CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE À LUZ DO DIREITO COMPARADO E DA TEORIA DO DIÁLOGO DE FONTES

Amanda Alves das Neves Santos

Presidente Prudente/SP
2022

CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE À LUZ DO DIREITO COMPARADO E DA TEORIA DO DIÁLOGO DE FONTES

Amanda Alves das Neves Santos

Monografia apresentada como requisito parcial de conclusão do curso e obtenção do grau de Bacharel em Direito, sob a orientação das Professoras Ana Laura Teixeira Martelli Theodoro e Carla Roberta Ferreira Destro

Presidente Prudente/SP
2022

RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE À LUZ DO DIREITO COMPARADO E DA TEORIA DO DIÁLOGO DE FONTES

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Direito.

_____
Carla Roberta Ferreira Destro

_____
Gilberto Notário Ligero

_____
João Pedro Brigatto Wehbe

Presidente Prudente, 22 de novembro de 2022.

Não fui eu que ordenei a você? Seja forte e corajoso! Não se apavore, nem desanime, pois o Senhor, o seu Deus, estará com você por onde você andar.

Josué 1:9 - Bíblia Sagrada

AGRADECIMENTOS

Primeiramente, agradeço a Deus por guiar meus passos ao longo desta graduação, especialmente na elaboração do presente trabalho, me concedendo energias para alcançar os propósitos almejados, apesar das adversidades advindas.

À minha mãe, Cristina, a quem remeto minha imensurável admiração e amor incondicional. Agradeço por ser meu sustentáculo ao longo da vida, me apoiando em meus sonhos, e nunca medindo esforços para me propiciar o melhor estudo.

Ao meu pai, Nilmo (*in memoriam*), por todos os ensinamentos me oportunizados durante os poucos anos que o tive em meu lado.

Ao meu avô, Osvaldo, por todo amor, carinho e preocupação para comigo.

Ao meu namorado, Fernando, que me acompanha desde o início dessa graduação, ofereço meus agradecimentos pelo amor, companheirismo, compreensão e incentivo.

Ao meu padrasto, Roberto, à minha avó do coração, Joana, e à minha grande apoiadora nesta vida, Dete, por sempre se fazerem presentes, me apoiando em cada passo do caminho por mim percorrido.

Ao meu pequeno Miguel, por trazer tanta alegria e luz à minha vida.

Agradeço à professora Ana Laura Martelli pela orientação nessa Monografia, e conhecimentos jurídicos transmitidos. Sem sombra de dúvidas, uma das grandes responsáveis pelo meu crescimento ao longo deste ano.

À professora Carla Destro, minha segunda orientadora, a quem agradeço imensuravelmente por toda a orientação e ensinamentos.

Aos demais professores que me acompanharam ao longo desta graduação, por toda a aprendizagem.

Agradeço aos profissionais com quem tive a feliz oportunidade de conviver durante esta graduação, doutores Eduardo Bielsa, Adriana Ligero, Gilberto Ligero, Mariah Zambelli e João Pedro Wehbe. A vocês, meu muito obrigada por todos os conhecimentos jurídicos transmitidos, que, de certo, estão aplicados no presente trabalho.

Por final, enfatizo meus agradecimentos aos meus amigos que me apoiaram nessa jornada.

RESUMO

O presente trabalho, através da adoção do método indutivo comparativo, possui como intuito realizar uma análise quanto aos principais contornos jurídicos da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), com enfoque na Responsabilidade Civil prevista em aludida lei. Após destacar seus precedentes jurídicos, bem como suas principais previsões legais, realiza-se uma análise da LGPD à luz do direito comparado europeu, especialmente sob a óptica do Regulamento Europeu de Proteção de Dados, e de julgados do Tribunal de Justiça da União Europeia voltados a esta temática. Na sequência, adentra-se ao núcleo desta pesquisa, realizando-se uma análise jurídica dos dispositivos que tratam do instituto da Responsabilidade Civil na lei de proteção de dados, a fim de se fixar seus pressupostos, considerando as especificidades do regime jurídico instituído pela LGPD, e concluindo-se pela configuração de uma responsabilidade subjetiva fundada na culpa presumida e no dever de segurança dos agentes de tratamento de dados pessoais. Por derradeiro, efetiva-se um estudo da responsabilidade civil pelo tratamento de dados pessoais no âmbito do comércio eletrônico, através da interpretação sistemática entre LGPD e CDC, diferenciando o regime geral de responsabilidade civil previsto na lei de proteção de dados, e as particularidades de referida responsabilidade quando consubstanciada no âmbito consumerista, o qual, diversamente do primeiro, é regido por uma responsabilidade objetiva.

Palavras-chave: LGPD. Dados Pessoais. Responsabilidade Civil. Comércio Eletrônico. Sociedade Informacional. Direito Comparado.

ABSTRACT

The present work, through the adoption of the comparative inductive method, aims to carry out an analysis of the main legal contours of the General Data Protection Law (Law nº 13.709/2018). After highlighting its legal precedents, as well as its main legal provisions, an analysis of the LGPD is carried out in the light of European comparative law, especially from the perspective of the European Data Protection Regulation, and judgments of the Court of Justice of the European Union aimed at to this theme. Subsequently, the core of this research is entered, carrying out a legal analysis of the provisions that deal with the Institute of Civil Liability in the data protection law, in order to establish its assumptions, considering the specificities of the legal regime established by the LGPD. , and concluding with the configuration of a subjective responsibility based on the presumed fault and on the security duty of the personal data processing agents. Finally, a study of civil liability for the processing of personal data in the scope of electronic commerce is carried out, through the systematic interpretation between LGPD and CDC, differentiating the general regime of civil liability provided for in the data protection law, and the particularities of said liability when embodied in the consumerist scope, which, unlike the first, is governed by strict liability.

Keywords: LGPD. Personal Data. Civil Responsability. E- commerce. Informational Society. Comparative Law.

LISTA DE SIGLAS E ABREVIATURAS

ANPD – Agência Nacional de Proteção de Dados

CC- Código Civil – Lei nº 10.406/2002

CDC- Código de Defesa do Consumidor – Lei nº 8.078/1990

LGPD- Lei Geral de Proteção de Dados – Lei nº 13.709/2018

GDPR- *General Data Protection Regulation - Regulation* (EU) 2016/679

SUMÁRIO

1 INTRODUÇÃO.....10

2 LGPD: UM MARCO REGULATÓRIO NO TRATAMENTO DE DADOS PESSOAIS.....12
2.1. O Cenário Histórico e Jurídico Interno Antecedente ao Advento da LGPD e os Impactos Trazidos pela Legislação 12
2.2. Os Principais Contornos Jurídicos da LGPD 20
2.3. Uma Análise Comparativa entre Marcos Regulatórios: LGPD X GDPR 32
2.4. Uma Análise da Jurisprudência do Tribunal de Justiça da União Europeia sob o Viés da Proteção de Dados Pessoais 39

3 RESPONSABILIDADE CIVIL NA LGPD NO ÂMBITO PRIVADO E OS IMPACTOS DA LEGISLAÇÃO NAS RELAÇÕES CONSUMERISTAS.....45
3.1. Análise Legal da Responsabilidade Civil na LGPD no Âmbito das Relações Privada 49
3.2. Pressupostos da Responsabilidade Civil na LGPD 58
3.2.1. Ato ilícito 59
3.2.2. Do elemento dano.....61
3.2.3. Do nexo de causalidade.....70
3.2.4. Do fundamento da responsabilidade civil na LGPD: culpa ou risco?.....72
3.2.4.1. Natureza objetiva da responsabilidade civil na LGPD.....74
3.2.4.2. Natureza subjetiva da responsabilidade civil na LGPD.....77
3.2.4.3. Natureza proativa da responsabilidade na LGPD.....81
3.2.4.4. LGPD: um sistema de culpa presumida embasado no dever de segurança e na prestação de contas.....82

4 RESPONSABILIDADE CIVIL NO COMÉRCIO ELETRÔNICO NA PESPECTIVA DA PROTEÇÃO DE DADOS PESSOAIS 94
4.1 Os Efeitos da Pandemia no E-Commerce e a Intensificação da Vulnerabilidade do Consumidor.....94
4.2. O Impacto da LGPD no Comércio Eletrônico.....99
4.3. Responsabilidade Civil no Comércio Eletrônico à Luz da Legislação de Proteção de Dados: uma Interpretação Sistemática entre as Normas.....103

5 CONCLUSÃO.....110

REFERÊNCIAS.....115

1 INTRODUÇÃO

Nos últimos anos, temática que tem ganhado relevantes certames argumentativos entre os operadores do direito diz respeito ao elemento regulatório do tratamento de dados pessoais no Brasil: a Lei nº 13.709/2018, popularmente conhecida como LGPD (Lei Geral de Proteção de Dados).

A lei sancionada em 2018,entrou em vigência parcial apenas em setembro 2020, regulando o tratamento de dados pessoais no Brasil, e em integral vigência em agosto de 2021, com a possibilidade de aplicação efetiva das penalidades administrativas previstas.

A LGPD surge como necessidade da pós-modernidade: em uma sociedade informacional que lida constantemente com dados em massa, fez-se imperioso a imposição de limites em relação ao tratamento desses, de modo a evitar abusos por parte dos chamados agentes de tratamento.

Destaca-se, contudo, que o marco regulatório brasileiro materializou como decorrência de um lento e gradual avanço legislativo que teve como escopo adequar o ordenamento jurídico brasileiro aos direitos e garantias fundamentais constitucionalmente garantidos, na perspectiva da sociedade informacional do século XXI, efetivando-se na legislação o direito à autodeterminação informativa.

Nesse sentido, a Lei nº 13.709/2018 inaugurou no sistema normativo brasileiro a regulação sistematizada do processo de tratamento de dados pessoais, desde a coleta ao descarte desses.

Como meio de efetivação de suas disposições legais, a LGPD regulou a responsabilidade civil dos agentes de tratamento pelo descumprimento da legislação, tal como elencou um rol de sanções administrativas a serem aplicadas em referidos casos por uma autoridade fiscalizadora, a Autoridade Nacional de Proteção de Dados (ANPD) a qual possui uma estrutura destinada a zelar pela efetivação da lei.

Não obstante à regulação da responsabilidade civil pela LGPD, seu texto normativo, claramente inspirado no Regulamento Europeu de Proteção de Dados Pessoais, não obteve o êxito em esgotar a temática no âmbito da proteção de dados, deixando lacunas a serem debatidas em sede doutrinária e jurisprudencial.

Desse modo, o presente tem como objetivo analisar um dos meios de efetivação do standard de condutas na legislação: a responsabilidade civil dos agentes de tratamento de dados pessoais no âmbito privado.

Para tanto, parte-se de uma análise de julgados do Tribunal de Justiça da União Europeia no âmbito da proteção de dados pessoais, que possui uma antiga e complexa estruturação em relação ao sistema jurídico pátrio em aludida temática, extraindo-se vetores interpretativos a serem considerados na aplicação da LGPD.

Assim, através do método indutivo-comparativo, objetiva se realizar uma análise jurídica dos dispositivos que tratam da responsabilidade civil na LGPD, interpretando-os a partir da Teoria do Diálogo de Fontes, e dos vetores acima citados, no intuito de se estabelecer os pressupostos caracterizadores da responsabilização civil, com enfoque nas divergências doutrinárias existentes quanto ao fundamento dessa em aludida lei. Ademais, será estudado o panorama jurídico do dano moral na legislação de proteção de dados.

Outrossim, sem ignorar os diversos setores afetados pela publicação da LGPD, pretende se efetivar um estudo no tocante ao impacto da lei sobre o e-commerce. Levando em conta o tratamento constante de dados pessoais nessa modalidade de comércio, tornou-se imprescindível que os fornecedores eletrônicos se adequassem integralmente à lei citada, o que ganhou maior repercussão diante do aumento significativo do comércio eletrônico durante a pandemia.

Assim, para o encerramento deste estudo, efetiva-se uma análise sistemática da responsabilidade civil pela violação à LGPD no âmbito do comércio eletrônico, através de um diálogo normativo entre aludida lei e o Código de Defesa do Consumidor, no intuito de se estabelecer as principais peculiaridades em relação às regras aplicáveis neste regime jurídico específico, em relação àquelas previstas estritamente no marco regulatório de proteção de dados.

De se enfatizar, desde o princípio, que a presente pesquisa não teve como objetivo esgotar a análise das matérias ora estudadas, mas sim trazer à lume os principais contornos jurídicos atinentes à LGPD, precipuamente no que concerne aos desdobramentos jurídicos das previsões legais relativas à responsabilidade civil dos agentes de tratamento no âmbito privado.

2 LGPD: UM MARCO REGULATÓRIO NO TRATAMENTO DE DADOS PESSOAIS

Fruto da sociedade informacional, a LGPD configurou-se como marco regulatório do tratamento de dados pessoais no ordenamento jurídico brasileiro. Embora já houvesse no sistema normativo pátrio previsões isoladas quanto à proteção de dados pessoais, nenhuma dessas aproximou-se de uma regulação sistematizada como se concretizou com a lei publicada em 2018.

Ressalta-se que a publicação de uma nova lei sempre será resultado de uma necessidade existente na sociedade, até então não suprida pela legislação vigente. Essa necessidade decorre da valoração de um fato, ensejando a regulação formal para tanto, conforme Teoria Tridimensional concebida por Miguel Reale (2013, p. 493), consubstanciada no tríplice fato, valor e norma.

No caso da LGPD, a partir das circunstâncias fáticas impostas pela sociedade informacional (fato), e orientando-se pelos preceitos constitucionais, observou-se a importância da consolidação da dignidade da pessoa humana na perspectiva do titular de dados pessoais (valor), culminando, por consequência, na publicação da Lei nº 13.709/2018 (norma).

Nessa sistemática, antes de adentrar ao estudo dos principais contornos jurídicos da Lei Geral de Proteção de Dados, imprescindível se mostra a análise de seus antecedentes históricos - jurídicos, isto é, as circunstâncias fáticas que corroboraram para a publicação da lei, bem como o avanço legislativo gradual e isolado sobre o tema, a fim de estabelecer uma interpretação teleológica de seus enunciados legais.

Aludido estudo possibilitará inferir os valores/finalidades que nortearam o legislador quando da elaboração da redação da lei de proteção de dados, fixando vetores para uma eficaz interpretação de dispositivos legais nela presentes.

2.1. O Cenário Histórico e Jurídico Interno Antecedente ao Advento da LGPD e os Impactos Trazidos pela Legislação

No intuito de realizar uma análise histórica/jurídica sobre os precedentes da LGPD no ordenamento jurídico brasileiro, comporta consignar, inicialmente, que a discussão sobre o tratamento de dados pessoais emana dos próprios direitos da personalidade elencados na Constituição Federal de 1988,

sobretudo no que tange ao direito à privacidade, consagrado no artigo 5º, inciso XII da Carta Magna.

A questão relativa à proteção de dados pessoais também se encontra disciplinada indiretamente no inciso XII, artigo 5º, da Constituição Federal, o qual preconiza a inviolabilidade do sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas (BRASIL, 1988).

Nessa perspectiva, não se pode ignorar o reconhecimento da necessidade de proteção de dados no âmbito público pelo legislador constituinte quando esse trouxe previsão do Habeas Data, como remédio constitucional apto para “assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público” tal como “para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo” (BRASIL, 1988).

Ressalta-se, contudo, que o remédio constitucional supracitado, apesar de ter capacidade, à princípio, de configurar-se “[...] como um verdadeiro habeas corpus na sociedade moderna tecnológica tendo em vista que a liberdade de locomoção pode ser violada na dimensão eletrônica [...]” (ELER, p. 190), não foi bastante para solucionar a conjuntura fática decorrente do avanço do tratamento de dados na sociedade informacional (DONEDA, 2020, p. 31).

Isto porque, ao disciplinar de forma genérica o direito ao sigilo de dados, o legislador constituinte brasileiro não era capaz de prognosticar os imensuráveis avanços tecnológicos e informacionais experimentados pela sociedade global nas décadas seguintes, sobretudo em face da revolução proporcionada pela expansão mundial da *internet*, e consequente estruturação de uma economia digital, a qual estava dando seus primeiros passos, no âmbito nacional, quando da promulgação da Carta Magna em 1988.

A cultura da informação proporcionada pela economia globalizada, associada ao processo de burocratização dos setores público e privado, ocasionou um constante processamento de informações e fluxo de dados (MENDES, 2014, p. 33), mormente individuais, e, por consequência o armazenamento em massa de mencionados dados pelos que, hodiernamente, são denominados pela LGPD como agentes de tratamento.

O cenário normativo internacional não era mais capaz de acompanhar a celeridade dos avanços tecnológicos. Neste ínterim, iniciou-se uma intensa

produção legislativa no âmbito global objetivando regular as consequências advindas da economia digital, inclusive, o tratamento de dados pessoais, ainda que de modo não extensivo. De acordo com Patrícia Peck Pinheiro (2021, p.10):

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

No âmbito jurídico interno, o avanço legislativo, em que pese gradual e moroso, também se figurou presente, a fim de promover a adequação do cenário normativo à sociedade informacional.

Pouco após a promulgação da Constituição Federal de 1988, sucedeu-se a entrada em vigor do Código de Defesa do Consumidor (Lei nº 8.078/1990). Em mencionada legislação, a temática de proteção de dados foi novamente apresentada pelo legislador, de modo discreto, ao tratar dos bancos de dados e cadastro, em seu artigo 43.

Ademais, a legislação em comento fixou princípios norteadores também aplicáveis à operação de tratamento de dados, e, ao estabelecer o Sistema Nacional de Defesa do Consumidor, abarcou um número relevante de demandas relativas a dados pessoais, visto que, muitas vezes, o tratamento desses ocorre justamente no âmbito consumerista (DONEDA, 2020, p. 33), como será oportunamente destacado na presente pesquisa.

