a partir da ideia de desvio de conduta, que leva em conta apenas o comportamento exigível diante das especiais circunstâncias do caso concreto” (GUEDES, MEIRELES, 2019).

O conceito, em outros termos, expressa que a investigação da culpa não se presta à análise do direcionamento do *animus* do agente para o “descumprimento da ordem jurídica em termos abstratos, mas, sim, a sua adequação (ou não) ao padrão de

comportamento esperado naquelas circunstâncias concretas.” (GUEDES, MEIRELES, 2019, p.123).

Nesse aspecto, as autoras enunciam que, no âmbito da LGPD, os *standards* - padrões de conduta socialmente esperados - são especificados na própria norma, originando o paradigma direcionador da atuação e dos procedimentos dos agentes de no exercício da atividade de proteção de dados, as quais são compelidos à adoção de medidas de segurança e mesmo preventivas. Concluem Guedes e Meireles (2019, p. 123) que, ocorrendo incidente no curso do tratamento de dados pessoais, a conduta do agente “não será examinada apenas no plano abstrato, mas, sim, em concreto, avaliando-se também o que tais agentes fizeram para evitar o dano e mesmo para conter os seus efeitos e, quando possível, remediá-los”.

O terceiro fundamento presente na LGPD que indica a adoção da modalidade subjetiva de tratamento de dados pessoais, está, segundo Guedes e Meireles (2019) na excludente de responsabilidade prevista no inciso II do art. 43 da norma de proteção de dados, pelo qual os agentes de tratamento só não serão responsabilizados quando provarem “que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados” (BRASIL, 2018).

Dessa forma, em oposição aos incisos I e III do art. 43 da LGPD, que preceituam a exclusão da responsabilidade do agente de tratamento com fundamento no rompimento do nexo de causalidade, o inciso II remete à culpa como fundamento para constatação da responsabilidade do agente de tratamento e do surgimento da conseqüente imputação do dever de indenizar, a qual, quando não constatada, obsta a pretensão ressarcitória do titular de dados pessoais frente à ausência de responsabilidade do agente de tratamento (GUEDES, MEIRELES, 2019).

Assim, da interpretação do inciso II verifica-se que, ainda que manifesto o nexo causal entre a conduta do agente e o dano alegado pelo titular, não haverá responsabilização quando o operador ou controlador de dados se desincumbir do ônus de provar o efetivo cumprimento dos deveres preceituados pela LGPD ao demonstrar que tomou as “medidas de segurança recomendadas (cumprindo programas, políticas internas, procedimentos, mecanismos de supervisão, internos e externos, padrões técnicos etc.)” (GUEDES, MEIRELES, 2019, p, 124), hipótese em que “o agente terá demonstrado que observou o *standard* esperado e, se o incidente ocorreu, não foi em razão de sua conduta culposa.” (GUEDES, MEIRELES, 2019, p, 124).

Ainda tratando das excludentes de responsabilidade preconizadas no art. 43 da LGPD, sobretudo a constante do inciso II, Bioni e Dias (2020, p. 7-8) evidenciam que a norma de proteção de dados não reproduziu as excludentes de responsabilidade previstas no CDC, o que, juntamente, a inserção do princípio da *accountability*, também denominado dever-princípio da responsabilização e prestação de contas, “acompanhada dos chamados relatórios de impacto à proteção de dados pessoais e, de forma mais ampla e geral, o estímulo e reforço à capacidade dos agentes de tratamento de dados pessoais de auto-organização”, além da existência de seção específica determinada à “boas práticas e governança”, reforça, ainda que por elementos indiretos, a adoção, na LGPD, de um regime de responsabilidade civil de natureza subjetiva.

Guedes, Tepedino e Terra (2022, p. 293), por fim, no que concerne às similitudes entre o CDC e a LGPD, potencialmente justificadoras, por analogia, da adoção de um regime jurídico de responsabilização objetivo dos agentes de tratamento de dados na LGPD, tal qual ocorrido com o fornecedor de serviços, fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador nas relações consumeristas, asseveram que, enquanto no CDC há expressa indicação, em ao menos dois art. s, “da natureza objetiva da responsabilidade (arts. 12 e 14 – ambos se valem da expressão “independentemente de culpa”, que deixa clara a opção do legislador pela responsabilidade objetiva)”, inexistente, no âmbito da LGPD, previsão análoga ensejadora da responsabilização objetiva dos agentes de tratamento.