Sem embargo, o avanço normativo reconhecendo a existência da necessidade de proteção de um banco de dados foi acompanhado de um período de longa inércia legislativa sobre o tema no âmbito nacional.

Após 21 (vinte e um) anos da entrada em vigor do Código de Defesa do Consumidor, o legislador voltou a abordar a temática que circunda a proteção de dados, com a Lei de Cadastro Positivo (Lei nº 12.414/2011), responsável por disciplinar “[...] a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.” (BRASIL, 2011)

Inclusive, em aludido diploma normativo, é possível notar elementos de similitude com a lei de proteção de dados, sobretudo na regulação das “informações

sensíveis", e nos vetores interpretativos da legislação, também presentes na LGPD, como os princípios da finalidade, transparência, minimização e segurança (DONEDA, 2020, p. 34)

No mesmo ano, foi sancionada a Lei de Acesso à informação (Lei nº 12.527/2011), que, nos termos de seu artigo 1º, é responsável por regular o dever do Estado em garantir o acesso às informações públicas pelos cidadãos, direito previsto no artigo 5º, inciso XXXIII da Carta Magna (BRASIL, 2011).

O diploma legal sob comento destinou seu Capítulo IV para tratar das restrições relativas ao direito de acesso à informação, prevendo em seu artigo 31 o *modus operandi* desejado para o tratamento das informações pessoais abordadas pela legislação, o qual deve ser norteado pela transparência, tal como pela observância de direitos constitucionalmente garantidos, como o respeito à intimidade, privacidade, honra, imagem, liberdade e garantias individuais (BRASIL, 2011).

Em mais uma tentativa de adequar o cenário legislativo à realidade fática que se apresentava, foi promulgado em 2014 o Marco Civil da Internet (Lei nº 12.965/14), visando regulamentar o uso da Internet no Brasil, fixando princípios, bem como garantias, direitos e deveres aos usuários da rede (BRASIL, 2014).

De acordo com Doneda (2020, p. 34), ao trazer ao Ordenamento Jurídico um regime de direitos aplicáveis aos usuários da rede de internet, o Marco Civil teria implementado sistemática normativa de direitos e procedimentos intrínsecos aos dados pessoais, apesar de não ser o objetivo fundamental da lei. Doneda ainda doutrina que, ao elencar em seu art. 3º, inciso III, como princípio vetor do uso da internet no Brasil a "proteção de dados pessoais", a qual deveria ser regulamentada por lei própria, o Marco Civil já estaria acenando para uma legislação ulterior especialmente destinada ao tratamento de dados pessoais.

Enquanto o legislador disciplinava de forma genérica e vagarosa a proteção de dados pessoais, a sociedade informacional e a economia digital progrediam em ritmo como nunca antes visto, tornando a regulação legal sobre a temática cada vez mais obsoleta.

Nesse ínterim, como lecionam Godinho, Neto e Tôledo (2020, p. 03), o armazenamento de dados, que teve início com um cartão perfurado responsável por registrar informações, através da repetição de padrões, criando as memórias de computador, progrediu de maneira inimaginável, a fim de se ter o denominado

“armazenamento de nuvem”, com capacidade de englobar um número imensurável de informações sobre bilhões de indivíduos.

Outrossim, os denominados dados pessoais passaram a adquirir valor político e econômico em face da sociedade informacional, tendo em vista que o importe dos dados obtidos não se sedimenta apenas no poder de armazenamento de uma vultuosa quantidade de informações, mas também na potencial construção de um perfil informativo dos cidadãos a partir de referidos dados (MENDES, 2014, p. 33).

Como apregoa Gabrielle Sarlete (2020, p.21), diante desse cenário de coleta massiva de dados com finalidades políticas e econômicas, fazia-se imperioso a específica regulamentação do tratamento de dados pessoais e sensíveis, os quais compõem conjuntamente o perfil digital de um indivíduo, configurando a proteção de dados pessoais como a proteção da própria pessoa humana, sobretudo na perspectiva do livre desenvolvimento de sua personalidade e de seu direito à autodeterminação informacional.

Por conseguinte, a regulação do tratamento de dados pessoais sustentava-se na necessidade de adequação da coleta massiva de dados na sociedade informacional ao ordenamento jurídico constitucional dos Estados democráticos, os quais eram regidos, precipuamente, pelo princípio da dignidade da pessoa humana e pelos direitos da personalidade, entre eles, o direito à privacidade.

Repisa-se que este último direito, em face do aparato histórico-jurídico exposto, tem o condão de desdobrar-se em um novo: o direito a autodeterminação informativa, consubstanciado como: “[...] o direito de manter o controle sobre as próprias informações; o direito de escolher aquilo que será revelado; direito ao esquecimento, em resumo, o direito de determinar a maneira de construir a própria esfera particular.” (ELER, 2016, p. 191)

A imprescindibilidade de uma lei própria destinada a tratar especificamente de dados pessoais tornava-se ainda mais veemente diante de diversos exemplos no cenário internacional circundando o vazamento de dados pessoais. Como exemplifica Eler (2016, p. 187):

> Casos recentes como o furto de informações pessoais, incluindo nomes, endereços e dados do cartão de crédito, de milhões de usuários do PlayStation Network (serviço oferecido pela Sony) em 2011 e o furto de dados de países como Estados Unidos, China e Japão pelo grupo de hackers TeamGhostShell em 2012 demonstram que aos cidadão deve ser conferido o

> direito de exercer um controle direto sobre aqueles sujeitos cujas informações fornecidas permitem a expansão de uma nova forma de poder – o poder fundado na informação.

Não obstante o cenário jurídico internacional, inclusive o brasileiro, já vir transparecendo há anos a necessidade de uma legislação específica voltada à proteção de dados pessoais, a conjuntura fática exposta mostrava não poder ser mais adiável.

Neste diapasão, foi aprovado em 27 de abril de 2016 o Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR). Como menciona Pinheiro (2021, p. 10), o marco regulatório visou disciplinar o direito a proteção de dados pessoais de pessoas físicas, sob o viés do adequado tratamento e livre circulação de referidos dados ("*free data flow*").

Ainda de acordo com Pinheiro, a exemplo do que ocorreu ulteriormente na legislação brasileira, o regulamento europeu trouxe previsão de dois anos para adequação às suas disposições, prazo que após decorrido, culminaria na aplicação das penalidades previstas pelo tratamento inadequado de dados

Embora não fosse a primeira legislação a normalizar os dados pessoais, tema o qual já era escopo de discussão em diversos outros países há décadas, já estando presente discretamente em outras legislações e diretivas no âmbito da União Europeia, o regulamento europeu em discussão materializou-se como pioneiro na regulação sistematizada do tema, de forma a adequar-se aos direitos e garantias previstos nas cartas legislativas dos Estados Democráticos de Direito, em face da economia digital do século XXI.

Considerando a economia globalizada que se faz presente, a GDPR, não bastando o impacto jurídico ocasionado nos países que compõem o bloco econômico europeu, ensejou um "efeito dominó" no panorama legislativo estrangeiro. Como leciona Patricia Peck Pinheiro sobre o Regulamento Europeu (2021, p. 10):

> Este, por sua vez, ocasionou um "efeito dominó", visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar.

Um dos países diretamente atingidos pelo “efeito dominó” aludido foi o Brasil. Em que pese anteprojetos da LGPD virem tramitando há anos no Congresso Nacional, a GDPR trouxe um impacto direto com sua publicação, tanto que, em diversos trechos da lei em comento, é possível notar evidentes semelhanças legislativas com o regulamento europeu.

Diante desse contexto econômico e jurídico, em 14 de agosto de 2018 foi sancionada pelo Presidente da República a Lei nº 13.709, comumente conhecida como Lei Geral de Proteção de Dados (LGPD).

Respectiva lei, não obstante regular o tratamento de dados pessoais nos meios físico e digital, configurou-se como resultado do avanço tecnológico, frente o qual se mostrou imperioso a regulação do tema no âmbito interno, adequando o tratamento de dados pessoais em massa, constantemente presente na sociedade informacional, aos direitos e garantias fundamentais elencados na Constituição Federal de 1988. Como elucidam Frazão, Tepedino e Oliva (2019, p. 677 e 678):

> [...] Com o acelerado desenvolvimento tecnológico e a consolidação de espaços públicos virtuais, a gestão de informação sobre si próprio tornou-se expressão fundamental do indivíduo. Por conseguinte, revela-se impossível cogitar de proteção integral à liberdade, à privacidade e ao desenvolvimento da pessoa natural sem que se lhe garanta eficaz defesa e controle de seus próprios dados – o que se traduz na expressão autodeterminação informativa. [...]

Sublinha-se que desde sua publicação em agosto de 2018, a Lei Geral de Proteção de Dados já sofreu alterações legislativas, bem como teve seu período de vacância, precipuamente previsto, prorrogado.

De acordo com Doneda (2020, p. 36), a Lei nº 13.853/2019 (inicialmente MP 869/2018) trouxe previsão quanto à Autoridade Nacional de Proteção de Dados (ANPD) e ao Conselho Nacional de Proteção de Dados e Privacidade, órgãos os quais haviam sido objetos de veto na redação da legislação submetida à sanção presidencial.

Ainda de acordo com o especialista em proteção de dados, aludida lei também foi responsável por trazer alterações quanto à extensão do período de vacância legislativa, que passaria de maio para agosto de 2020, excecionando-se a aplicação imediata quanto às previsões referentes aos órgãos criados pela mesma lei, retro elencados (DONEDA, 2020, p. 36).

Como preconiza Oliveira (2021, p. 07), em que pese ter entrado em vigor em 18 de setembro de 2020, as disposições gerais da lei, e consequente responsabilização civil dos agentes de tratamento, o legislador, através da Lei nº 14.010/2020, ampliou a vacância legislativa das previsões quanto à aplicação das sanções administrativas até agosto de 2021.

A extensão do período de vigência da legislação tinha notório embasamento: os impactos de cunho jurídico, social e econômico que a legislação traria à sociedade informacional, diante das sanções administrativas e responsabilização civil prevista pelo tratamento inadequado de dados.

Os impactos trazidos pela legislação fundam-se na abrangência e alcance de seus efeitos sobre a sociedade em geral. Conforme elucidações de Renato Oliveira (2021, p. 07):

> A Lei 13.709, de 14 de agosto de 2018, mas conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), provocou um dos maiores reboliços jurídicos que se tem notícia nos últimos anos. Não sem motivo: a LGPD é uma lei que não encontra fronteiras em segmentos de negócios, tipos societários, natureza da pessoa jurídica ou qualquer coisa desse tipo. Para sua aplicação basta termos diante de nós dados pessoais, simples assim. E de tão simples, o problema é comum, pois empregar uma única pessoa, ter pessoas físicas como clientes ou ser uma pessoa jurídica já torna a empresa ou órgão público um controlador, ou seja, o responsável na linha de frente pelo tratamento de dados pessoais realizado, atraindo para si a responsabilidade principal por eventuais violações de direitos.

A publicação da LGPD ampliou os debates em sede nacional sobre o direito à proteção de dados pessoais, resultando em seu reconhecimento como direito fundamental por meio da Emenda Constitucional 115/2022, responsável por acrescer ao artigo 5º da Constituição o inciso LXXIX, segundo o qual “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.” (BRASIL, 2022).

Sem ignorar o avanço na regulação do tratamento de dados pessoais no âmbito nacional trazido pela LGPD, tal como a importância de seu conhecimento como direito fundamental, importa enfatiza a lei de proteção de dados ainda apresentou lacunas regulatórias. Com base nas lições de Ingo Wolfgang Sarlet (2022, *online*):

> O direito fundamental à proteção de dados assume particular relevância, pelo fato da existência de uma série de lacunas regulatórias, posto que a LGPD não contempla os setores da segurança nacional, segurança pública,

> investigação criminal, execução penal, apenas para citar os mais relevantes. Por tal razão, com o reconhecimento do referido direito fundamental, passa a inexistir uma "zona livre" de proteção dos dados pessoais na ordem jurídica brasileira.

A fim de compreender os impactos ocasionados pela legislação de tratamento de dados pessoais, bem como identificar as lacunas legislativas citadas, faz-se mister a análise dos principais contornos jurídicos do marco regulatório brasileiro de tratamento de dados, com destaque para seus princípios, objetivos, e previsões relativas ao órgão fiscalizador da LGPD: a ANPD.

2.2. Os Principais Contornos Jurídicos da LGPD

Nos termos já pontuados alhures, a Lei Geral de Proteção de Dados inaugurou no ordenamento jurídico brasileiro a regulação sistematizada e específica do tratamento de dados sob o viés constitucional.

Para o fim de melhor compreensão da presente pesquisa, sobretudo quanto à análise da natureza da responsabilidade civil prevista na legislação, a ser posteriormente examinada, apresenta-se como ponto primordial o estudo dos principais contornos jurídicos da LGPD.

Anota-se, contudo, que o estudo a ser ora realizado não possui como propósito o esgotamento da análise quanto ao tema, considerando a abrangência e complexidade das disposições normativas previstas na LGPD. Em verdade, tem-se como objetivo trazer à lume o panorama geral que norteia a lei, com destaque para os fundamentos da legislação, seus princípios norteadores, objetivos, objeto de aplicação, dentre outras desdobramentos legais.

De início, comporta enfatizar que a lei sobre proteção de dados foi responsável por concretizar no ordenamento jurídico o direito à autodeterminação informativa, regulamentando especificamente o tratamento de dados pessoais em consonância com os direitos e garantias fundamentais previstas na Carta Magna.

Assim, nos termos do art. 1º da LGPD, referida legislação seria responsável por regular o tratamento de dados pessoais, realizado por pessoa física ou jurídica, de direito público ou privado, em meio físico ou digital. O dispositivo legal ainda prevê a teleologia legislativa do marco regulatório, o qual possui como propósito oportunizar a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da pessoa natural (BRASIL, 2018).

Ainda no parágrafo único do enunciado legal em comento, o legislador elenca os dispositivos constantes na legislação como de interesse nacional, devendo, portanto, serem observados por todos os entes da Administração Pública (BRASIL, 2018).

Em continuidade, a legislação, em seu artigo 2º, relaciona seus fundamentos norteadores, sendo eles o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Por este ângulo, a exemplo de outros marcos regulatórios nacionais, como o CDC, o art. 6º LGPD enuncia os princípios basilares da legislação, quais sejam: boa fé; finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação e prestação de contas (BRASIL, 2018).

Sobreleva-se neste ponto a necessidade de ser levado em consideração tanto as bases quanto os princípios da LGPD, como elementos vetores quando da interpretação de seus demais enunciados legais, frente à estruturação sistemática de aludida legislação.

Em seu artigo 3º, a LGPD demarca os limites de sua aplicação. Nos termos do dispositivo normativo, *ipsis literris*:

> Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional; [...]
> (BRASIL, 2018)

Porém, ainda que o tratamento de dados sob análise encontre subsunção nas hipóteses acima elencadas, a Lei Geral de Proteção de Dados, em

seu artigo 4º, explicita que ela não será aplicada a depender da finalidade que orientou o tratamento. Entre as exceções delineadas, encontra-se tratamento executado por pessoa física com fins estritamente particulares e não econômicos (BRASIL, 2018).

Dando continuidade, merece ser dado destaque ao caráter didático-normativo da LGPD: em seu artigo 5º, a legislação arrola a definição de termos técnicos empregados em sua redação, orientando tanto o aplicador do direito quanto pessoas leigas.

A técnica legislativa empregada materializa-se como importante meio para efetivação das finalidades da própria lei. Tomando como norte o fato de que a LGPD objetiva justamente regular o tratamento de dados pessoais no intuito de proteger o titular desses dados, concretizando, por consequência o direito à autodeterminação informativa, seria ilógico e desproporcional que os titulares desses dados, na maior parte das vezes, pessoas leigas, sofressem limitações à leitura e interpretação de lei pelo emprego de conceitos técnicos.

Posto isto, imprescindível trazer à análise os principais conceitos técnicos empregados pela legislação que se encontram diretamente relacionados ao objeto de estudo da presente pesquisa.

No artigo 5º, inciso I, o legislador lista “dados pessoais” como primeiro conceito técnico. Não poderia ser diferente, visto que referida definição orienta todos os demais enunciados legais. Para os efeitos da LGPD, é considerado dado pessoal a “informação relacionada a pessoa natural identificada ou identificável;” (BRASIL, 2018) .

A legislação ainda especifica o conceito de dado pessoal sensível, assim definido o “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018).

A diferenciação empregada pelo legislador é consequência da previsão de tratamento distinto entre aludidos dados pela LGPD, em face da complexidade protecional demandada pelos dados sensíveis.

Como doutrinam Sarlet e Ruaro (2021, p. 101 e 102), os dados conceituados como sensíveis estariam intimamente ligados aos elementos intrínsecos da personalidade, o que demandou que a lei trouxesse previsão de um

rol de direitos que focalizassem sua proteção, frente à possibilidade de uso discriminatório desses, atingido diretamente à dignidade da pessoa humana.

Frisa-se que tanto os “dados pessoais” quanto os “dados pessoais sensíveis” objetos do tratamento previsto estão relacionados a uma pessoa natural, denominada pela legislação, em seu artigo 5º, inciso V, como “titular” (BRASIL, 2018).

Com o enfoque em estabelecer uma interpretação sistemática, a LGPD também conceitua em seu artigo 5º, inciso X, o “tratamento” de referidos dados, assim abrangendo o procedimento empregado desde coleta até o descarte dos dados. De acordo com a redação legal, é considerado como “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)

Nesta sistematização, a LGPD trás previsão quanto aos agentes envolvidos na atividade de tratamento.

Em acordo com o artigo 5º, inciso VI da LGPD, considera-se controlador a “(...) pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL,2018).

Por seu turno, o operador de dados seria a “(...) pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”. (BRASIL, 2018)

Nos termos do art. 5º, inciso IX, da LGPD, o operador e o controlador seriam considerados “agentes de tratamento” de dados pessoais.

A legislação ainda trás previsão, em seu artigo 5º, inciso VIII, da figura do encarregado, assim considerado a “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de dados (ANPD)”; (BRASIL, 2018).

Último conceito técnico a ser exposto refere-se ao “consentimento”, definido pela legislação como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018). Como será especificado, o “consentimento”

consubstancia-se como umas das hipóteses autorizadoras da realização de tratamento de dados pessoais.

Uma vez esquadrinhados os conceitos técnicos basilares empregados no âmbito da LGPD, vale adentrar à análise dos preceitos estabelecidos pelo legislador para realização da atividade de tratamento.

A título de elucidação, releva-se que a LGPD, ao regular em seu capítulo II o tratamento de dados pessoais, o organizou em 4 (quatro) seções, relativas, respectivamente, aos requisitos exigidos para o tratamento de dados pessoais; ao tratamento de dados pessoais sensíveis; ao tratamento de dados pessoais de crianças e adolescentes; e ao término da atividade de tratamento.

A fim de delimitar a análise dos contornos jurídicos objeto de estudo do presente trabalho, analisar-se-á as principais disposições das duas primeiras seções, conforme retro transcritas.

A Seção I, responsável por regular os requisitos necessários para o tratamento de dados pessoais, é inaugurado pelo artigo 7º, o qual elenca as hipóteses permissivas da atividade de tratamento. Nesse sentido:

> Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I-mediante o fornecimento do consentimento pelo titular;
> II-para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III-pela administração pública, para o tratamento e uso compartilhado de dados necessário à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV-para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V-quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular de dados;
> VII-para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VIII-para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX-quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X- para proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
> [...]
> (BRASIL, 2018).

Como se nota, uma das bases legais permissivas para a atividade de tratamento é o consentimento. De acordo com Tarcísio Teixeira (2021, p. 80), o

consentimento adequado seria aquele demonstrado por escrito, em cláusulas com destaque em relação ao demais, ou por outro meio que seja apto a provar a manifestação de vontade do titular, como as ferramentas digitais.

No mesmo sentido, lecionam Sarlet e Ruaro (2021, p. 97) que o consentimento, preferencialmente deve estar relacionado a uma expressa e específica finalidade, de modo que no caso de mudança da finalidade do tratamento de um dado pessoal, figurar-se-ia fundamental um novo consentimento expresso do titular de dados, ou de seu pai/responsável no caso de tratamento de dados de crianças e adolescentes.

No entanto, nem sempre será possível atingir um plano ideal de consentimento nos termos relatados, mormente em face do dinamismo do mundo real e digital.

Dessa forma, no que tange aos dados pessoais, segundo Sarlet e Ruaro (2020,p. 98) o consentimento como base permissiva de seu tratamento deve ser interpretado a partir de um standard mínimo, isto é, que possibilite identificar que o titular dos dados, ao exercer o ato de consentir, tomou ciência, ao menos de uma forma genérica, que estaria oportunizando o tratamento de seus dados pessoais.

Por sua vez, no que diz respeito aos dados sensíveis, por expressa previsão legal do artigo 11, inciso I, da LGPD, o consentimento do titular para seu tratamento deve ser específico, destacada e para finalidades específicas (BRASIL, 2018).

Fato incontestável, todavia, é que o ônus da prova quanto à obtenção do consentimento para a atividade do tratamento é do controlador (TEIXEIRA, 2021, p . 80).

Outra base permissiva para a atividade de tratamento prevista pelo LGPD é o “legítimo interesse”, o qual, segundo Tarcísio Texeira (2021, p. 81) se trataria de um conceito aberto e abstrato, devendo ser interpretado conjuntamente com o artigo 10 da legislação.

Nessa lógica, nos termos do artigo 10 da LGPD o legítimo interesse estaria relacionado ao “apoio e promoção de atividades do controlador”, bem como à “proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais [...]” (BRASIL, 2018).

Desse modo, quando embasado no legítimo interesse do agente de tratamento, o tratamento de dados deve ocorrer em observância ao princípio da necessidade e da transparência, apenas podendo ser objeto de tratamento os dados estritamente necessários para a finalidade a ser atingida pelo controlador, devendo adotadas por este todas as medidas para garantir a clareza, aptidão e acessibilidade referentes ao tratamento (TEIXEIRA, 2021).

Ainda conforme enunciado pelo art. 10, §3º, quando a atividade de tratamento de dados pessoais tiver como fundamento o legítimo interesse, poderá ser solicitado ao controlador o relatório de impacto à proteção de dados pessoais, em observância aos segredos comercial e industrial (BRASIL, 2018).

Na seção seguinte, é regulado pelo legislador o tratamento de dados pessoais sensíveis. Nos termos do art. 11:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
> (BRASIL, 2018)

Como ensina Teixeira (2021, p. 82) as bases legais para o tratamento de dados pessoais sensíveis são divididas em duas categorias: com o consentimento ou sem o consentimento do titular. De tal feita, na primeira hipótese, a atividade de tratamento de dados só será possível desde que haja consentimento, específico e destacado, e para finalidades específicas. Na segunda categoria, são arroladas 7 (sete) subcategorias permissivas da atividade de tratamento

semelhantes, em maioria, às previstas no artigo 7º da legislação. Todavia, consoante lições de Tarcísio Teixeira, o interesse legítimo não é considerado base legal para tratamento de dados pessoais sensíveis, pela ausência de previsão.

A comunicação e uso compartilhado entre controladores de dados pessoais sensíveis relativos à saúde com o objetivo de obter vantagem econômica encontra vedação no artigo 10, §4º, excecionando a proibição em casos relativos a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

A LGPD ainda regula os direitos do titular de dados pessoais, os quais podem ser exercidos perante órgão administrativos (a exemplo da ANPD), judiciais, ou até mesmo frente aos controladores (TEIXEIRA, 2021, p. 83).

Em consonância com o artigo 18, caput, da LGPD, são direitos dos titulares a obtenção, a qualquer momento e mediante requisição ao controlador: da confirmação da existência de tratamento; do acesso aos dados; da correção de dados incompletos, inexatos ou desatualizados; da anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; da portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; da eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da lei; da informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; e da revogação do consentimento (BRASIL. 2018).

Consigna-se que o rol de direitos supra elencado visa efetivar um dos fundamentos da legislação: a autodeterminação informativa. De modo evidente, o rol de direitos catalogados no artigo 9º propicia o controle do titular em relação a seus dados, garantido a esse o acesso a esses dados, tal como o poder decisório em relação a eles.

Em seu capítulo IV, a LGPD regula o tratamento de dados pelo Poder Público. Nos termos do artigo 23, mencionado tratamento de dados seria realizado “[...] para o atendimento de sua finalidade pública, na persecução do interesse público, objetivando-se executar as competências legais ou cumprir as atribuições legais do serviço público” (BRASIL, 2018).

De acordo com a LGPD, caberia aos entes da Administração Pública cumprirem seu dever de informação, orientando os titulares, de modo explícito, sobre as hipóteses em que realizam o tratamento de dados no exercício de suas competências, a previsão legal que o autoriza, sua finalidade, e os procedimentos a serem utilizados na execução. Todavia, a LGPD ressalva que as empresas públicas e as sociedades de economia mista só serão consideradas como entidade do Poder Público, para os efeitos da lei, quando estiverem desempenhando a função típica administrativa, de modo que, nas demais hipóteses, serão regidas pelo disposto às pessoas jurídicas de direitos privado. (BRASIL, 2018).

Os órgãos públicos, para os efeitos da lei, poderão ser responsabilizados perante a ANPD, cabendo a esta adotar as medidas necessárias para fazer cessar o tratamento inadequado de dados, sem prejuízo da possibilidade da autoridade solicitar aos agentes do poder público “relatórios de impactos de dados pessoais” (BRASIL, 2018), a fim de controlar o cumprimento efetivo das disposições da LGPD

. Frisa-se que os órgãos públicos também se encontram sujeitos à responsabilização civil pelo tratamento inadequado de dados pessoais, a ser orientada pela interpretação conjunta da LGPD com o sistema normativo que rege a responsabilidade civil do Estado, o qual não se adentrará no presente estudo, tendo em vista suas peculiaridades.

A fim de concretizar suas disposições legais e finalidades, a LGPD traz dentro de seu Capítulo VI, a Seção II, nomeada como “Da Responsabilidade e do Ressarcimento de Danos”, trazendo, dentro da legislação, um microssistema normativo de responsabilidade civil pelo tratamento inadequado de dados pessoais no âmbito privado, como será pormenorizadamente estudado no próximo capítulo.

De mais a mais, foi destinado um capítulo específico para tratar do denominado pela legislação como “segurança e boas práticas”. Nesse sentido, conforme redação do art. 46, caput, da LGPD, dispositivo principiante do capítulo mencionado, cabe aos agentes de tratamento adotarem:

> [...]medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018)

Ao prever o que denominou como medidas de segurança, o legislador reconhece a insegurança presente no ambiente digital, prevendo, indiretamente, a possibilidade de invasão a sistemas de banco de dados por terceiros, o que, conseguintemente, implicaria no vazamento de dados pessoais.

Nesse espectro, a LGPD traz a obrigatoriedade de adoção de medidas de segurança por parte do agente de tratamentos, justamente no intuito de evitar qualquer violação às normas de proteção de dados.

Assim, a adoção da cultura de segurança ganha vultuosa e indispensável importância para os agentes de tratamento, uma vez que, qualquer pessoa, incluindo funcionários ou terceiros, poderá agir em desacordo com a legislação, o que implicará, por consequência, na responsabilização por parte dos agentes de tratamento responsável. (TEIXEIRA, 2021, p. 94)

Desse modo, em caso de vazamento de dados pessoais, uma das primeiras avaliações a ser realizada reside justamente na análise da adoção das técnicas de segurança e boas práticas previstas na legislação pelo agente de tratamentos:

> Caso ocorra algum incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiro não autorizado a acessá-los. (TEIXEIRA, 2021, p. 94).

Na Seção I do Capítulo VIII da LGPD, foi disciplinado pelo legislador as sanções administrativas pelo tratamento de dados em desacordo com a legislação. Aludidas sanções podem ser aplicadas independentemente ou conjuntamente com a responsabilização civil do agente de tratamento de dados pessoais, como será oportunamente exposto.

Entre as penalidades administrativas elencadas pelo legislador no artigo 52 da LGPD, destaca-se a advertência; multa simples, podendo chegar ao patamar R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração;

e até mesmo proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. As aplicações de referidas sanções, no entanto, dependem de prévio procedimento administrativo com observância da ampla defesa (BRASIL, 2018).

Como destaca Teixeira (2021, p. 92), apesar de não disciplinar especificamente tipos penais decorrentes do tratamento inadequado dos dados pessoais, tais condutas podem restar tipificadas como crimes em outras normas penais.

Ocorre que, a mera previsão de sanções administrativas na LGPD, ainda que associado à possibilidade de responsabilização civil dos agentes de tratamento, certamente, não seria o bastante para garantir o cumprimento de seus comandos legislativos: em que pese, pela primeira vez no ordenamento jurídico brasileiro se ter um diploma legal específico regulando o tratamento de dados, fazia-se fundamental a criação de um órgão administrativo que desse efetividade às suas previsões.

Nesse contexto, foi instituída a Autoridade Nacional de Proteção de Dados (ANPD). Este órgão estava previsto ainda na redação original que foi submetida à sanção presidencial. Contudo, as disposições atinentes à autoridade foram vetadas pelo então Presidente da República, sendo a LGPD publicada sem previsão de um órgão fiscalizador no âmbito da legislação.

A ANPD voltou ao sistema normativo da LGPD através da Lei nº 13.853, de 2019, responsável por incluir na legislação o artigo 55-A e seguintes, tendo sido instituída com o objetivo central de garantir eficácia às disposições da LGPD, sendo posteriormente disciplinada pelo Decreto nº 10.474/2020.

Sobre a importância da autoridade fiscalizadora, doutrina Danilo Doneda (2020, p.471):

> A atuação de uma autoridade de proteção de dados merece atenção dado que, nesse caso, a simples atuação do indivíduo para a proteção de seus interesses – o controle individual, que pode se materializar em algumas das concepções de proteção de dados pessoais – em muitas ocasiões não é capaz de proporcionar uma tutela adequada. A impossibilidade de que os direitos que hoje estão relacionados à proteção de dados sejam contemplados unicamente pela ação singular de seu interessado é patente em vista da desproporção entre as possibilidades do indivíduo e as estruturas hoje dedicadas ao tratamento de seus dados.

Elucida-se que, embora tenha sido criada como um órgão administrativo vinculado Presidência da República, a MP nº 1.124 DE 19/06/2022, alterou a previsão do art. 55-A da LGPD, a fim de transformar a natureza da ANPD em “autarquia de natureza especial dotada de autonomia técnica e decisória” (BRASIL, 2018).

O art. 55-J da LGPD é responsável por disciplinar uma série de competência atribuídas à ANPD, todas elas estando diretamente relacionadas à fiscalização e cumprimento da legislação de proteção de dados.

Entre as atribuições da autoridade, a mais conhecida está prevista no inciso IV do artigo citado, concretizando-se no poder de fiscalização e aplicação das sanções administrativas previstas na LGPD pelo descumprimento de seus comandos (BRASIL, 2018)

Sem embargo, a competência ANPD possui um alcance substancialmente maior, alcançando, conforme inciso VI do art. 55 J, o dever da autoridade em “promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança”; (BRASIL, 2018).

Vale sublinhar que apesar de ser trazida para o ordenamento jurídico em 2019, a ANPD só começou a atuar ativamente a partir de agosto de 2021, quando entrou em vigência as sanções administrativas previstas na legislação. De tal feita, a autoridade ainda está começando-se a estruturar-se em sua atuação, e, por conseguinte, apenas nos próximos anos poderá ser analisado de forma exauriente seu desempenho para a efetivação das disposições legislativas.

Aliás, não somente a efetividade da ANPD, como também das demais previsões legislativas da LGPD só poderão se verificar com o decorrer do tempo.

Entretanto, considerando a notória influência da GDPR no texto legislativo da LGPD, configura-se importante uma análise do marco regulatório brasileiro a partir do Regulamento Europeu de Proteção de Dados, bem como de jurisprudência do Tribunal de Justiça da União Europeia, considerando reunir os Estados que compõem o bloco econômico uma base normativa-jurisprudencial sobre proteção de dados pessoais mais sólida em relação aos demais países, inclusive o Brasil.

2.3. UMA ANÁLISE COMPARATIVA ENTRE MARCOS REGULATÓRIOS: LGPD X GDPR

Conforme analisado, a criação da LGPD no ordenamento jurídico brasileiro não se solidificou como um fenômeno isolado, mas sim como resultado de um avanço da sociedade digital e informacional, caracterizada pelo tratamento constante de um volume imensurável de dados.

O fenômeno citado também se verificou em escala global, sendo acompanhado por inúmeros marcos regulatórios que passaram a regulamentar o tratamento de dados pessoais no âmbito jurídico de diversos países. Dentre esses marcos regulatórios, certamente, o que exerceu maior poder de influência na criação da Lei Geral de Proteção de Dados Brasileira foi o Regulamento Europeu sobre Proteção de Dados, internacionalmente conhecido como GDPR (*General Data Protection Regulation*).

A influência mencionada pode ser comprovada pela análise comparativa entre os marcos regulatórios europeu e brasileiro, sendo que diversos enunciados legais da LGPD são notoriamente inspirados na redação legal do Regulamento Europeu.

Primeira similitude a ser trazida a estudo diz respeito às conceituações técnicas trazidas tanto pela LGPD, quanto pelo regulamento europeu.

O artigo 6º do marco regulatório brasileiro foi, veementemente, inspirado no artigo 4º da GDPR, classificado pelo subtítulo de “definição” e responsável por trazer uma série de conceitos concernentes a termos técnicos empregados pela legislação.

Tal como na LGPD, o primeiro termo técnico previsto pelo regulamento europeu é “dados pessoais”[1], conceituado como a informação relativa a uma pessoa natural identificada ou identificável, denominada como “titular de dados”. A redação legal ainda complementa que o titular de dados seria a pessoa que pode ser identificada, de forma direta ou indireta, em particular, por referência a um identificador, como um nome, um número de identificação, dados de localização, um

[1] Conforme artigo 4º (1) da GDPR: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (UNIÃO EUROPEIA, 2016)

identificador online ou a um ou mais fatores específicos da natureza física, fisiológica, identidade genética, mental, económica, cultural ou social dessa pessoa singular. (UNIÃO EUROPEIA, 2016).

Em que pese não especificar no rol do artigo 4º um termo técnico específico que corresponda aos “dados sensíveis” do marco regulatório brasileiro, a GDPR disciplina em referido artigo os “dados genéticos”, “dados biométricos” e os “dados relativos à saúde”.

Nessa perspectiva, menciona-se que os dados aludidos se incluem no tratamento dos “dados pessoais especiais” regulados pela GDPR em seu artigo 9º, de acordo com o qual, em seu tópico “1”, preconiza que:

> Artigo 9, (1) - Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited. [2] (UNIÃO EUROPEIA, 2016)

De forma veemente, os dados pessoais especiais abordados pelo marco regulatório europeu, em relação aos quais o diploma legal prevê um tratamento diferenciado, deram ensejo às disposições legais atinentes aos dados sensíveis na legislação brasileira.

O Regulamento Europeu ainda elenca, em seu artigo 4º[3], a definição de tratamento, assim considerado como:

> [...]‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; [4](UNIÃO EUROPEIA, 2016)

---

[2] Artigo 9, (1) - O tratamento de dados pessoais que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas ou filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para efeitos de identificação inequívoca de uma pessoa singular, dados relativos à saúde ou dados relativos a uma pessoa singular a vida sexual ou orientação sexual da pessoa deve ser proibida” (Tradução nossa).