Nesse aspecto, enquanto “o art. 42 da LGPD não faz referência expressa à culpa como elemento da responsabilidade civil, mas também não faz qualquer alusão ao risco como fundamento da responsabilidade objetiva”, problemática encerrada com a interpretação sistemática, supramencionada, pela qual conclui-se que a responsabilidade dos agentes de tratamento de dados é subjetiva (GUEDES; TEPEDINO; TERRA, 2022, p. 293).

Por conseguinte, o inciso II do art. 43, o capítulo VII e o art. 6º, X, ambos da LGPD, assim como o histórico do trâmite legislativo da norma de proteção de dados, refletem que a modalidade de responsabilidade adotado pela LGPD encontra-se intrinsecamente relacionada ao elemento “culpa”, motivação pela qual faz-se mister, segundo os autores referidos ao longo deste subcapítulo, o reconhecimento, no âmbito da LGPD, do regime de responsabilidade civil subjetiva para os agentes de tratamento de dados.

6.3.3 Responsabilidade a partir de regime diferenciado (aversão à culpa, ao risco e concepções dualistas)

Intermediariamente às asserções de responsabilidade objetiva e subjetiva, encontram-se os defensores de que, com a vigência da LGPD, instituiu-se um regime diferenciado de responsabilidade civil, aplicável exclusivamente aos agentes de tratamento de dados pessoais, assentado no “dever geral de segurança” positivado no art. 44 da LGPD, o qual aspira demover o operador e o controlador do tratamento irregular de dados, conceito legal que, segundo Andrade e Magro (2022), assemelha-se à noção consumerista de defeito do produto ou do serviço, e no dever-princípio de responsabilização e prestação de contas preconizado no art. 6º, X, da LGPD, também denominado *accountability*.

Dessa feita, a adoção de regime diferenciado reflete a concepção de que a LGPD, de fato, concebeu novas formas de responsabilidade civil que, afastando-se do risco e da culpa, fundamentos clássicos para imputação do dever de indenizar, destoam essencialmente dos regimes objetivo e subjetivo, positivados no CC/2002 e consagrados na doutrina civilista.

Moraes e Queiroz (2019, p.125-126) sustentam que a LGPD inaugurou sistema especial de responsabilidade civil denominado “proativo” ou “ativo”, caracterizado pela reunião entre os conceitos de “responsabilidade” e de “prestação de contas”, o qual encontra fundamento no art. 6º, X, da LGPD.

Os autores indicam, nesse sentido, que os princípios e fundamentos da LGPD a estruturam no intuito de viabilizar uma análise preventiva de riscos, pautada na adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados, e, inclusive, a eficácia dessas medidas, de forma a mitigar, ao máximo, a incidência de danos causados aos titulares de dados pessoais (MORAES; QUEIROZ, 2019).

Assim, considerando-se a prevenção de danos como valor máximo a ser alcançado, os agentes de tratamento de dados pessoais não devem apenas se preocupar em não descumprir a lei, buscando, de forma diligente, prevenir a ocorrência de danos aos titulares dos dados pessoais ao adotar medidas eficazes e demonstrando-as eficazmente (MORAES; QUEIROZ, 2019).

Incumbe, assim, ao agente de tratamento de dados, “além da simples adequação de contratos-padrão” (ANDRADE, MAGRO, 2022), provar:

i) que avaliou e, se necessário, redesenhou adequadamente o processamento de dados pessoais; ii) que as medidas de segurança implementadas são adequadas e eficazes; iii) que aplica uma política de privacidade interna com obrigações claras, ações concretas vinculadas a cada uma e que foram designados os responsáveis pelo cumprimento; iv) que nomeou um encarregado e que exige esse mesmo cumprimento responsável de seus funcionários e na sua cadeia de terceirização. (MORAES; QUEIROZ, 2019, p. 129)

A responsabilidade civil na LGPD, tal qual decorrida no modelo europeu, no qual se inspira, articula-se em torno de três noções fundamentais e cumulativas: “i) dano, ii) violação da legislação de proteção dos dados por parte do controlador e/ou operador e iii) reparação” (MORAES; QUEIROZ, 2019, p. 126).