[3] Artigo 4 (4) - ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; (UNIÃO EUROPEIA, 2016)

[4]“[...] qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais, por meios automatizados ou não, tais como recolha, registo, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por

A divisão dos agentes de tratamento de dados pessoais em controlador e operador também decorre da GDPR. O regulamento europeu emprega uma distinção entre os agentes responsáveis pelo tratamento, sendo estes segmentados em “controlador” e “processador de dados”.

Segundo lições de Pinheiro (2021, p. 24), o controlador seria aquele quem toma as decisões atinentes ao tratamento de dados, enquanto o processador quem efetua mencionado tratamento. Correspondem, respectivamente, ao “controlador” e “operador” no marco regulatório brasileiro.

Sem prejuízo de outras semelhanças entre o rol de termos técnicos entre os marcos regulatórios, passa-se à análise de outra herança da GDPR na LGPD: a limitação do tratamento de dados pessoais conforme sua finalidade.

Consoante leciona Patrícia Pinheiro (2021, p. 24), no marco regulatório brasileiro, compete aos agentes de tratamento de dados pessoais delinear a finalidade certa, garantida e justificável que autoriza o tratamento de um dado pessoal, de modo que o tratamento de referido dado pessoal só pode ser operar nos limites da finalidade especificada. No mesmo sentido, o regulamento europeu também prevê a imprescindibilidade da utilização do dado e adequação à sua finalidade, trazendo exceções ao tratamento que ocorra em razão de interesse público, segurança e saúde.

As hipóteses permissivas do tratamento de dados pessoais também advêm do conjunto normativo da GDPR. Em seu artigo 6º, o marco regulatório da União Europeia arrola as hipóteses em que o processamento de dados será considerado lícito.

Entre as bases legítimas de tratamento de dados relacionadas no artigo 6[5], sob estudo, também se identifica o consentimento de tratamento dos

---

transmissão, disseminação ou disponibilização de outra forma, alinhamento ou combinação, restrição, apagamento ou destruição.” (Tradução nossa).

[5] Consoante artigo 6º (1) da GDPR: Processing shall be lawful only if and to the extent that at least one of the following applies:
1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;

dados para determinada(s) finalidade(s), tal como o legítimo interesse do responsável pelo tratamento de dados pessoais (UNIÃO EUROPEIA, 2016).

Ademais, registra-se que diversos outros capítulos da GDPR serviram como base inspiradora da redação legal da LGPD. A convergência das previsões normativas pode ser notada nos capítulos que regulam, respectivamente, os direitos do titular dos dados, as disposições referentes ao controlador e processador, tal como no capítulo sobre a transferência de dados pessoais para países terceiros ou organizações internacionais. Todos os capítulos citados também se encontram presentes na legislação de dados brasileira.

Salienta-se que em seu artigo 32, o marco regulatório da União Europeia, aborda padrões de segurança no tratamento de dados pessoais, cabendo ao responsável pelo tratamento ou subcontratante implementar as medidas técnicas adequadas para garantir um nível de segurança adequado ao risco do processamento de dados (UNIÃO EUROPEIA, 2016). Mais uma vez, se nota a semelhança do Regulamento europeu com a LGPD, quando esta trata , em seu Capítulo VII, das medidas de segurança e das boas práticas no tratamento de dados pessoais.

O Regulamento Europeu também traz previsão, em seu artigo 83, de um rol de multas administrativas a serem aplicadas em caso de violação às disposições da legislação, parametrizando as condições que devem nortear a aplicação das penalidades, consoante circunstâncias do caso concreto.

A fim de garantir a efetividade das previsões legais, a GDPR traz previsão em seu Capítulo 6 de uma autoridade supervisora, com poderes semelhantes à da ANPD brasileira.

No entanto, considerando que o marco regulatório em estudo possui vigência sobre todos os países membros da União Europeia, a fim de garantir uma atuação centralizada, e, por consequência, efetiva, dessas autoridades supervisoras, a GDPR especifica em seu artigo 51 que em cada Estado-Membro do bloco econômico deve haver uma ou mais autoridades independentes, responsáveis pela

---

4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (UNIÃO EUROPEIA, 2016).

aplicação efetiva do regulamento. Em que pese a independência existente entre cada autoridade supervisora, o regulamento assevera o dever de atuação em cooperação uma às outras (UNIÃO EUROPEIA, 2016).

Como elucida Lorenzon (2021, p. 45), referidas autoridades supervisoras são denominadas como *Data Protectio Authorities* (DPA). Para que seja efetivada a cooperação entre as DPA's, agindo estas em cooperação para aplicação do regulamento europeu, o diploma legal traz previsão do *European Data Protection Board (*Conselho Europeu para Proteção de Dados), o qual é composto por representantes das autoridades de fiscalização (DPA's) de cada país membro, e possui competência para emitir diretrizes a respeito das disposições da GDPR.

Digno sublinhar que a GDPR ainda regulou existência de um profissional, responsável por verificar a adequação das previsões do regulamento ao tratamento de dados realizado, por entes públicos ou empresas privadas, o DPO (*Data Protection Officer*). (LORENZON, 2021, p. 44).

Nos termos do artigo 37 do Regulamento europeu, haverá obrigatoriedade na designação de um DPO pelos agentes de tratamento quando: o tratamento for efetivado por autoridade ou órgão público (com exceções dos órgãos judiciais); as atividades dos agentes de tratamento, em razão de sua finalidade, exigirem um acompanhamento regular dos titulares de dados em massa; e quando as atividades dos agentes do tratamento consubstanciarem em tratamento em grande escala de categorias de dados especiais, nos termos do regulamento (UNIÃO EUROPEIA, 2016). Rememora-se que referidos dados especiais são os tratados pela LGDP como dados sensíveis.

Figura profissional similar ao DPO foi prevista na LGPD: o denominado encarregado, responsável, como já elucidado, por funcionar como canal de comunicação entre controlador, titular de dados e a ANPD, nos termos do art. 5º, inciso VIII, da legislação brasileira. Sublinha-se que a LGPD elenca, em seu artigo 41, o rol de atribuições do encarregado, especificando que a ANPD poderá complementar as normas atinentes a referido cargo. (BRASIL, 2018).

No intuito de garantir a efetividade de suas previsões legais, ambos marcos regulatórios também preveem a possibilidade de ser solicitado ao responsável pelo tratamento de dados o relatório de impacto de dados pessoais. De acordo com o artigo 35 da GDPR, o qual encontra semelhança legal com o artigo 10, §3º, do diploma legal brasileiro:

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. [2]A single assessment may address a set of similar processing operations that present similar high risks. [6] (UNIÃO EUROPEIA, 2016)

Cabe enfatizar, por derradeiro, a similitude existente entre as previsões legais referentes à responsabilidade civil na LGPD (a ser estudada no capítulo subsequente) com a GDPR, regulada nesta última em seu artigo 82.

Com redação extremamente similar ao artigo 42 da LGPD, o marco regulatório europeu preconiza que qualquer pessoa que venha a sofrer danos materiais ou imateriais decorrentes da violação do regulamento, terá direito à indenização do controlador ou processador pelos danos sofridos (UNIÃO EUROPEIA, 2016)[7].

As demais previsões da GDPR quanto à responsabilidade civil no âmbito do regulamento também foram integralmente reproduzidas pela legislação brasileira.

De acordo com o Regulamento europeu (UNIÃO EUROPEIA, 2016), o controlador envolvido no tratamento de dados poderá ser responsabilizado quando este implicar em violação do regulamento. Por sua vez, assim como prevê a LGPD, o processador só será responsável pelos danos decorrentes do tratamento quando tiver deixado de cumprir suas obrigações nos termos da GDPR, ou quando tiver agido em contrariedade às instruções legais do controlador.

De mais a mais, a GDPR também exclui a responsabilidade dos agentes de tratamento quando estes provarem que não forem responsáveis pelo evento que ocasionou o dano.

A similitude existente entre os marcos regulatórios faz com que o operador de direito, por vezes, se utilize da GDPR como base interpretativa por

---

[6]Art. 35, (1) da GDPR: “Sempre que um tipo de tratamento, em particular que utilize novas tecnologias, e tendo em conta a natureza, âmbito, contexto e finalidades do tratamento, possa resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve, previamente ao tratamento, proceder a uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais. Uma única avaliação pode abordar um conjunto de operações de processamento semelhantes que apresentam riscos elevados semelhantes.” (tradução nossa)

[7] Art. 82, (1) da GDPR: “Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.” (UNIÃO EUROPEIA, 2016)

analogia da LGPD, sobretudo nas hipóteses em que o legislador brasileiro foi omisso ao regular determinado tema.

Por exemplo, ambos os marcos regulatórios dispõem sobre o dever do controlador em comunicar a autoridade fiscalizadora e o titular de dados sobre a ocorrência de incidente de segurança que implique em violação dos dados. Todavia, enquanto nos termos do artigo 48 da LGPD, a comunicação só deve ocorrer quando houver risco ou dano relevante ao titular de dados, e a comunicação deve ser feita em "prazo razoável" (BRASIL, 2018), segundo o artigo 33 da GDPR[8], essa comunicação se torna regra. Em havendo violação de dados pessoais, salvo na hipótese de improvável risco dessa violação, deve ser feita a comunicação pelo responsável pelo tratamento no prazo máximo de 72 horas (UNIÃO EUROPEIA, 2018).

A ausência de previsão expressa quanto ao prazo máximo para ser realizada à comunicação à ANPD sobre o vazamento de dados pessoais faz com que, os operadores de Direito interpretem o "prazo razoável", presente na redação do artigo 48 da LGPD, como 72 horas.

Pelo exposto, não obstante a existência de determinadas divergências pontuais entre os marcos regulatórios, a maior parte delas decorrentes das especificidades do ordenamento jurídico no qual estão inseridos, vê-se notória a influência exercida pela GDPR sobre a redação legal da Lei Geral de Proteção de Dados brasileira, sobretudo em relação às suas bases fundadoras e objetivos legais.

Observa-se, em diversas oportunidades, que a LGPD se utiliza de disposição legal praticamente idêntica ao Regulamente Europeu. Até mesmo aparentes inovações da LGPD, como é o caso dos denominados como "dados sensíveis" e da figura do encarregado, tiverem como base inspiradora a GDPR.

Mencionadas semelhanças permitem que a interpretação doutrinária e jurisprudencial a respeito da GDPR seja, por vezes, utilizada em conjunturas que circundam o diploma legal brasileiro, em relação às quais permeiam divergências.

[8] Art. 33, (1) da GDPR: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [2]Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay." (UNIÃO EUROPEIA, 2016)

2.4. Uma Análise da Jurisprudência do Tribunal de Justiça da União Europeia sob o Viés da Proteção de Dados Pessoais

Consoante exposição realizada, o marco regulatório brasileiro de proteção de dados foi claramente inspirado nos fundamentos e principais disposições do *General Data Protection Regulation*.

Nessa lógica, há que se enfatizar que o pioneirismo da União Europeia quanto à regulamentação sistematizada do tratamento de dados pessoais e seus principais desdobramentos é resultado direto de suas bases histórico-normativas. Antes mesmo da consolidação da União Europeia, o Ordenamento Jurídico de seus Estados - Membros mostraram-se percussores na normatização da proteção de dados pessoais.

Em uma breve análise histórica, cabe ser citada a Lei de Proteção de dados de Hesse, publicada em 1970, na Alemanha. Consoante explica Doneda (2020, p. 26), aludida legislação possuiu um caráter vanguardista, trazendo uma mudança de paradigmas no sistema normativo, ao preconizar um modelo legislativo autônomo de proteção de dados pessoais, sendo resultado dos avanços experimentados pela sociedade da época.

Como demonstrativo da mudança da perspectiva ocasionada pela legislação, Doneda (2020, p. 23) cita que pela primeira vez foi utilizado em um texto legal o termo “proteção de dados”, além de sua redação trazer um novo panorama em relação ao direito à segurança de informação e de sigilo: concebia-se na Lei de Hesse um embrião do direito à proteção de dados.

É possível perceber que a Lei de Hesse sobre proteção de dados pessoais figurou-se como um importante avanço na perspectiva da proteção de dados pessoais no âmbito internacional. Aliás, foi no âmbito do Tribunal Constitucional alemão que foi proferida uma marcante decisão no que diz respeito ao reconhecimento do direito à proteção de dados pessoais como garantia constitucional em Estados democráticos. Como preconiza Doneda (2020, p. 26), no ano de 1983, em análise de um caso no qual era discutido a atividade estatística, referido tribunal entendeu que o processamento de dados em massa, resultante dos avanços tecnológicos experimentados pela sociedade, propiciavam ameaças e riscos, os quais exigiam a revisitação dos direitos fundamentais sob esse viés. O

Tribunal Constitucional alemão reconhecia, pela primeira vez, o direito à autodeterminação informacional.

Enfatiza-se que aludido direito, nas décadas posteriores, passaria a ser reconhecido na legislação de diversos Estados-Democráticos, entre eles o Brasil.

Dando seguimento, importa elucidar que pouco tempo após a formação da União Europeia, foi publicada em 1995, a Diretiva/95/46/CE do Parlamento Europeu, "[...] relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados." (UNIÃO EUROPEIA, 1995). A diretiva foi responsável por nortear a regulação referente proteção de dados pessoais na perspectiva do bloco econômico.

De acordo com seu artigo 1º, a diretiva tinha como principal objetivo estabelecer parâmetros para que os Estados - Membros da União Europeia assegurassem "[...] a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais" (UNIÃO EUROPEIA, 1995).

Ao observar sua estrutura normativa, é possível notar, de plano, que a Diretiva serviu como âmago para o texto legal da GDPR, a ser publicado duas décadas depois. Como exemplo, cita-se que até mesmo conceitos técnicos, dispostos, em seu artigo 2º, foram mantidos e aprimorados pelo regulamento europeu.

Desse modo, embora ainda se possa considerar recente a vigência do Regulamento Europeu de Proteção de Dados, a União Europeia já possuía um sólido sistema normativo no tocante à proteção de dados pessoais, em comparação ao Brasil.

Por tal razão, o Tribunal de Justiça da União Europeia foi responsável por proferir importantes julgados, ainda sob a vigência da Diretiva/95/46/CE, os quais podem ser utilizados como vetores interpretativos da GDPR, e, inclusive, da LGPD, considerando a semelhança legal e teleológica existente entre os marcos regulatórios, conforme exposto no tópico anterior.

Sob esse ângulo, sublinha-se que o Tribunal de Justiça da União Europeia possui uma ficha temática responsável por reunir importantes julgados do tribunal na perspectiva da proteção de dados pessoais.

De tal feita, almeja-se realizar uma breve análise de julgados constantes em citada ficha temática, com o fim de estabelecer um norte de

interpretação para os dispositivos legais da GDPR, e principalmente, da LGPD, mormente em relação à delimitação dos pressupostos da responsabilidade civil nesta última, a ser posteriormente analisada.

Primeira jurisprudência a ser trazida à colação concerne a Acórdão publicado pelo Tribunal de Justiça da União Europeia (UNIÃO EUROPEIA, 2021, p.24) em 16 de dezembro de 2008, responsável por delimitar o conceito de "necessidade" do tratamento de dados pessoais sob o viés da Diretiva 95/46/CE.

A demanda sob julgamento do Tribunal (UNIÃO EUROPEIA, 2021, p. 24) teria sido ajuizada por H. Huber, um nacional austríaco que exercia na Alemanha a profissão de agente de seguros de forma autônoma, e que se opôs a política realizada pelo Serviço Federal das Migrações e Refugiado, ao criar um sistema de registro de dados pessoais de estrangeiros que residiam no território por período superior a 3 (três anos).

Nesse sentido, vale ressaltar os parâmetros utilizados pelo Tribunal para o balizamento do conceito de "necessidade":

> No que diz respeito ao conceito de «necessidade» do tratamento na acepção do artigo 7.°, alínea e), da Diretiva 95/46, o Tribunal começou por recordar que se tratava de um conceito autónomo do direito da União que deve receber uma interpretação suscetível de cumprir plenamente o objetivo da Diretiva 95/46, definido no seu artigo 1.°, n.° 1. Em seguida, o Tribunal constatou que um sistema de tratamento de dados pessoais só é conforme ao direito da União se contiver unicamente os dados necessários à aplicação dessa legislação pelas referidas autoridades e o seu caráter centralizado permitir uma aplicação mais eficaz dessa legislação no que respeita ao direito de residência dos cidadãos da União Europeia que não são nacionais desse Estado-Membro. (UNIÃO EUROPEIA, 2021, p. 24)

Transportando mencionado entendimento para a LGPD, é possível constatar que o tratamento a ser realizado pelos agentes de tratamento deve restringir-se aos dados estritamente necessários à finalidade do tratamento.

Na análise sob a perspectiva do ato ilícito, pressuposto da responsabilização civil na LGPD a ser analisada oportunamente, conclui-se que, em casos nos quais a coleta de dados pessoais se dê fora dos parâmetros balizadores da necessidade/finalidade do tratamento, este será considerado ilícito, e, por conseguinte, potencialmente ensejador de responsabilização civil em um caso concreto.

À título de exemplo, menciona-se a situação em que um agente de tratamentos que, no âmbito do *e-commerce*, realize a coleta de dados além dos

imprescindíveis para a realização de uma transação comercial, com a finalidade de formar um banco de dados de seus consumidores. Sem sombra de dúvidas, estar-se-á figurado um ato ilícito.

Outro Acórdão a ser analisado, proferido pelo Tribunal de Justiça da União Europeia, diz respeito ao direito de esquecimento na perspectiva da proteção de dados pessoais na internet.

No caso sob julgamento, no qual envolvia um provedor de julgamento da internet, o Tribunal (UNIÃO EUROPEIA, 2021, p. 47/48) fixou entendimento no sentido de que em determinadas circunstâncias, o provedor de internet seria obrigado a retirar os resultados da busca realizada a partir do nome de uma pessoa, bem como os resultados de páginas *web* publicadas por terceiros e que possuam informações associadas ao titular de dados.