O regime proativo de responsabilidade demanda, portanto, que o dano seja decorrente de tratamento irregular de dados pessoais por parte dos agentes de tratamento, seja por violação da LGPD no cumprimento de seus deveres, seja pelo descumprimento do dever legal de segurança dele esperado, para que seja imposta a obrigação de ressarcir a parte lesada (MORAES; QUEIROZ, 2019).

Dresch (2020), por sua vez, postula que a LGPD instituiu regime diferenciado de responsabilidade dos agentes de tratamento de dados denominado “especial”. Nesse aspecto, o autor expressa que a legislação de proteção de dados brasileira adotou critério novo, diverso e especial (DRESCH, 2020).

O autor designa, assim, que o “enunciado normativo chave” (DRESCH, 2020, online) para fundamentar a responsabilização civil na LGPD encontra-se em seu art. 44, o qual preceitua “um dever geral de segurança aos agentes de tratamento de dados, cuja violação geradora de danos a outrem ensejará a responsabilização civil.” (DRESCH, 2020, ONLINE)

Esta violação à norma de proteção de dados, essencial à imputação da responsabilidade civil aos agentes de tratamento de dados, segundo o autor, ocorre “através de ilícitos específicos, caracterizados pela contrariedade a deveres expressamente estabelecidos em lei para o tratamento de dados, mas também por uma forma de ilícito geral, própria desse sistema protetivo” (DRESCH, 2020, ONLINE).

Na LGPD, o ilícito geral expressa a inobservância do dever de segurança, o que ocorre com o tratamento irregular de dados pessoais, conforme preconizado pelo art. 44 da LGPD, a partir da “quebra de legítimas expectativas quanto à segurança dos processos de tratamento de dados” (DRESCH, 2020, ONLINE).

Assim, o “dever geral de segurança” e o “tratamento irregular” são os parâmetros que alicerçam a responsabilidade civil dos agentes de tratamento de dados na LGPD, a qual determina-se a partir de “análise objetiva que parta de padrões - standards - de conduta como critério para se avaliar objetivamente se o tratamento forneceu a segurança esperada ou foi irregular” (DRESCH, 2020, ONLINE).

A partir dessa premissa, conclui que as modalidades tradicionais de responsabilidade civil, seja subjetiva, pautada na culpa, seja objetiva, centrada no risco, são inservíveis à averiguação de responsabilidade dos agentes de tratamento de dados na LGPD, pelo que adotou-se uma nova e especial forma de responsabilidade civil, derivada da responsabilidade objetiva, pautada, contudo, na garantia da segurança no tratamento de dados pessoais.

Armelin e Teixeira (2020, p. 292), por fim, argumentam que, em matéria de responsabilidade civil, é imanente o cotejo analítico entre a LGPD e o CDC, uma vez que “o “espírito” da LGPD está muito alinhado a tal norma de defesa do consumidor. E, sendo uma lei de 1990, já houve tempo razoável para a construção doutrinária acerca das temáticas que cercam a tutela dos consumidores no Brasil.”, de tal modo que as controvérsias surgidas das temáticas concernentes à tutela da proteção de dados em território nacional podem ser potencialmente dirimidas pelos entendimentos doutrinários e jurisprudenciais erigidos em torno do CDC, o que ocorre com a responsabilidade civil.

Disso resulta a conclusão que o fundamento da responsabilidade dos agentes de tratamento de dados na LGPD é a violação à lei, não estando centrada na culpa, o que afasta a incidência da responsabilidade civil subjetiva, nem no risco, o que retira, em regra, do âmbito da LGPD a responsabilidade civil objetiva, de forma que é estabelecido pela norma de proteção de dados pessoais um regime de responsabilidade *sui generis*. (ARMELIN; TEIXEIRA, 2020). Os autores especificam, contudo, que, na hipótese na qual a violação à legislação que ocasiona danos ao titular de dados pessoais ocorre em relação de consumo, subsiste a incidência do CDC no tocante à responsabilidade do controlador e do operador, pelo que devem ser, então, responsabilizados objetivamente.

As correntes de pensamento doutrinariamente denominadas “dualistas” são assim concebidas devido a compreensão de que as disposições normativas da LGPD ensejam a responsabilização dos agentes de tratamento de dados pessoais tanto pela modalidade objetiva, quanto pela modalidade subjetiva, a ser aferida mediante análise casuística, uma vez que são as circunstâncias delineadas nos casos concretos que viabilizam a percepção de qual regime de responsabilidade aplicável ao agente causador de dano.

Bruno (2020), nesse sentido, reputa que o regime de responsabilidade civil adotado na LGPD é, em regra, subjetivo, no qual o elemento culpa deverá ser demonstrado para caracterização do dever de indenizar.

O autor aduz, entretanto, que a LGPD elenca hipóteses específicas, tal qual ocorrido com o tratamento de dados pessoais em relações de consumo e o tratamento de dados pessoais sensíveis, nas quais a responsabilidade do agente é assentada no risco da atividade de tratamento de dados exercida, evidenciando-se que a atividade de tratamento de dados, por si só, não caracteriza-se como atividade cujo risco é inerente à sua própria natureza, motivação pela qual deve subsistir um elemento adicional que, de fato, enquadre o tratamento de dados como atividade risco, o que ocorre, conforme retromencionado, com o tratamento de dados pessoais sensíveis (BRUNO, 2020).

Ferreira (2020) igualmente denota que, em regra, a responsabilidade civil dos agentes de tratamento de dados pelos danos causados é subjetiva, uma vez que o exercício da atividade de dados pessoais não traz, por si só, graves riscos ao titular de dados pessoais.

A incidência do regime de responsabilidade subjetiva na LGPD, no qual a aferição de culpa é elemento central para a responsabilização do causado, segundo o autor, resulta da ausência de previsão expressa do regime de responsabilidade objetiva e da excepcionalidade de aplicação da teoria do risco, posto que, conforme supramencionado, a atividade de tratamento de dados, em regra, não possui risco inerente à sua natureza.

Dessa feita, a responsabilização objetivas dos agentes de tratamento de dados é medida excepcional, a qual se dará em relações de consumo, consoante preconizado pelo art. 45 da LGPD, ou quando há risco criado devido à natureza ou os elementos que circundam a atividade de tratamento, o que ocorre, exemplificativamente, em “incidentes de segurança envolvendo o tratamento de dados de crianças ou grupos vulneráveis, ou de pacientes de um hospital” (FERREIRA, 2020, ONLINE).

Andrade e Magro (2022, p. 225), por sua vez, após cotejo analítico das principais linhas de pensamento acerca da responsabilidade civil dos agentes de tratamento de dados, concluem que, usualmente, o tratamento de dados pessoais não é atividade que possui risco intrínseco, considerando, para chegar à esta conclusão, “a amplitude intencional do conceito de dados e tratamento (art. 5º, I e X, LGPD)”, manifestando, assim, que a responsabilidade imputável aos agentes é subjetiva quando do de tratamento de dados pessoais gerais.

Aos dados sensíveis, contudo, “a LGPD defere proteção obviamente particular e mais cautelosa – dada a própria natureza de seu conjunto, deferindo-se, inclusive, base legal própria e mais restritiva do que à aplicada aos dados gerais” (ANDRADE E MAGRO, 2022, p. 225).

Dessa forma, o tratamento de dados pessoais sensíveis configura-se como atividade de risco, uma vez que incidentes a eles relacionados, pelo conteúdo íntimo e grave que conservam, causam aflições mais severas aos titulares, o que atrai, portanto, a aplicação da cláusula geral de responsabilidade civil objetiva do art. 927, parágrafo único, do CC/2002 (ANDRADE E MAGRO, 2022).