O Tribunal de Justiça aludido trouxe, mais uma vez, a "necessidade do tratamento" como parâmetro interpretativo, estabelecendo que o direito do esquecimento também se materializa na hipótese em que os dados coletados já não atendem mais à finalidade para qual foram coletados, hipótese em que devem ser suprimidos da página de buscas. De mais a mais, conforme entendimento do Tribunal, a análise da "necessidade do tratamento", deve estabelecer ponderação entre direitos fundamentais e interesse público. Assim, o direito ao esquecimento do titular de dados prevalece, como regra, aos interesses do provedor de internet e do interesse público, em ter acesso às informações do titular. Sem embargo, se em face das peculiaridades do caso, o titular de dados tenha função pública, o interesse público pode sobressair-se ao direito ao esquecimento. (UNIÃO EUROPEIA, 2021, p. 48)

Apesar do julgado em menção ter sido proferido antes mesmo da publicação da GDPR, ainda no manto da Diretiva/95/46/CE, é possível denotar pelo menos 3 (três) vetores interpretativos que podem ser extraídos do caso narrado, a serem aplicados LGPD.

Como já ressaltado, repisa-se a imprescindibilidade da aplicação do fator "necessidade do tratamento" para delimitação do ato ilícito. Um dos fatores primordiais a serem analisados no caso concreto para determinar se presente ou não o ato ilícito dos agentes de tratamento é a verificação se o tratamento de dados ocorreu conforme a necessidade e finalidade que justificaram, inicialmente, a coleta de referidos dados.

No mais, anota-se a importância da aplicação da ponderação de direitos sob o viés da LGPD, mormente no que tange ao legítimo interesse como base permissiva do tratamento de dados pessoais.

Nessa linha de raciocínio, observa-se que ao analisar o tratamento de dados fundado em suposto legítimo interesse do controlador, comporta ser realizada uma ponderação entre o “apoio e promoção de atividades do controlador” e “a proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais [...]”, consoante artigo 10, incisos I e II, da LGPD (BRASIL, 2018)

Em prevalecendo, em um caso concreto, o direito da proteção do titular de dados pessoais sobre o interesse do controlador, o tratamento de dados pelo último realizado não pode ser considerado legítimo, tendo sido efetivado, por conseguinte, em desacordo com as bases permissivas do diploma legal, consubstanciando, destarte, o ato ilícito.

Considerando a abstratividade do legislador ao conceituar o legítimo interesse com base permissiva do tratamento de dados pessoais, nota-se que a ponderação de direitos do titular e o interesse do controlador terão papel fundamental na condução da interpretação judicial em casos levado à análise do Estado-Juiz.

Última consideração a ser destacada em relação ao julgado refere-se ao “prejuízo”, materializado na LGPD como um dos pressupostos da responsabilidade civil: o dano.

Conforme interpretação do Tribunal de Justiça da União Europeia (UNIÃO EUROPEIA, 2021, p. 48), nem sempre a existência de um direito, e consequente violação, implicará em um necessário prejuízo à parte.

Infere-se que a execução do tratamento de dados de dados pessoais em desacordo com a LGPD, sem qualquer potencial prejuízo ao titular, não pode ser considerado passível de ensejar danos morais *“in res ipsa”* sob o fundamento da violação de um direito constitucionalmente garantido.

Por fim, importa trazer à análise julgado recente do Tribunal de Justiça da União Europeia, já durante a vigência da GDPR, responsável por estabelecer preceitos sobre o “consentimento”.

No Acórdão de 01 de outubro de 2019 (Grande Seção), discutia-se a validade do consentimento através de cookies já instalados no dispositivo eletrônico. Conforme entendimento do Tribunal de Justiça de União Europeia (UNIÃO EUROPEIA, 2021, p. 56), o consentimento para o tratamento de dados pessoais, a partir de uma opção pré-validada decorrente de *cookies* (informações já armazenadas no equipamento), na qual o titular deve operar a desmarcação da opção para demonstrar seu consentimento, não pode ser considerado um consentimento válido.

Para o Tribunal, a mera aceitação do titular de dados quanto à utilização de *cookies* não exprime, necessariamente, a sua concordância para que o ato de consentir quanto ao tratamento de seus dados se dê por opções pré-validadas por esses *cookies.* (UNIÃO EUROPEIA, 2021, p. 56)

Como se verifica, o Tribunal de Justiça da União Europeia adotou um posicionamento que tende a ser seguido pelos tribunais brasileiros: a qualificação do consentimento.

Neste diapasão, o consentimento para tratamento de dados deve ser dar de modo expresso e específico, através de cláusulas em destaque, principalmente no que tange aos dados sensíveis, sob pena de se ter um tratamento ilícito de dados.

Não se ignorando que os parâmetros interpretativos ora firmados tendem a ser aprimorados nos próximos anos, conforme entendimento jurisprudencial a ser firmado em situações concretas em que se figurar a Lei Geral de Proteção de Dados como causa de pedir, estas premissas serão utilizadas no decorrer desta pesquisa com o intuito de orientar a fixação e interpretação dos pressupostos do regimento jurídico trazido pela LGPD quanto à responsabilidade civil dos agentes de tratamentos de dados pessoais.

3 RESPONSABILIDADE CIVIL NA LGPD NO ÂMBITO PRIVADO E OS IMPACTOS DA LEGISLAÇÃO NAS RELAÇÕES CONSUMERISTAS

Conforme exposto no Capítulo anterior deste trabalho, o Marco Civil da Internet e a Lei Geral de Proteção de Dados proporcionaram um grande avanço no tocante à regulação legal das relações existentes no ambiente virtual, tema que até então não possuía legislação específica sobre seu tratamento.

No tangente à LGPD, pontua-se que a legislação visou disciplinar diversos aspectos relacionados ao tratamento, armazenamento, e descarte de dados pessoais, trazendo conceitos relativos ao tema, sanções administrativas aos agentes de tratamento de dados pessoais pelo incorreto tratamento desses dados, e, sobretudo, a previsão da Responsabilidade Civil desses agentes, separando a responsabilidade do Poder Público e de particulares, esta última objeto de estudo do presente trabalho.

A LGPD transparece a tentativa de adequação da legislação infraconstitucional à realidade hodierna, com enfoque no tratamento da responsabilidade civil diante da temática. Nesse sentido, conveniente trazer à colação pensamento da professora Giselda Hironaka (2005, p. 128), que ao realizar uma comparação com a tese do escritor italiano Norberto Bobbio, enfatiza que:

> De acordo, ou não, com as conclusões de Bobbio, o que é inegável é esse caráter variável dos direitos humanos ou fundamentais, e o que é completamente verdadeiro, conforme depoimento da própria vida e da própria História, é o fato de que novas pretensões, a respeito das quais nem se cogita, poderão surgir, impondo a geração de novos direitos. É assim, exatamente assim, o que ocorre no plano da responsabilidade civil, cuja trajetória, ao longo do tempo, certamente abona a afirmação.

De certo, a criação da LGPD, e sua consequente previsão quanto à responsabilização civil dos agentes de tratamento de dados pessoais, é uma marca evidente da hodiernidade, sendo uma das “novas pretensões” citadas por Hironaka. Prova de tal fato é a elevação do direito à proteção de dados pessoais ao patamar de direito fundamental, nos termos da Emenda Constitucional 115/2022 (BRASIL, 2022).

Esse cenário que é abrangido pela LGPD, à época da promulgação do Código Civil não padecia de vultuosa notoriedade, sendo resultado de um

inestimável avanço tecnológico ao longo das últimas décadas, demandando o tema de regulação posterior.

Superada essa análise, comporta esclarecimentos sobre a previsão de responsabilidade civil, e de sanções administrativas na lei em estudo.

A Lei nº 13.709/2018 traz previsão da responsabilidade civil pelo tratamento de dados pessoais no âmbito privado nos artigos 42 a 45, e das sanções administrativas nos artigos 52 a 54, dispositivos estes que devem ser interpretados em sistemática com todo o texto legal em comento, visando dar efetividade à legislação.

Destaca-se que a responsabilidade civil e as sanções administrativas podem ser aplicadas cumulativamente aos operadores de dados pessoais pelo incorreto tratamento desses. Isto porque, no primeiro caso, se está diante de consequências jurídicas pelo inadequado de dados pessoais, e, no segundo caso, de consequências administrativas.

Sobre essa diferenciação, frisa-se que o valor decorrente das sanções administrativas previstas na LPGD será exclusivamente destinado ao Poder Público, de modo que possuem essas sanções um caráter eminentemente administrativo. Conforme preconizam Godinho, Queiroga Neto e Tôledo (2020, p. 07):

> Nesse ínterim, a multa aplicada às empresas pode chegar a 2% de seu faturamento anual, limitado tal patamar a até R$ 50 milhões por infração. Não obstante a lei preveja um valor tão elevado como sanção para casos de difusão de dados pessoais, por exemplo, o montante arrecadado será inteiramente destinado aos cofres do Estado, de modo que não será convertido como indenização para os verdadeiros prejudicados, os titulares dos dados compartilhados. Destaca-se, neste particular, o viés pedagógico e punitivo – mas não indenizatório – da aludida sanção.

Por sua vez, a responsabilidade civil possui um aspecto muito mais complexo, considerando a multifuncionalidade desta, e sua destinação à reparação do dano sofrido pelo titular de dado pessoal. Cumpre salientar que não existem posicionamentos pacíficos quanto à função da Responsabilidade Civil, no entanto, a doutrina aponta para três funções em essência: a função reparadora, a função precaucional e a função punitiva.

Sobre o caráter funcional da responsabilidade civil, merece colação as lições de Braga Netto, Farias e Rosenvald (2019, p.67):

> [...] Especificamente, no setor da responsabilidade civil há uma pluralidade de funções, sem qualquer prioridade hierárquica de uma sobre outra. Cremos que no direito brasileiro do alvorecer do século XXI, a conjunção dessas orientações permite o estabelecimento de três funções para a responsabilidade civil: (1) Função reparatória: a clássica função de transferência dos danos do patrimônio do lesante ao lesado como forma de reequilíbrio patrimonial; (2) Função punitiva: sanção consistente na aplicação de uma pena civil ao ofensor como forma de desestímulo de comportamentos reprováveis; (3) Função precaucional: possui o objetivo de inibir atividades potencialmente danosas.[...]

Conveniente adotar o raciocínio firmado por Braga Netto, Farias e Rosenvald, de modo a considerar uma multiresponsabilidade da responsabilidade civil na LGPD.

O inadequado tratamento de dados pessoais pelos agentes de tratamento, e um consequente dano ao titular desses dados, invoca imediatamente a função de reparação desse dano, uma vez que o titular teve seu direito à privacidade violado.

Na mesma toada, não se pode ignorar a necessidade de levar em consideração a função punitiva e a função precaucional na análise da responsabilidade civil na LGPD.

O armazenamento de dados pessoais, com a formação de banco de dados pelos agentes de tratamento, mostra-se um lucrativo negócio para esses, que fornecem referidos dados pessoais a terceiros, objetivando o lucro.

Se desconsiderada totalmente a função punitiva na fixação da responsabilidade, há grandes chances de ser mais viável para esses agentes fornecerem esses dados pessoais a terceiros, mesmo tendo que arcar com uma possível responsabilização civil futura. Desta feita, deve ser ponderada a “punição” do agente de tratamento pela violação ao dever de segurança que norteia a lei de proteção de dados na fixação do *quantum* indenizatório. No entanto, essa função punitiva deve ser analisada com cautela.

À princípio, salienta-se que considerar a função punitiva na fixação dessa responsabilidade não significa objetivar a responsabilidade civil na LGPD, mas sim criar parâmetros mais rigorosos para excluir essa responsabilidade no caso concreto. Ademais, em determinados casos, a função punitiva já terá se concretizado através das funções administrativas, devendo ganhar papel menos relevante na fixação da indenização.

Por sua vez, no que diz respeito à função precaucional, enfatiza-se que está é privilegiada pela própria Lei Geral de Proteção de Dados. De acordo com o artigo 6º, inciso VIII, um dos princípios vetores da legislação seria justamente a prevenção, isto é, a "[...] adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;" (BRASIL, 2018)

No mesmo sentido, implicitamente prevendo referida função, o artigo 6º, inciso X, aponta como outro princípio a responsabilização e prestação de contas, devendo ser adotado pelo agente de tratamento "[...] medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;" (BRASIL, 2018). Essa prestação de contas preconizada pela legislação seria justamente com o objetivo de prevenir possíveis danos.

Assim, a interpretação sistemática da própria legislação leva a inferir que uma das funções a serem consideradas na fixação da responsabilidade civil na LGPD é a precaucional.

Vale pôr em evidência que a previsão específica de responsabilidade civil na LGPD não exclui as previsões pertinentes e aplicáveis ao tema previsto no Código Civil, isto porque, o Ordenamento Jurídico deve ser interpretado como um sistema, e não uma norma excluindo a outra em razão de pertencerem a diferentes áreas jurídicas, maximizando a tese da Teoria do Diálogo de Fontes, do jurista alemão Erik Jayme.

Sobre a teoria citada, merece destaque as lições de Cláudia Lima Marques, responsável por introduzir a Teoria alemã no Brasil. De acordo com a professora (2002, p. 502 e 503):

> Assim, o aplicador da lei deve examinar o conflito com olhos plurais, adaptando sua própria formação e seus preconceitos às necessidades desta sociedade de consumo de informação, de rapidez fantástica e de uma produção legislativa cada vez mais impressionante e plural (de Tratados, leis gerais, leis especiais, leis praticamente materiais, leis complementares, leis com números e sem números, de medidas provisórias mensais, de decretos, portarias, circulares etc.). O aplicador deve também visar o diálogo de fontes, de forma a dar efeito útil a um grande número de normas, privilegiando as normas narrativas, os valores constitucionais e sobretudo os direitos humanos [...]

Seguindo o raciocínio de Marques, observa-se que a LGPD deve ser interpretada em consonância com os demais ramos jurídicos, com enfoque no Direito Civil, Direito Processual Civil, Direito do Consumidor e Direito Constitucional.

Isto é, este trabalho partiu do pressuposto que a LGPD não é uma lei isolada, mas sim um texto legal que faz parte de um sistema maior, e deve ser interpretada conforme as disposições de todo esse sistema. Esse sistema é o ordenamento jurídico vigente, que tem como elemento central a dignidade da pessoa humana.

Inclusive, esse diálogo entre normas está implicitamente previsto no artigo 64 da lei de proteção de dados, segundo o qual os direitos disciplinados na lei referida não excluem outros previstos no ordenamento jurídico brasileiro ou em tratados internacionais ratificados pelo Brasil, relacionados à matéria tratada (BRASIL, 2018).

Assim sendo, indispensável realizar-se uma análise legal da Responsabilidade Civil prevista entre os artigos 42 a 45 da LGPD, em diálogo com o sistema normativo brasileiro, no intuito de fixar os pressupostos de aludida responsabilidade no âmbito da lei.

De mais a mais, busca-também a consolidação do fundamento da responsabilidade civil prevista na Lei Geral de Proteção de Dados, partindo-se da conjugação de citado estudo, com a análise do direito comparado e dos posicionamentos doutrinários concernentes ao estado atual da arte do tema no ordenamento jurídico brasileiro.

3.1. Análise Legal da Responsabilidade Civil na LGPD no Âmbito das Relações Privadas

Em um primeiro momento, digno enfatizar que a responsabilidade civil na LGPD estará presente diante do ato ilícito, caracterizado quando o agente de dados pessoais violar norma (em sentido *latu*) da legislação de proteção de dados pessoais, agindo em desrespeito aos limites estabelecidos pela norma e aos princípios que norteiam a LGPD.

Adentrando à análise dos dispositivos legais que tratam de Responsabilidade Civil na própria LGPD, cabe colacionar o art. 42 , caput, que inaugura o tema, trazendo uma cláusula geral de Responsabilidade Civil para os efeitos da lei sob comento, *in verbis*:

> O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. [...] (BRASIL, 2018)

Nota-se que o dispositivo supra traz uma cláusula de responsabilidade na legislação de proteção de dados. Em seus termos, o controlador ou operador de dados pessoais, que, violando a LGPD, no exercício de atividade de tratamento de dados pessoais, causar danos a outrem, fica obrigado a repará-lo, podendo ser esse dano de natureza patrimonial ou moral, individual ou coletivo.

Nos termos do artigo 42, podem ser responsabilizados civilmente no âmbito da LGPD, o controlador e operador de dados pessoais, denominados pela legislação como “agentes de tratamento”.

A não inclusão do encarregado no rol dos agentes de tratamento, aliás, é apontado como uma contradição. Nessa linha de raciocínio, elucida Tarcísio Teixeira (2021, p.87):

> Embora a Seção II (Do Encarregado pelo Tratamento de Dados Pessoais) pertença ao Capítulo IV (Dos Agentes de Tratamento de Dados Pessoais), não se pode afirmar categoricamente que o encarregado seja um dos agentes. Isso pois, nos termos do art. 5º, IX, agentes de tratamento são apenas o controlador e o operador. Trata-se de outra contradição da lei.

Os agentes de tratamento, à letra do disposto pela norma colacionada, respondem perante “outrem” a quem foi causado o dano. Pela utilização de referida expressão, considera-se que qualquer indivíduo pode sofrer dano decorrente da atividade de tratamento de dados, não apenas o titular. Contudo, mostra-se de difícil visualização, em um caso concreto, um terceiro ser atingindo pelo tratamento de dados que não o pertence.

Nesse seguimento, importante trazer à lume que é considerado pela LGPD, nos termos do artigo 5º, inciso V, como titular de dados, a pessoa natural cujos dados pessoais são objetos do tratamento (BRASIL, 2018).

Seguindo nessa perspectiva, preceitua o art. 42 da LGPD, em seu parágrafo primeiro, hipóteses de responsabilização solidária dos agentes de tratamento.