Subsistem, portanto, entendimentos de que a LGPD instituiu regime de responsabilidade civil inédito no Brasil, próprio à sistemática de proteção de dados pessoais, desvinculando-se das modalidades preexistente de responsabilidade civil no ordenamento jurídico pátrio. Opondo-se à esta perspectiva, defende-se a tese de que a LGPD não afastou os regimes de responsabilidade subjetivo e objetivo, pelo que instituiu-se uma sistemática dualística de responsabilidade civil, cuja modalidade aplicável é depreendida diante do fato concreto, de forma que tanto o risco, quanto a culpa mantem-se como parâmetros para fundamentar o dever de indenizar no âmbito da norma de proteção de dados.

7. CONSIDERAÇÕES FINAIS

Na presente pesquisa, pretendeu-se analisar os regimes jurídicos de responsabilidade civil potencialmente aplicáveis aos agentes de tratamento de dados pessoais na LGPD, uma vez que esta legislação, apesar de constituir-se como elemento central de um marco regulatório sistematizador da proteção de dados pessoais no Brasil, foi omissa na estipulação de critérios para assentar modalidade de responsabilidade civil a qual suscetíveis os agentes de tratamento que, no exercício da atividade de tratamento de dados pessoais, em violação aos seus dispositivos normativos, causarem dano à outrem.

Vislumbrou-se, inicialmente, que o estabelecimento de paradigmas pós-modernos, inerentes à Sociedade da Informação, como a noção de que os dados pessoais constituem ativo comercial e reserva de valor fomentadores da econômica digital e de que seu tratamento em massa, invasivo ao titular de dados pessoais, ensejou a emancipação da proteção de dados pessoais do direito à privacidade, instituindo-o enquanto direito autônomo.

Demonstrou-se, nesse aspecto, que a constitucionalização do direito à proteção de dados, pela qual tornou-se direito fundamental, positivado no inciso LXXIX do artigo 5º da CRFB/1988, fora fundamental para assegurar a isonomia entre os titulares de dados pessoais e efetivar a tutela de liberdades individuais em face do contexto hodierno de ampliação de fluxos informacionais e comunicação pautada essencialmente pelos meios digitais, além de fomentar discussões acerca da LGPD, norma infraconstitucional regulamentadora da proteção de dados pessoais, e dos elementos que lhe são correlatos.

Evidenciou-se o processo histórico de consolidação de tutela da proteção de dados no mundo e no Brasil, a partir do qual notou-se a tendência, nos ordenamentos jurídicos dos Estados Unidos da América, de nações europeias e da União Europeia, de conferir à proteção de dados o *status* de ramo jurídico autônomo, iniciada ainda na década de 1970 com o estabelecimento de marcos normativos com o intento de salvaguardar direitos fundamentais do cidadão diante do gradual e ininterrupto desenvolvimento do tratamento informatizado de dados, o qual demandou, no curso do final do século XX e no século XXI, constante adaptação das legislações de proteção de dados.

Identificou-se, contudo, que a tutela da proteção de dados pessoais no Brasil, por fatores sociais, políticos e legislativos, desenvolveu-se tardiamente quando contraposto

às regulamentações do tema nos Estados Unidos e Europa, de tal modo que a estruturação de sistema jurídico de proteção de dados pessoais só instituiu-se em 2018, com a vigência da LGPD, norma própria à tutela da proteção de dados pessoais, o que denota a contemporaneidade das discussões que permeiam o diploma normativo de proteção de dados pessoais.

Elucidaram-se conceitos fundamentais à LGPD, pelos quais explicitou-se seus objetivos, fundamentos e princípios. Demonstrou-se que, a despeito da ausência de distinção conceitual no âmbito legislativo, os termos “dados” e “informação” não são sinônimos, na medida em que este refere-se a algo que principia a cognição, enquanto aquele denota uma informação em potencial, em estágio rudimentar. No mesmo aspecto, mostrou-se que a LGPD não tutela qualquer dado, mas sim dados pessoais, os quais devem ser necessariamente vinculados ou vinculáveis à pessoa natural, o titular de dados pessoais, cerne da existência da LGPD. Detectou-se que ao tratamento de dados pessoais fora conferida concepção abrangente, pela qual compreende a integralidade do ciclo de manuseio de dados pessoais, desde a coleta até a eliminação. Distinguiram-se os agentes de tratamento de dados, apresentando-se as figuras do operador do controlador, e suas respectivas responsabilidades, denotando-se que a LGPD impôs sobre este agente maiores encargos jurídicos, na medida em que responsável pelas principais decisões concernentes ao tratamento de dados, enquanto o operador é encarregado pelo tratamento de dados, mas tem sua ação condicionada às determinações do controlador.

Averiguou-se que a compreensão sobre as dez hipóteses autorizativas preconizadas na LGPD, além de elementar ao entendimento da norma de proteção de dados, é indispensável à discussão sobre responsabilidade civil na LGPD, visto que, em regra, o agente de tratamento de dados pessoais detém o encargo de fundamentar a operação de tratamento a ser realizada a partir de uma base legal, isto é, de uma das hipóteses autorizativas de dados pessoais. Constatou-se, assim, que a ilegitimidade do tratamento de dados pessoais decorrente da falha no proceder em relação à fundamentação da atividade de tratamento de dados em uma base legal acarreta em responsabilização do agente de tratamento.

Afirmou-se a omissão legislativa na seção correspondente à responsabilidade civil dos agentes de tratamento de dados pessoais, a qual define que o controlador e o operador, este quando descumprir as determinações do controlador, respondem solidariamente pelos danos causados a outrem, em violação à legislação de proteção de

dados, no exercício da atividade de tratamento de dados pessoais, sem, contudo, fixar um regime de responsabilidade civil concreto a estes agentes.

Verificou-se, diante do ensejo conferido pela ausência de clareza redacional da LGPD, a inexistência de uniformidade no âmbito doutrinário quanto à definição do regime de responsabilidade civil aplicável aos agentes de tratamento de dados pessoais, cujos entendimentos foram ramificados de forma preponderante em três linhas de pensamento.

Compreendeu-se que, para a primeira corrente, partidária do regime jurídico de responsabilidade objetiva, faz-se necessário o reconhecimento de toda e qualquer atividade de tratamento de dados pessoais como atividade de risco frente ao desenvolvimento tecnológico e científico no âmbito de tratamento de dados pessoais, vez que possui condão de causar prejuízos quantitativamente elevados e qualitativamente graves ao titular de dados pessoais, ensejando a violação do direito fundamental à proteção de dados, o que enquadra o tratamento de dados pessoais na regra do parágrafo único do art. 927 do CC/2002, na qual subsiste o dever de indenizar independentemente de culpa. Ademais, partindo-se de análise sistemática da LGPD pela corrente objetivista, depreendeu-se como pressupostos para incidência de modalidade objetiva de responsabilidade civil o rol de excludentes de responsabilidade preceituado no art. 43 da LGPD, no qual estariam positivadas as únicas hipóteses de afastamento da responsabilização dos agentes de tratamento de dados, não constando a ausência de culpa na conduta dentre elas, além das convergências explícitas entre o regramento de proteção ao consumidor e de proteção de dados pessoais, o que, analogicamente, implica na adoção de regime objetivo de proteção de dados pessoais.

Atestou-se que, para a segunda corrente, defensora do regime jurídico de responsabilidade subjetiva, os elementos primordiais para adoção deste regime residem pautam-se em três pressupostos. Consubstancia-se o primeiro na análise do histórico de tramitação da LGPD, a partir do qual constatou-se que o legislador retirou no curso das discussões sobre o projeto de lei que culminou na promulgação da LGPD expressas previsões normativas referentes à responsabilidade objetiva presentes na versão original. O segundo pressuposto reside na instituição de *standards* de conduta de observância obrigatória pelos agentes de tratamento de dados pessoais, pela qual verificou-se que não há sentido, seja lógico, seja jurídico, para a imputação de deveres de cuidados fundamentos em padrões direcionadores da conduta dos agentes de tratamento de dados apenas para desconsiderá-los em eventual análise de sua responsabilização, de tal forma que a responsabilidade objetiva mostra-se incongruente à sistemática da LGPD. O

terceiro pressuposto exprime que a excludente de responsabilidade preconizada pelo inciso II do art. 43 isenta o agente de responsabilidade quando, ainda que causado incidente no tratamento de dados pessoais, não haverá responsabilização do agente de tratamento de dados pessoais quando não subsistir violação à legislação de proteção de dados, fator que pauta a excludente com fundamento da ausência de culpa.