De acordo com o artigo 42, §1º, inciso I, no intuito de assegurar a efetiva indenização do titular, o operador de dados responde de forma solidária pelos danos causados em razão da atividade de tratamento quando houver descumprimento das obrigações impostas por referida lei, ou na hipótese em que não tiver seguido as instruções lícitas do controlador (BRASIL, 2018).

Em relação à referida responsabilização solidária, Tarcísio Teixeira (2021, p. 87) aponta a relevância do contrato firmado entre controlador e operador, no tocante as orientações do primeiro em relação ao último, bem como a fiscalização do agente se essas orientações estão em consonância ao que dispõe a Lei Geral de Proteção de Dados, não bastando a alegação de que cumpriu ordem superior para excluir sua responsabilidade:

> Aqui vale destacar a relevância de uma elaboração minuciosa e criteriosa do contrato firmado entre controlador e operador, visto que será por meio dele que será possível apurar quais as instruções dadas pelo controlador e eventual direito de regresso entre ambas as partes, a depender do que estava previsto contratualmente. Vale destacar que empresas precisarão revisar os contratos que já possuem nos seus mais diversos setores/prestadores (Recursos Humanos, Marketing etc.) para incluir cláusulas mínimas para compartilhamento de dados entre controlador e operador, de forma a regular essa relação. Nesse sentido, a boa elaboração de um contrato contendo as instruções fornecidas pelo controlador ao operador não exime a responsabilidade deste último de verificar se o que está sendo-lhe instruído obedece às normas sobre a matéria (art. 39, LGPD), não podendo se escusar do cumprimento da lei alegando o cumprimento de ordens ou de cláusulas contratuais. Aqui, o “temor reverencial” em razão da hierarquia/subordinação não é excludente de responsabilidade. (TEIXEIRA, 2021, p. 87)

Por sua vez, o artigo 42, §1º, inciso II, da legislação de proteção de dados preconiza que em havendo uma pluralidade de controladores, todos serão solidariamente responsáveis dos danos decorrentes da atividade de tratamento (BRASIL, 2018).

Sublinha-se que, em ambas as hipóteses de solidariedade, a legislação exceciona as hipóteses do artigo 43, o qual será oportunamente analisado.

Ao que se observa, a responsabilidade dos agentes de tratamento em sede da lei de tratamento de dados foi definida com base no poder decisório tanto do controlador quanto do operador, delimitando a hipóteses casuísticas, e não impondo uma responsabilidade solidária entre os agentes de tratamento em qualquer hipótese, como foi a opção do legislador consumerista em relação aos fornecedores.

Considerando que a LGPD não trouxe previsões específicas no tocante a essa responsabilização solidária, e sim genéricas, e mais uma vez tendo como norte a Teoria do Diálogo de Fontes, aplica-se subsidiariamente as enunciações legais previstas no Código Civil sobre tal modalidade de responsabilidade.

Digno de nota que a previsão de responsabilidade solidária do operador e do controlador trata-se de uma tentativa de proteção mais efetiva ao titular de dados pessoais, em razão de estar-se diante de uma relação de vulnerabilidade entre o titular desses dados e os agentes de tratamento, mormente, do ponto de vista técnico. A previsão tem como norte a função reparadora da responsabilidade civil, visando dar enfoque ao lesado pelo dano, reduzindo ao máximo o número de “vítimas” não ressarcidas.

Essa tentativa de proteção do titular de dados pessoais, em razão da vulnerabilidade existente na relação em tela, se torna ainda mais veemente no art. 42, §2º, que apregoa:

> O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa (BRASIL, 2018).

Levando em consideração serem aplicadas à LGPD as regras processuais dispostas no Código de Processo Civil no tocante à responsabilidade civil, em regra, conforme preceitua o art. 373, do CPC, em seu inciso I (BRASIL, 2015), cabe ao autor, no caso, o titular de dados pessoais e que sofreu o dano, o ônus da prova relativo aos fatos constitutivos de seu direito.

No entanto, semelhantemente ao §1º do art. 373 do CPC, a LGPD traz em seu artigo 42, §2º, uma hipótese de inversão do ônus da prova *ope judices*, dando liberdade ao juiz para inverter o ônus da prova em favor do titular dos dados pessoais quando “for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.” (BRASIL, 2018).

Referida previsão se apresentaria como uma equiparação do titular ao consumidor, considerando sua vulnerabilidade, e materializando-se como uma importante ferramenta para a proteção efetiva dos direitos daqueles (GODINHO, NETO, TÔLEDO, 2020, p. 15). Como lecionam Divino e Lima (2020, p. 15):

> [...] Trata-se de uma tendência determinada por fenômenos interdependentes: de um lado a proteção e defesa dos titulares dos dados e de outro a verificação do excessivo poderio econômico, técnico ou jurídico do controlador ou operador. Em uma situação comum, a vulnerabilidade técnica é a mais verificável, pois os procedimentos

> algorítmicos existentes para realização do tratamento de dados somente podem ser compreendidos por aqueles que o realizam.

Ressalta-se que, não obstante ser uma hipótese de inversão *ope judices,* em casos concretos, há chances ínfimas de o titular de dados pessoais comprovar o ato ilícito do agente de tratamento, sobretudo se tratando de relação por meio eletrônico, levando em consideração a complexidade do tratamento de dados pessoais e a sua veemente vulnerabilidade técnica. Conforme entendimento de Tarcísio Teixeira (2021, p. 90):

> A hipossuficiência do titular de dados se torna facilmente constatável quando se tem uma sociedade permeada pela cultura do Big Data, em que há uma coleta massiva de dados, muitas vezes até desnecessária. Diante dessa realidade, o titular de dados se encontra em uma posição claramente desfavorável, em que beira o impossível saber quais de seus dados estão sendo tratados, de que forma isso tem sido feito e até quem seriam os agentes de tratamento.

Nesse ínterim, infere-se a alta probabilidade de aplicação de referido dispositivo em favor do titular lesado em casos *sob judice*, tendo, na maioria das vezes, os agentes de tratamento superiores capacidades técnicas de demonstrar que não houve tratamento de dados em desrespeito à legislação, em face da hipossuficiência do titular de dados.

A LGPD ainda traz previsão sobre a possibilidade de existência de danos coletivos envolvendo vazamento de dados pessoais. Sobre a matéria, é a lição do texto legal no art. 42, §3º:

> As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. (BRASIL, 2018)

Conforme dispõe o §3º, do artigo 42, é possível que, na hipótese de danos coletivos à titulares de dados pessoais, a ação seja exercida coletivamente em juízo. O dano coletivo pressupõe o prejuízo a valores considerados essenciais para a sociedade, e, a possibilidade de tutela coletiva exprimiria modo mais eficiente em face de possíveis violações da legislação cometidas pelos agentes de tratamento (TEIXEIRA, 2021, p. 90).

Desse modo, segundo Teixeira (2021, p. 90) o Ministério Público, a Defensoria Pública e as denominadas associações de classe seriam legitimadas

para propor medidas judicias visando reparar danos coletivos pela violação de dados em face dos agentes de tratamento, regulando referida previsão pela LGPD, pelo art. 81 do CDC e, sobretudo, pela Lei 7.347/1985 (Lei da Ação Civil Pública).

De todo mais, salienta-se que aludida previsão legal tem como intuito a economia processual. Parte-se da probabilidade de que uma situação de inadequado tratamento de dados pessoais pelos agentes responsáveis não afetará um único titular. Por conseguinte, admite o legislador a possibilidade de que à reparação desses lesados possa ser reivindicada coletivamente em juízo.

Comporta destaque o entendimento Fernando Antônio Tasso (2020, *informação verbal)* no sentido de que a LGPD tratou de forma tímida a possibilidade de ajuizamento de ação coletiva. De acordo com o Magistrado, há grande probabilidade de, em hipóteses de vazamento de dados, essas atingirem inúmeros indivíduos de uma só vez. Se cada titular lesado propuser uma ação relativa ao mesmo vazamento, poderia ocasionar a sobrecarga do Judiciário, sobretudo em comarcas de pequeno porte.

Desse modo, Tasso (2020, *informação verbal*) entende que a tutela coletiva deveria ter sido tratada como prioridade pela legislação, e não como uma mera possibilidade.

Ainda abordando responsabilidade civil dos agentes de tratamento, preconiza o artigo 42, §4º da legislação discutida que: “Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.” (BRASIL, 2018).

Nos termos das lições de Tarcísio Teixeira (2021, p. 87), como consequência da responsabilidade solidária entre controladores e operadores de dados pessoais prevista no art. 42, §1º, incisos I e II, a própria LGPD traz especificamente a previsão quanto à possibilidade de ação de regresso por aquele que respondeu em juízo pela responsabilidade em face demais responsáveis, de acordo com o grau de participação desses no evento danoso, a ser apurado no caso concreto.

Trata-se de uma exceção à regra geral da responsabilidade civil que se avalia pela extensão do dano, nos termos do art. 944 do Código Civil (BRASIL, 2002).

Dispositivo de grande relevância sobre o tema é o art. 43, da LGPD, que elenca as hipóteses de exclusão de responsabilidade, *in verbis*:

> Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.
> (BRASIL, 2018)

O art. 43, a exemplo e com redação inspirada no art. 14, §1º, do Código de Defesa do Consumidor, traz possíveis matérias de defesa a serem alegadas pelos agentes de tratamento ao serem demandados em juízos, em vista de trazerem as hipóteses em que esses agentes não serão responsabilizados pelo vazamento de dados pessoais de terceiros (excludentes de responsabilidade).

A primeira hipótese elencada trata da exclusão da responsabilidade pela comprovação pelos agentes de tratamento de que não realizaram o tratamento de dados pessoais do qual decorreu o dano ao titular. Conforme ensina Bruno Miragem (2021, p. 497):

> A hipótese de demonstrar que não realizaram o tratamento de dados que lhes é atribuído compreende o afastamento daquele determinado controlador ou operador de qualquer atividade de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados, que tenha dado causa ao dano sofrido pelo titular.

Em continuidade, o incido II do artigo em questão preceitua que também não serão responsabilizados os agentes de tratamento que embora assumam que tenham realizado o tratamento de dados pessoais, comprovem que em nenhum momento violaram a Lei Geral de Proteção de Dados. Sobre a norma em discussão, digno de merecimento as explicações de Bruno Miragem (2021, p. 497):

> No caso do inciso II do art. 43, trata-se da demonstração de atuação lícita do controlador ou operador de dados, independentemente da existência de algum prejuízo alegado pelo titular. Neste caso, merece destaque a norma do art. 7º da LGPD que dispõe sobre as hipóteses em que há permissão legal para a realização do tratamento de dados. Conforme já foi mencionado, a existência de consentimento do titular dos dados é o critério dominante (inciso I). Contudo, diversas outras hipóteses permitem a realização do tratamento. Nestes casos, deverão ser observados, especialmente, os princípios da finalidade, da adequação e da necessidade, previstos no art. 6º da LGPD. Por finalidade, define-se a “realização do

> tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (art. 6º, I); adequação, por sua vez, compreende a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (art. 6º, II); necessidade será a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (art. 6º, III).

Observa-se que na hipótese do inciso II, o agente de tratamento de dados, conforme preconiza Miragem (2021, p. 497), demonstra sua atuação lícita no tratamento de dados pessoais, pois essa se deu dentro das hipóteses permissivas de realização de tratamento de dados previstas no art. 7º da legislação de proteção de dados brasileiras. Cabe salientar, todavia, que, como será oportunamente exposto, existem posições doutrinárias apontando referida previsão como uma cláusula de culpa presumida na LGPD.

Por final, o art. 43 relaciona a última previsão quanto à exclusão de responsabilidade dos agentes de tratamento, que ocorre quando esses demonstram a culpa exclusiva do titular dos dados pessoais ou de terceiro. Comporta pontuar que em caso de culpa concorrente da vítima ou de terceiro, ainda subsistirá a responsabilidade do agente de tratamentos:

> Frise-se que se houver culpa "concorrente" da vítima ou de terceiro ainda assim o controlador ou operador será responsável pelo dano. Nesse caso, havendo culpa concorrente da vítima, é aplicável a regra do art. 945 do CC ao estabelecer que a indenização deve ser fixada considerando a gravidade da culpa da vítima em confronto com a do autor do dano. Ou seja, a culpa concorrente não afasta a responsabilidade do controlador ou do operador, apenas pode atenuar o valor da indenização. (TEIXEIRA, 2021, p. 88)

Cabe enfatizar que, conforme leitura do próprio dispositivo, nas três hipóteses, independente da inversão do ônus da prova *ope judices* prevista no art. 42, §2º da LGPD, trata-se primordialmente de adequação legal ao art. 373, inciso II, do Código de Processo Civil, cabendo ao(s) réu(s), ora agentes de tratamento, provarem o fato impeditivo, modificativo, ou extintivo do direito do autor (titular dos dados pessoais).

Dessa forma, indubitavelmente, as matérias de defesa dos agentes de tratamento elencadas no art. 43 fixam o ônus da prova para os controladores e operadores de dados pessoais.

Em continuidade à regulação da responsabilidade civil, aborda o art. 44 da LGPD:

> O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. (BRASIL, 2018)

Notadamente, o art. 44 é, em parte, uma inspiração do art. 14, §1º do Código de Defesa do Consumidor, e esclarece as hipóteses em que o tratamento de dados é considerando irregular, seja pela violação das disposições da LGPD, ou por não fornecer ao titular a proteção aos seus dados pessoais que razoavelmente se esperava, de acordo com os critérios elencados pelo dispositivo.

O parágrafo único, por sua vez, estabelece o “dever de indenizar derivado da violação de normas técnicas oriundas da autoridade nacional de proteção de dados (ANPD)[...]” (NOVAKOSKI; NASPOLINI, 2020, p. 163).

Assim a análise do dever de segurança e atuação diligente será norteador do dever de indenizar, de modo a se verificar no caso concreto se a atuação dos agentes de tratamento para obstar a ocorrência do dano ocorreu de modo satisfatório ou não (SANTOS, 2021, p.15).

Salienta-se que a análise do dever de segurança nos termos do artigo 44 da LGPD deve ser realizado considerando a velocidade do desenvolvimento tecnológico a época do tratamento de dados:

> [...] Isso é especialmente relevante considerando a grande velocidade do desenvolvimento da tecnologia no tratamento de dados, e os riscos inerentes, em especial as situações de vazamento e acesso não autorizado de terceiros aos dados armazenados pelo controlador ou pelo operador. Nestas hipóteses trata-se de definir em relação ao controlador e operador dos dados, se seria possível identificar um dever de atualização técnica imputável, e nestes termos, eventual adoção de novas técnicas que permitam o uso indevido do dado, especialmente por terceiros, venha a caracterizar espécie de risco inerente (fortuito interno), que não exclui sua responsabilidade pelos danos que venham a suportar os titulares dos dados; ou se delimitação quanto às técnicas disponíveis à época em que foi realizado o tratamento exclui eventual responsabilização do controlador e do operador pelo desenvolvimento tecnológico que permita obtenção de dados ou tratamento indevido por terceiros, desviado da finalidade originalmente prevista. (MIRAGEM, 2019, p.26)

Em consonância com o entendimento firmado acima, constata-se que um dos parâmetros para o juiz analisar e fixar o dever de indenizar consiste na

análise do juízo de reprovabilidade da conduta do agente de tratamento, em acordo com o disposto no art. 44 da LPGD, o que, segundo Santos (2021, p.15) não pode implicar na objetivação da responsabilidade civil.

Por derradeiro, é a lição do art. 45 da Legislação de Proteção de Dados Pessoais: “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”. (BRASIL, 2018)

Nota-se que a LGPD enfatizou a aplicação da legislação específica às relações de consumo no tangente à responsabilidade civil pela violação dos deveres fixados, qual seja, o Código de Defesa do Consumidor.

Contudo, considerando o aumento exponencial do comércio eletrônico nos últimos anos, o estudo quanto à responsabilidade civil dos fornecedores no comércio eletrônicos pelo vazamento de dados não pode ser resumido numa disposição que preconiza que nesses casos, as relações ficam “sujeitas às regras de responsabilidade previstas na legislação pertinente” (BRASIL, 2018).

Como já pontuado nesse trabalho, o ordenamento jurídico brasileiro não deve ser interpretado de forma a uma norma excluir a outra, mas sim como um sistema.

Isto posto, a responsabilidade civil pelo vazamento de dados pessoais de consumidores no comércio eletrônico não deve ser interpretada exclusivamente a partir do Código de Defesa do Consumidor, mas em sintonia e complementariedade com a LGPD, nos termos da Teoria do Diálogo de Fontes.

Diante da complexidade desse tema, há que ser reservado um tópico específico para essa análise, a ser feita em momento oportuno. Antes, imprescindível trazer à lume os pressupostos para caracterização do dever de responsabilização na LGPD.

3.2. Pressupostos da Responsabilidade Civil na LGPD

Nos termos do que já foi explanado no presente trabalho, a LGPD abordou de forma sucinta o tema relativo à responsabilidade civil, cabendo ao aplicador do Direito realizar uma interpretação sistemática da legislação com o ordenamento jurídico vigente.

Nessa interpretação sistemática, digno de importância a análise dos pressupostos caracterizadores da responsabilidade civil extracontratual em um caso concreto, debatidos em sede doutrinária, e transpostos para a Legislação de Proteção de Dados pessoais nessa pesquisa.

Não se pode ignorar as divergências existentes na doutrina pátria no tocante a tais pressupostos. No entanto, no presente trabalho, visando não adentrar em tais divergências, adota-se como referencial para a análise dos pressupostos na LGPD a teoria tetrapartida abordada por Nelsol Rosenvand, Cristiano Chavez Farias e Felipe Braga Netto (2019, p. 187):

> Optamos assim por uma classificação tetrapartida dos pressupostos da responsabilidade civil, cujos elementos são: (a) ato ilícito; (b) culpa; (c) dano; (d) nexo causal. Aliás, não é outro o resultado que se alcança ao compulsarmos o art. 927, caput, do Código Civil – dispositivo introdutório ao Título dedicado à responsabilidade civil:
> "Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo"

Parte-se em tal divisão da responsabilidade subjetiva como regra do ordenamento jurídico brasileiro. Todavia, considerando ser o elemento "culpa" dispensado na responsabilidade objetiva, esse será minuciosamente analisado, em subtópico específico, no tocante à sua necessidade (ou não) para configuração da responsabilidade civil na LGPD. Isto é, será analisado se o elemento "culpa" se configura de fato como pressuposto da responsabilidade civil na LGPD, reconhecendo-se a presença de uma responsabilidade subjetiva na legislação, ou se esta é norteada pelo elemento risco, pairando sobre a LGPD a responsabilidade objetiva.