Aferiu-se que a terceira corrente erige-se a partir de regime de responsabilidade diferenciado, pautado em concepções aversas ao risco e à culpa, ou, ainda, dualistas, considerando-se que a LGPD recepciona tanto o risco e a culpa como fundamentos para constatação da responsabilidade do agente de tratamento de dados.

Verificou-se que parcela da doutrina defensora de regime jurídico diferenciado de responsabilidade civil constitui a tese da “responsabilidade proativa”, pautada na análise preventiva de riscos, enquanto outra parcela institui a modalidade de “responsabilidade especial”, assentado no dever geral de segurança e no tratamento irregular de dados pessoais, enquanto terceira parcela atesta que o pressuposto da responsabilidade na LGPD não está na culpa, nem no risco, mas na violação à lei.

Constatou-se, por fim, que as correntes dualistas pautam-se pela compreensão de que a LGPD comporta tanto o regime de responsabilidade subjetiva, quanto o regime de responsabilidade objetiva, a qual será aferida diante do caso concreto, mediante análise da atividade de tratamento de dados pessoais exercida pelo agente respectivo.

Trata-se de tema ainda não abordado no Superior Tribunal de Justiça, nem no Supremo Tribunal Federal, e que necessitará de profunda discussão não apenas pelos valores e princípios constitucionais em discussão, mas também pelos impactos econômicos, sob a ótica da Análise Econômica do Direito, que a definição do regime de responsabilidade civil aplicável aos agentes de tratamento de dados pessoais ocasionará no mercado.

REFERÊNCIAS

ALMEIDA, Juliana Evangelista de; LUGATI; Lys Nunes. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, [S. l.], v. 12, n. 02, p. 01–33, 2020. DOI: 10.32361/2020120210597. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/10597>. Acesso em: 27 nov. 2022.

ARMELIN, Ruth Maria Guerreiro da Fonseca; TEIXEIRA, Tarcisio. Responsabilidade e Ressarcimento de Danos por Violação às Regras Previstas na LGPD: um Cotejamento com o CDC. *In*. LIMA, Cíntia Rosa Pereira de (coord). **Comentários à lei geral de proteção de dados**. São Paulo: Almedina, 2020.

ANDRADE, Landolfo; MAGRO, Américo Ribeiro. **Manual de Direito Digital**. 2. ed. rev., atual e ampl. Salvador: JusPodivm, 2022.

ANPD. AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 20 set. 2022.

BIONI, Bruno.; 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**, v. 9, n. 3, p. 1-23, 22 dez. 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.

BORGES, Natasha Malara. *et al.* Developing a Global Data Breach Database and the Challenges Encountered. **Journal of Data and Information Quality (JDIQ)**, [S.l.]. v. 13. p. 1, 2021. Disponível em: <https://dl.acm.org/doi/abs/10.1145/3439873>. Acesso em: 10 abr. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 abr. 2022.

_____. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 10 abr. 2022.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2022.

BRUNO, Marcos Gomes da Silva. Dos Agentes de Tratamento de Dados Pessoais. *In.* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD: Lei Geral de Proteção de Dados comentada.** 2. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2020.

CHAVES, Suellen. Proteção de dados como direito fundamental é marco histórico do respeito à privacidade. **Migalhas.** [S.l.], 15. fev. 2022. Disponível em: <https://www.migalhas.com.br/depeso/359688/protecao-de-dados-como-direito-fundamental>. Acesso em: 12 ago. 2022.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais: comentada.** 2. ed. São Paulo: Revista dos Tribunais, 2019.

DIVINO, Sthéfano Bruno Santos; LIMA, Taisa Maria Macena de. RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA. **Revista Em Tempo,** [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3229>. Acesso em: 18 out. 2022. doi: <https://doi.org/10.26729/et.v20i1.3229>.

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

_____. PANORAMA HISTÓRICO DA PROTEÇÃO DE DADOS PESSOAIS. *In.* DONEDA, Danilo *et al* (coord). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

DRESCH, Rafael de Freitas Valle. A especial responsabilidade civil na Lei Geral de Proteção de Dados. **Migalhas.** [S.l.], 02 jul. 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados>. Acesso em: 12 out. 2022.