3.2.1. Ato ilícito

O ato ilícito, de maneira genérica, se refere à ação ou omissão humana que dá ensejo ao dano, passível de responsabilização civil. De acordo com Rosenvald, Farias e Braga Netto (2019, p. 198 e 199), o ato ilícito é um fato jurídico, com potencial para produzir efeitos jurídicos, *in casu*, contrários ao ordenamento jurídico. Segundo os doutrinadores, o ato ilícito teria dois atributos: a antijuricidade e a imputabilidade.

A antijuridicidade, elemento objetivo do ato ilícito, configura-se pela contrariedade a lei. Como definem Rosenvald, Farias e Braga Netto (2019, p.189): “O comportamento antijurídico se instala no momento em que o agente ofende o dever genérico e absoluto de não ofender, sem consentimento, a esfera jurídica alheia[...].”

A imputabilidade, elemento subjetivo, por sua vez, remeteria ao imputável, definido pelos autores como “aquela pessoa a quem se pode legitimamente atribuir um comportamento antijurídico” (ROSELVAND; FARIAS; NETTO; 2019, p.190 e 191).

Trazendo tal conceituação para a Lei Geral de Proteção de Dados, infere-se que o ato ilícito estaria presente nas hipóteses de violação ao disposto no ordenamento jurídico, partindo do preconizado no art. 42, da LGPD, como cláusula geral do dever de indenizar.

Em outros termos, a antijuridicidade do ato ilícito sedimenta-se pela contrariedade ao sistema norteador da LGPD, incluindo as normas e princípios que orientam a atividade de tratamento de dados, sobretudo diante da violação ao direito fundamental de privacidade e proteção de dados.

Nesse sentido, digno transcrever o ensinamento de Novakoski e Naspolini (2020, p.161):

> Uma vez em posse (legítima e consentida) dos dados pessoais gerais ou sensíveis (art. 5º, I e II, LGPD), o controlador ou operador do banco de dados poderá tratá-los livremente (art. 5º, X, LGPD), observando os princípios e limites estabelecidos pela legislação e regulação oriunda da autoridade nacional de proteção de dados (ANPD) (art. 6º, I a X; art. 46, LGPD), sob pena de incorrer em responsabilidade civil.

Como pontuam Novaroski e Naspolini, o tratamento de dados deve seguir os princípios e limites estabelecidos pela legislação. Avançando nessa lógica, depreende-se que toda vez que o agente de tratamento violar o direito fundamental de proteção de dados pessoais do titular, ou agir em desacordo com a LGPD, sobretudo nos termos do que é preceituado no art. 44, da legislação, restará presente o ato ilícito, podendo este dar ensejo à responsabilidade civil, se presentes os demais elementos.

A LGPD elenca os princípios vetores da atividade de tratamento de dados pessoais em seu art. 6º, a saber: princípio da boa- fé; princípio da finalidade;

princípio da adequação; princípio da necessidade; princípio do livre acesso; princípio da qualidade dos dados; princípio da transparência; princípio da segurança; princípio da prevenção; princípio da não discriminação; e princípio da responsabilização e prestação de contas. (BRASIL, 2018)

Toda vez que o operador de dados pessoais age em desrespeito a tais princípios, comete ato ilícito, sendo possível ser responsabilizado civilmente, desde que presentes os demais pressupostos para configurar a responsabilidade.

Enfatiza-se, neste ponto, a importância dos vetores interpretativos fixados no tópico “2.4” desta pesquisa, quando do estudo de julgados do Tribunal de Justiça da União Europeia, verificou a “necessidade” e “finalidade” como parâmetros balizadores para configuração do ato ilícito.

À título de exemplo, menciona-se a situação em que um agente de tratamentos que, no âmbito do *e-commerce*, realize a coleta de dados além dos imprescindíveis para a realização de uma transação comercial, com a finalidade de formar um banco de dados de seus consumidores. Sem sombra de dúvidas, estar-se-á figurado um ato ilícito.

Outrossim, também estará presente o ato ilícito na violação de qualquer dispositivo da Lei Geral de Proteção de Dados, ou mesmo, da violação ao direito da privacidade e de proteção de dados pessoais, protegidos constitucionalmente.

Relativamente à imputabilidade, destaca-se que o agente do ato ilícito será o denominado pela LGPD como “agente de tratamento”. Em razão da complexidade de referida atividade, geralmente, esses serão imputáveis, não havendo divergências que produzam efeitos relevantes nesse sentido.

3.2.2. Do elemento dano

Segundo sustentam Rosenvald, Farias e Netto (2019, p. 293), o dano seria o elemento que desencadeia a responsabilidade civil, ensejando o mecanismo ressarcitório, e podendo assumir formas diferenciadas.

Como pontuam os autores, o Brasil adotaria um sistema aberto quanto ao dano, não o restringindo a possibilidades casuísticas, através de um *numerus clausus*, como o fez legislações alienígenas. Desta feita, a opção do legislador brasileiro ocasionaria “[...] um alargamento das possibilidades de identificação de

hipóteses de interesses dignos de proteção” (ROSENVALD; FARIAS; NETTO, 2019, p. 297)

O artigo 42 da LGPD traz dentro da cláusula de responsabilidade a imprescindibilidade do dano, resultante da atividade de tratamento de dados pessoais, admitindo o legislador ser esse de natureza individual ou coletiva, patrimonial ou extrapatrimonial (BRASIL, 2018).

Nos termos do que já pontuado no presente trabalho, além da possibilidade de tutela individual do direito à proteção de dados pessoais, regra no sistema da responsabilidade civil, foi admitido na LGPD o direito à demanda judicial coletiva em face de possíveis violações, reconhecendo o legislador que, nessas hipóteses, em suma maioria, a violação de direitos dos titulares não ocorrerá de forma isolada, mas em massa.

Superada essa pontuação, merece ponderações a análise atinente aos danos patrimoniais e extrapatrimoniais.

Quanto ao dano patrimonial, ensinam Rosenvald, Farias e Netto (2019, p. 346) que a indenização deve englobar tanto o dano emergente, caracterizado pela perda material efetiva da vítima, quanto os lucros cessantes, sedimentado no que a vítima, segundo “o curso normal das coisas” teria deixado de obter, coadunando- se com a redação do art. 402 do Código Civil (BRASIL, 2002)

A fim de melhor elucidação, exemplo que se coloca da configuração de danos de caráter patrimonial concerne a um indivíduo que é lesado pelo vazamento de seus dados pessoais sensíveis, fato que o prejudica diretamente na contratação de um emprego. Se demonstrado o nexo de causalidade entre o ato ilícito imputado ao agente de dados pessoais com a comprovação de dano efetivo ocasionado pelo ilícito do vazamento, mostra-se possível a indenização desse indivíduo na perspectiva dos lucros cessantes.

Em vista do exposto, em sendo hipótese de dano patrimonial, cabe, como regra, ao lesionado constituir prova sobre referido dano, lógica esta que rege o Sistema de Responsabilidade Civil, não remanescendo consideráveis dúvidas a respeito.

Questão que se coloca em discussão é pertinente aos danos extrapatrimoniais, exteriorizados como o conhecido e constitucionalmente previsto dano moral. Sem ignorar as divergências pontuadas por determinados doutrinadores, relativas a possíveis diferenças entre os danos citados, no presente

trabalho, adota-se as terminologias como sinônimas, considerando as próprias obras tomadas como referência nesta pesquisa.

Em face do reconhecimento nas últimas décadas pelos tribunais brasileiros de hipóteses excepcionais de *dano in res ipsa*, a doutrina tem discutido se o dano moral/extrapatrimonial tratado pela LGPD se amoldaria na sistemática dessa prova presumida.

Por conseguinte, torna-se importante ponderar sobre as delimitações envolvendo o dano moral *in res ipsa*.

De acordo com Hellman (2019, p. 04), o dano moral *in res ipsa*, decorre de uma presunção judicial em razão da complexidade de se determinar, muitas vezes, o abalo psicológico gerado pela lesão ocasionada funcionando como hipótese excepcional no Ordenamento Jurídico Brasileiro.

Segundo entendimento de Caitlin Sampaio Mulholland (2021, informação verbal), o dano decorrente da LPGD sempre será moral, e, eventualmente, patrimonial.

Diante desse critério de dano exposto pela LPGD, a professora apresenta críticas em razão da suposta problemática na qualificação e identificação de um dano no âmbito da legislação. De acordo com o que pontua Mulholland (2021, informação verbal), a comprovação de um dano deve estar relacionada a uma perda patrimonial ou um desvalor psíquico, e no caso de “danos aos dados”, a prova desse desvalor seria ínfima. Nesse seguimento, para a professora, o dano moral se caracterizaria pela violação de um interesse existencial, assim, qualquer situação em que houvesse a violação de um direito fundamental, haveria dano moral, e, portanto, referido dano deveria ser reconhecido *in res ipsa*.

Todavia, definir o dano moral na LGPD como de difícil identificação e comprovação, e reconhecê-lo como *in res ipsa*, demonstra-se arriscado, sobretudo considerando a própria problemática que circunda o dano moral, a qual merece ser analisada.

Nas últimas décadas, um dos temas que mais geram posicionamentos divergentes no âmbito doutrinário e jurisprudencial no estudo da responsabilidade civil brasileira é a temática de danos morais, sobretudo envolvendo seu conceito, função e valoração. Fato é que, até o presente momento, doutrina e jurisprudência distanciam-se de uma uniformização de entendimento.

Como leciona Maria Celina Bodin de Moraes (2019, p. 02), com a Carta Magna de 1988, a responsabilidade civil, sobretudo na nuance da reparação do dano moral, revelou-se de grande importância para proteção de direitos fundamentais da pessoa humana no ordenamento jurídico brasileiro. Contudo, na contramão, a identificação e qualificação desse dano teria aberto um vultoso campo de arbitrariedade judicial.

Não bastante referidas arbitrariedades jurisprudenciais na sistemática do dano moral, esse tem tido seu sentido desvirtuado, de modo que, não raras as vezes, indivíduos, valendo-se da má-fé, utilizam do Judiciário como uma loteria, visando obter um possível enriquecimento em face de um suposto dano moral:

> O sistema, tal como é, não apenas permite, mas incentiva fortemente a má-fé e o lucro fácil: se não se sabe, nem se tem como ter ideia de quanto se irá receber, e se se sabe que, considerando o que normalmente acontece, se ganhará alguma coisa, talvez até, com sorte, uma quantia significativa, por que não ingressar com a ação, principalmente quando se usufrui, como ocorre na maioria dos casos, do benefício da justiça gratuita? As vítimas e seus advogados só têm a ganhar, enquanto os juízos e os tribunais se abarrotam, vindo assim a prejudicar a prestação jurisdicional oferecida à sociedade como um todo. (MORAES, 2019, p. 04)

Esse desvirtuamento do dano moral ganha espaço diante da dificuldade em se chegar à conceituação de referida espécie de dano, o qual, majoritariamente, é relacionado a sentimentos subjetivos abstratos, materializados na dor e no sofrimento:

> [...] Ao adotar-se a posição de que o dano moral é “o sentimento de dor, vexame e humilhação(causado injustamente a alguém)”, como hoje é sustentado nos tribunais do País, a jurisprudência tem se mostrado vacilante e confusa, seja no que toca à identificação do dano, seja, em consequência, no que se refere, à sua avaliação.[...] (MORAES, 2003, p. 45 e 46)

Por esse raciocínio, Bodin de Moraes (2019, p. 11) aponta que diante da situação de indefinição de dano moral, este não poderia ser atribuído ao sofrimento humano, deixando a identificação deste sofrimento à livre interpretação do magistrado, como vem ocorrendo. Dessa forma, a qualificação e identificação de citado dano deveria ser determinado com certo grau de tecnicidade. Essa tecnicidade, de acordo com a professora, estaria relacionada à análise do dano moral sob a perspectiva de garantias e direitos fundamentais constitucionalmente previstos, norteando-se pela dignidade da pessoa humana:

> A reparação do dano moral corresponde, no ambiente de constitucionalização em que vivemos à contrapartida do princípio da dignidade humana: é o reverso da medalha. Quando a dignidade é ofendida, há que se reparar o dano injustamente sofrido. (MORAES, 2019, p. 15).

A tecnicidade atribuída por Bodin de Moraes (2019, p. 15) aos danos morais, relacionando-os à violação de direitos fundamentais, certamente, é um grande avanço diante das imprecisões conceituais existentes.

No entanto, referida tese deve ser analisada com cautela, pois não transparece prudente afirmar que a mera violação de um direito fundamental, sem qualquer potencialidade lesiva à vítima, ensejaria um dano moral, e, portanto, a este seria dispensado prova, sendo considerado *in res ipsa.*

Se assim o fosse, pelo fato de ser o direito à proteção de dados pessoais elencado constitucionalmente no artigo 5º, inciso LXXIX (BRASIL, 2022), em havendo vazamento de dados pessoais de um titular, sem qualquer possibilidade de potencialidade lesiva a ele, por si só, ensejaria o dano moral, visto que esse seria *in res ipsa*.

Aludido entendimento vai na contramão ao vetor interpretativo fixado no tópico “2.4” da presente pesquisa, a partir de análise de julgado do Tribunal de Justiça da União Europeia (UNIÃO EUROPEIA, 2021, p. 48), no qual restou consignado que a mera violação de um direito não culminaria em obrigatório prejuízo à parte.

Sob essa perspectiva, considerar como regra a desnecessidade da prova do dano moral na LGPD, além de romper com a excepcionalidade atribuída ao dano *in res ipsa*, desemboca no problema inicialmente discutido pela própria professora Bodin de Moraes (2019, p. 15): o desvirtuamento do dano moral, sendo este utilizado como fundamento para ações de má-fé que transformam o Judiciário em uma loteria.

Seguindo por esse sentido, merece dar destaque aos apontamentos de Humberto Theodoro Jr. (2016, p. 06), que preconiza que a vida em sociedade pressupõe direitos e deveres de caráter jurídicos, éticos e sociais, o que, fatalmente gera conflitos e aborrecimentos, os quais podem ensejar abalos psicológicos, e até mesmo, efetivos danos. Entretanto, para a configuração do dever de indenizar, não

se mostraria razoável a simples demonstração de dor, mas sim de todos os elementos da responsabilidade civil (dano, ilicitude e nexo causal).

Nessa toada, para a configuração do dano moral, imprescindível seria, se, de acordo com um juízo de razoabilidade, houvesse ao menos a presunção de um prejuízo grave, e não insignificantes pretensões. De acordo com o processualista:

> [...] Para que se considere ilícito o ato que o ofendido tem como desonroso é necessário que, segundo um juízo de razoabilidade, autorize a presunção de prejuízo grave, de modo que “pequenos melindres”, insuficientes para ofender os bens jurídicos, não devem ser motivo de processo judicial. [...] (THEODORO JÚNIOR, 2016, p. 06)

Segundo Theodoro Júnior (2016, p. 115), o dano moral decorreria de uma lesão ao plano psíquico do ofendido, o que se mostraria como terreno onde a pesquisa probatória não poderia chegar. Contudo, isso não significaria que a vítima poderia obter reparação pela simples afirmação de ter suportado dano moral, considerando ser o ato danoso integrante da causa de pedir, e, portanto, ônus da prova do autor:

> Na verdade, o que não se prova é a dor moral, porque se passa na esfera subjetiva do ofendido, onde a pesquisa probatória não tem como alcançar. O dano, porém, objetivamente, atinge um direito da personalidade, que exteriormente pode ser detectado e cuja ofensa pode ser evidenciada, indiferentemente da penetração do psiquismo da vítima. (THEODORO JÚNIOR, 2016, p.115)

Nesse seguimento, o processualista entende que deve o autor provar a gravidade da ofensa ao direito da personalidade, de modo que o dano será analisado exteriormente: “[...] a vítima não pode deixar de provar que um direito ligado à sua personalidade foi realmente ofendido, de maneira grave e ilícita.” (THEODORO JÚNIOR, 2016, p. 117)

Realizando uma interpretação sistemática das ponderações de Maria Celina Bodin de Moraes e Humberto Theodoro Júnior, infere-se que a configuração do dano moral não estaria relacionada à prova da dor ou sofrimento, visto que esses sentimentos se passariam no plano subjetivo do indivíduo.

Todavia, isso não denotaria a dispensabilidade da produção de prova na perspectiva dano moral. O dano moral estaria relacionado à violação de direitos fundamentais, sendo cabível a constituição de prova, ao menos, das consequências responsáveis por gerar o potencial prejuízo grave psíquico causado ao indivíduo.

Isto é, tanto a violação de direitos fundamentais, quanto o prejuízo grave, seja efetivo ou potencial, de referida violação, deveriam ser demonstrados, a partir de um juízo de razoabilidade.

Vale elucidar que aludida presunção não se refere ao dano, mas sim ao potencial prejuízo psíquico à vítima, cabendo a esta demonstrar, como regra, as consequências do ato ilícito, a partir das quais se presume o potencial abalo psicológico. Diferentemente, no dano moral *in res ipsa*, as próprias consequências do ato ilícito seriam presumidas.

Adaptando essa análise conclusiva ao exemplo citado no início deste subtópico, imaginemos que um indivíduo, em razão do vazamento de seus dados pessoais por seu antigo empregador (ainda que dados não sensíveis), não consegue uma nova vaga de emprego em outra empresa, permanecendo por longo período desempregado. Aqui, para configuração do dano moral, cabe ser demonstrado, de forma cabal, as consequências geradas pelo vazamento de dados pessoais, como, por exemplo, o desemprego, a hipossuficiência de recursos financeiros para prover a própria família.