FERREIRA, Diogo Ramos. Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva?. **JOTA.** [S.l.], 21 nov. 2019. Disponível em:

<https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019>. Acesso em: 12 abr. 2022.

GONDIM, Glenda Gonçalves. A responsabilidade civil no uso indevido dos dados pessoais. **Revista IBERC**, v. 4, n. 1, p. 19-34. 09 mar. 2021

GUEDES, Gisela Sampaio da Cruz; VENCELAU MEIRELES, Rose Melo. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2019.p. 275-303.

GUEDES, Gisela Sampaio da Cruz; TEPEDINO, Gustavo; Terra, Aline de Miranda Valverde. **Fundamentos do direito civil: responsabilidade civil**. 3. ed. Rio de Janeiro: Forense, 2022.

LIMA, Caio César Carvalho. Do Tratamento de Dados Pessoais. In. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD: Lei Geral de Proteção de Dados comentada**. 2.ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2020.

LIMA, Cíntia Rosa Pereira de. Agentes de Tratamento de Dados Pessoais (Controlador, Operador e Encarregado pelo Tratamento de Dados Pessoais). In. LIMA, Cíntia Rosa Pereira de (coord). **Comentários à lei geral de proteção de dados**. São Paulo: Almedina, 2020.

_____.; RAMIRO, Livia Froner Moreno. Direitos do Titular dos Dados Pessoais. In. LIMA, Cíntia Rosa Pereira de (coord). **Comentários à lei geral de proteção de dados**. São Paulo: Almedina, 2020.

MAIMONE, Flávio Henrique Caetano de Paula. **Responsabilidade Civil na LGPD: efetividade na proteção de dados pessoais**. Indaiatuba: Foco, 2022.

MARTICAST: Mudanças na LGPD em tempo de Coronavírus. [Locução de]: Patrícia Mendlowicz e Felipe Ribeiro. [S.l.]: Martinelli Advogados, 30 abr. 2020. Podcast. Disponível em: <https://open.spotify.com/episode/6ufW08HyIOmiHqMEjTw7Q6>. Acesso em: 02 ago. 2022.

MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?. **Migalhas**. [S.l.], 30 jun. 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-dedados-pessoais-culpa-ou-risco>. Acesso em: 12 abr. 2022.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa. In: Proteção de dados pessoais: Privacidade versus avanço tecnológico. **Cadernos Adenauer**. Rio de Janeiro, ano XX, p. 113-135, n. 3, 2019.

NOVELINO, Marcelo. **Curso de direito constitucional**. 11. ed. Salvador: JusPodivm, 2016.

PEREIRA, Caio Mário da Silva; TEPEDINO, Gustavo. **Responsabilidade Civil**. 12. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2018.

PESQUISA MOSTRA QUE 82,7% DOS DOMICÍLIOS BRASILEIROS TÊM ACESSO À INTERNET. Gov.br, 2021. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet>. Acesso em: 07 abr. 2022.

QUINTILIANO. Leonardo David. A proteção de dados pessoais e as competências dos entes federativos - Análise dos efeitos da PEC 17/2019. **Migalhas**. [S.l.], 26 nov. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355602/a-protecao-de-dados-pessoais-e-as-competencias-dos-entes-federativos>. Acesso em: 11 abr. 2022.

QUINTILIANO. Leonardo David. Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD). Instituto Avançado de Proteção de Dados. [S.l.], 17. mar. 2021. Disponível em: <https://iapd.org.br/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 12. ago. 2022.

SOLER, Fernanda Galera. **Proteção de dados: reflexões práticas e rápidas sobre a LGPD**. [S.l.]: Editora Saraiva, 2022.

TARTUCE, Flávio. **Manual de direito civil**: volume único. 11. ed. Rio de Janeiro: Método, 2021.

TEFFÉ; Chiara Spadaccini de. Viola, Mario. TRATAMENTO DE DADOS PESSOAIS NA LGPD: ESTUDO SOBRE AS BASES LEGAIS DOS ARTIGOS 7.º E 11. In. DONEDA, Danilo *et al* (coord). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

VAINZOF, Rony. DISPOSIÇÕES PRELIMINARES. *In.* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2020.