Nesse caso, ato ilícito de vazamento de dados pessoais cometido pelo empregador culminou em consequências, as quais devem ser provadas, e a partir dessas consequências, observa-se o potencial abalo psicológico sofrido, uma vez que este, por ser subjetivo, não pode ser demonstrado objetivamente.

Por sua vez, nas hipóteses excepcionalíssimas de violação ao direito fundamental em que o potencial prejuízo psíquico ao indivíduo mostrar-se evidente, independente da demonstração das consequências, esse dano seria *in res ipsa*, dispensando-se constituição de prova.

Suponhamos o vazamento de um dado pessoal responsável por noticiar que um indivíduo é um portador de AIDS, sem que houvesse sua devida permissão para tanto. Não é necessário demonstrar as consequências desse vazamento, a fim de depreender o abalo psicológico. É evidente o abalo sofrido pelo titular desse dado por seu simples vazamento, configurando, portanto, um dano moral presumido decorrente da violação de um dado pessoal sensível.

Denota-se, por esse raciocínio, que a mera violação de um direito fundamental não ensejaria por si só, dano moral, sendo imprescindível a constituição de prova no sentido de que essa violação gerou consequências capazes de criar, ao menos, potencial prejuízo grave psíquico ao indivíduo lesado. O dano *in res ipsa* só

estaria presente nas hipóteses que, diante das circunstâncias casuísticas, tornou-se latente referido prejuízo psíquico causado ao indivíduo, dispensando-se prova em relação às consequências geradas pelo ato ilícito.

Aplicando-se esse raciocínio no âmbito da LGPD, verifica-se que o dano extrapatrimonial não se materializaria pela simples insubordinação à lei e consequente violação ao direito fundamental de proteção de dados pessoais, mas sim quando diante dessa violação, o autor constituísse prova, no mínimo das consequências responsáveis por culminar em potencial prejuízo psíquico grave que sofreu, bem como do nexo de causalidade existente entre esse dano e a violação da lei. Entendimento contrário, como já salientado, potencializaria o desvirtuamento da função do dano moral.

Inclusive, em recentes casos julgados pelo Tribunal de Justiça de São Paulo, este tem firmado entendimento pacífico quanto à necessidade de prova do dano moral sofrido em ações tendo como causa de pedir próxima a Legislação de Proteção de Dados, de modo que o mero vazamento de dados não ensejaria por si só direito à reparação.

Conforme posicionamento jurisprudencial firmado na Apelação Cível nº 1014245-32.2019.8.26.0196, a 27ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo (SÃO PAULO, 2021), no julgamento de um caso no qual haveria ocorrido a inserção dos dados pessoais do apelante em um site administrado pela parte apelada, entendeu que a configuração de dano moral no âmbito da LGPD dependeria de “prova segura”, não se figurando, no caso dos autos, como *in res ipsa*:

> AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. Responsabilidade civil objetiva extracontratual. Lei Geral de Proteção de Dados – LGPD. Autor que reclama prejuízo moral em razão de inserção de seus dados pessoais em "site" administrado pela ré, passando a receber ligações indevidas. SENTENÇA de improcedência. APELAÇÃO do autor, que insiste no acolhimento do pedido inicial. EXAME: Pressupostos da responsabilização civil que consistem em ato ou conduta humana, nexo de causalidade e dano. Ausência de prova segura quanto ao dano e ao nexo de causalidade. Dano moral que no caso dos autos não se constitui "in re ipsa". Sentença mantida. RECURSO NÃO PROVIDO.(TJSP; Apelação Cível 1014245-32.2019.8.26.0196; Relator (a): Daise Fajardo Nogueira Jacot; Órgão Julgador: 27ª Câmara de Direito Privado; Foro de Franca - 4ª Vara Cível; Data do Julgamento: 26/11/2021; Data de Registro: 26/11/2021)

No mesmo sentido, na análise da Apelação Civil nº 1000641-85.2021.8.26.0405, referentes à relação consumerista consistente na prestação de

serviços de energia elétrica, a 33ª Câmara de Direito Privado de citado Tribunal entendeu pela improcedência da pretensão indenizatória de danos morais ajuizadas por um consumidor, cuja causa de pedir pautava-se “[...] prejuízo potencial advindo do receio de uso futuro dos dados do consumidor em eventuais fraudes no comércio [...]” (SÃO PAULO, 2021), entendendo que aludida situação não era capaz de ensejar dano moral. Conforme julgado:

> PRESTAÇÃO DE SERVIÇOS – Energia elétrica – Pretensão indenizatória de dano moral julgada improcedente – Vazamento de dados pessoais dos consumidores – Pretensão escorada em situações hipotéticas, prejuízo potencial advindo do receio de uso futuro dos dados do consumidor em eventuais fraudes no comércio – Situação inapta a autorizar reparação – Apelação não provida. (TJSP; Apelação Cível 1000641-85.2021.8.26.0405; Relator (a): Sá Duarte; Órgão Julgador: 33ª Câmara de Direito Privado; Foro de Osasco - 8ª Vara Cível; Data do Julgamento: 29/11/2021; Data de Registro: 30/11/2021)

Colacionados julgados demonstram que o dano moral não irá se consubstanciar a partir de uma situação hipotética de prejuízo, confirmando a tese quanto à necessidade, em regra, da demonstração das consequências geradas pelo ato ilícito, em relação às quais, em determinados casos, pode se inferir o potencial abalo moral sofrido.

Ressalta-se, nessa perspectiva, que no julgamento da Apelação Civil nº 1001032-45.2021.8.26.0177, a 23 ª Turma do TJSP deixou implícito no julgado que a possibilidade de configuração de danos morais *in res ipsa* tenderá a estar relacionada com o tratamento inadequado de dados pessoais sensíveis, senão vejamos:

> Ação de obrigação de fazer c.c. indenização por danos morais. Vazamento de dados pessoais. Sentença de improcedência. Apelação do autor. Vazamento de dados pessoais. Falha na prestação de serviço. Dever da empresa de adotar medidas de segurança visando à proteção de dados pessoais do consumidor. Inteligência do artigo 46 da Lei Geral de Proteção de Dados (Lei n. º 13.709/2018). Danos morais não verificados. Vazamento de dados que não ensejou dano efetivo ao requerente. Dados vazados que não estão abrangidos no conceito de dado pessoal sensível (art. 5º, II, da LGPD). Ausência de prova acerca da utilização dos dados vazados e do efetivo dano. Dano hipotético não enseja indenização. Precedentes do TJSP. Sentença mantida. Honorários majorados. Recurso desprovido. (TJSP; Apelação Cível 1001032-45.2021.8.26.0177; Relator (a): Virgilio de Oliveira Junior; Órgão Julgador: 23ª Câmara de Direito Privado; Foro de Embu-Guaçu - Vara Única; Data do Julgamento: 01/12/2021; Data de Registro: 03/12/2021)

A partir da análise doutrinária e jurisprudencial trazida à cena, não parece razoável considerar o dano extrapatrimonial de difícil identificação e qualificação.

Sobre o risco de desvirtuamento da própria responsabilidade civil, infere-se que não se deve partir da premissa que o dano moral em sede de LGPD seria *in res ipsa*, sob justificativa da violação do direito fundamental da proteção de dados.

Assim, faz-se indispensável a prova quanto às consequências do ato ilícito, em relação às quais se infere ao menos potencial prejuízo grave àquele que supostamente sofreu a violação de seus dados pessoais. Nessa toada, nos termos do posicionamento do Egrégio Tribunal de Justiça do Estado de São Paulo, cabe ao autor constituir prova do dano moral sofrido, do ponto de vista externo (consequências do ato ilícito capazes de ensejam o abalo grave psicológico), e do nexo de causalidade desse com a violação da LGPD.

Sem embargo, não é razoável afastar totalmente a possibilidade de reconhecimento de um dano *in res ipsa* em demanda tendo como fundamento jurídico a LGPD.

Em se tratando de hipótese casuística em que, pelas circunstâncias do caso concreto, é latente o prejuízo psicológico sofrido, o dano *in res ipsa* pode ser admitido pelo Judiciário, dispensando-se prova a seu respeito. Nesse sentido, ganha destaque o aumento da probabilidade de reconhecimento de um dano *in res ipsa* em circunstâncias de vazamento de dados sensíveis, considerando uma situação de evidente discriminação decorrente da divulgação de referido dado, consoante entendimento fixado no último julgado colacionado.

3.2.3. Do nexo de causalidade

O nexo de causalidade configura pressuposto abstrato da responsabilidade civil, mas de extrema importância, pois estabelece, em termos genéricos, a relação de causalidade existente entre a conduta antijurídica e o dano, seja ele provado ou *in res ipsa*. Conforme preceituam Rosenvald, Chavez Farias e Braga Netto (2019, p. 556), o nexo causal teria duas funções:

> No setor da responsabilidade civil, o nexo causal exercita duas funções: a primeira (e primordial) é a de conferir a obrigação de indenizar aquele cujo

> comportamento foi a causa eficiente para a produção do dano. Imputa-se juridicamente as consequências de um evento lesivo a quem os produziu (seja pela culpa ou risco, conforme a teoria que se adote). A seu turno, a segunda função será a de determinar a extensão desse dano, a medida de sua reparação. Ou seja, pela relação da causalidade seremos capazes de determinar quem repara o dano e quais os efeitos danosos que serão reparados. [...]

Seguindo essa lógica, os doutrinadores supracitados ensinam que em razão da complexidade existente na sociedade hodierna, na qual as causas relativas aos danos se tornam de difícil identificação, o nexo de causalidade, sobretudo na teoria objetiva, será analisado sob um viés jurídico, e não físico. Isto é, "[...]não resultará propriamente de um liame entre o dano e um fato, mas sim entre o evento lesivo e o fator de atribuição previamente selecionado pelo legislador." (ROSELVAND; FARIAS; NETTO, 2019, p. 556)

Nos termos citados, o nexo de causalidade estará presente em uma relação regida pela LGPD quando a atividade de tratamento de dados pessoais, realizada pelos agentes de tratamento em contramão ao apregoado pela legislação e ao dever de segurança imposta, guardar relação da causalidade com o dano ocasionado ao titular de dados pessoais.

Em que pese a discussão existente quanto à natureza do art. 43, em seu inciso II (BRASIL, 2018), fato uníssono é a previsão do mesmo artigo, nos incisos I e II, de hipóteses de rompimento do nexo de causalidade. Situações em que, não obstante a existência do dano, este não é causa direta da atividade de tratamento de dados pessoais.

Assim sendo, preconiza o artigo citado que os agentes de tratamento só não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais, que lhes é atribuído; que, mesmo tendo realizado referido tratamento, não houve qualquer violação à LGPD; ou ainda utilizar como defesa que o dano decorreu de culpa exclusiva do titular dos dados ou de terceiro (BRASIL, 2018).

Cabe ressaltar que referidas hipóteses de excludente de nexo de causalidade adquirem grande valia para exclusão da responsabilidade de agentes de tratamento em se reconhecendo um Sistema de Culpa Presumida ou de Responsabilidade Objetiva na LGPD:

> Ocorre que atualmente as demandas que se amoldam à responsabilidade objetiva dispensam o filtro da contenção do ilícito, restando apenas ao

> lesante ao recurso ao nexo causal como forma de exclusão da obrigação de indenizar. Isso implica na adoção de uma linha de raciocínio objetiva e técnica por parte dos julgadores e na autonomização e consequente valorização do pressuposto do nexo causal. (ROSELVAND; FARIAS; NETTO, 2019, p. 555)

Sucintamente, como será exposto no próximo subtópico, doutrinadores que defendem um Sistema de Culpa Presumida na Lei nº 13.709/2018, o fundamentam no inciso II do art. 43, hipótese na qual não será o agente de tratamento de dados responsabilizado desde que constitua prova de que apesar de ter realizado o tratamento de dados, não violou a LGPD.

Fato é que, para todos os efeitos, reconhecendo-se na legislação de proteção de dados a responsabilidade civil de natureza objetiva ou fundada culpa presumida, as principais teses a serem invocadas a fim de afastar a responsabilização dos agentes de tratamento residem justamente nas hipóteses elencadas no artigo 43 da LGPD. (BRASIL 2018)

3.2.4. Do fundamento da responsabilidade civil na LGPD: culpa ou risco?

Em complementação à série de deveres e obrigações impostas aos agentes de tratamento, a LGPD trouxe como um dos meios de efetivação dessas disposições a previsão de responsabilização civil dos agentes em caso de descumprimento de respectivos encargos e conseguinte ocorrência de dano ao titular, ou terceiros, em decorrência do tratamento desses dados.

Certamente, no pouco tempo de vigência da LGPD, um dos temas que mais resta divergido em âmbito doutrinário circunda o fundamento da responsabilidade prevista na legislação pelo tratamento de dados pessoais no âmbito privado. Isto é: questiona-se se o elemento culpa é inerente à caracterização dessa responsabilidade, ou se esta tem como fundamento o elemento risco, sendo dispensável, para tanto, a “culpa” do agente de tratamento de dados pessoais para a sua responsabilização pelo dano ocasionado ao titular.

A divergência é consequência da omissão legislativa. Ao passo que a Lei nº 13.709/2018 guarda notórias semelhanças com o Código de Defesa do Consumidor, a LGPD não traz expressa previsão quanto à responsabilidade objetiva dos agentes de tratamento de dados pessoais, a despeito do que foi preconizado pela legislação consumerista em relação aos fornecedores.

Ressalta-se que a discussão ainda não tem ganhado relevantes decisões nos tribunais, considerando que a maior parte de julgados envolvendo responsabilidade civil na LGPD embasam-se em relações consumeristas, o que implica na imediata transição para a responsabilidade objetiva, sem que os tribunais tenham fixados posicionamentos sólidos sobre a natureza da responsabilidade civil na legislação de proteção de dados.

Antes de adentrar na discussão atinente à natureza da responsabilidade civil na LGPD, importante discorrer sobre o sistema de Responsabilidade Civil vigente no ordenamento jurídico brasileiro atual, o qual compreende posições divergentes em âmbito doutrinário.

Discutem os doutrinadores sobre ser a responsabilidade objetiva uma exceção à regra do fundamento subjetivo da responsabilidade, como entende Fernando Tasso (2020, p. 15), ou se ambos os fundamentos teriam sido eleitos pelo legislador, sem qualquer prevalência de um em detrimento do outro.

Adotando-se como premissa o último posicionamento para a presente discussão, comporta ênfase o entendimento de Roselvand, Farias e Braga Netto (2019, p. 630) de que haveria uma coexistência entre a responsabilidade subjetiva e objetiva no Código Civil de 2002.

Segundo os autores, o legislador teria disposto sobre um variável rol de hipóteses em que haveria responsabilidade objetiva, cabendo à doutrina e ao judiciário delimitar outras situações de dever de indenizar objetivo, pautado na cláusula geral de risco. Ambas as hipóteses coexistiriam com a teoria subjetiva, fundada no descumprimento de um dever de cuidado. Em suas palavras:

> Inexiste hierarquia normativa ou axiológica entre teoria subjetiva ou objetiva. O Código Civil não concedeu primazia a uma ou outra forma de imputação de danos. Nas hipóteses em que prevalece a teoria subjetiva (art. 927, caput), mantém-se firme o substrato moral da responsabilidade civil, sendo imperiosa a investigação da falta do agente diante do descumprimento de um dever de cuidado e a consequente reprovação do ilícito e sua censurabilidade pela imposição da sanção reparatória. A outro lado, se a pretensão do legislador for a de promover o princípio da solidariedade, mediante a repartição de riscos sociais, direcionará a norma para a teoria objetiva. O ideal, como vimos, é a convivência entre vários fatores de imputação de danos, cada qual com os seus próprios fundamentos. (ROSENVALD; FARIAS; NETTO, 2019, p. 629 e 620)

Pela interpretação do dispositivo supra, infere-se que a responsabilização objetiva estará presente quando especificada em lei, ou quando a

atividade desenvolvida pelo autor do dano for iminentemente de risco, não fixando o legislador parâmetros para a determinação desse, muito menos as extensões da Teoria do Risco.

Cabe observar que a previsão quanto à responsabilidade objetiva é fruto da evolução histórica, de modo que uma sociedade que lida constantemente com riscos, não pode ignorá-los, e deve assumir a responsabilidade de suas atividades.

Considerando os fundamentos legais da Teoria da Culpa e da Teoria do Risco, situação indiscutível é a existência de diversos posicionamentos sobre a natureza da responsabilidade na LGPD. No presente trabalho, apresenta-se as 3 (três) correntes principais, a seguir destacadas.

3.2.4.1. Natureza objetiva da responsabilidade civil na LGPD

A corrente da responsabilidade objetiva na LGPD ganha consideráveis adeptos. De acordo com esses doutrinadores, na eleição do sistema de responsabilidade teria sido privilegiada a proteção efetiva dos titulares de dados pessoais. De tal forma, o dever de indenizar dos agentes de tratamento estaria presente pela simples ocorrência do dano, independente da análise de culpa em relação ao descumprimento dos deveres da LGPD:

> Segundo essa segunda corrente, a intenção do legislador teria sido a de responsabilizar os agentes pelos danos causados a partir do tratamento de dados independentemente da demonstração de culpa. Dito diversamente, a simples configuração do dano seria suficiente para gerar o dever de indenizar, sem qualquer necessidade de se aferir, no caso concreto, se houve ou não descumprimento de algum dos deveres específicos impostos pela LGPD aos agentes de tratamento de dados. (SANTOS; SILVA; PADRÃO, 2021, p. 19)

Entre os adeptos da responsabilidade objetiva está Bruno Miragem (2021). Apesar de não adentrar especificamente na discussão sobre a natureza da responsabilidade civil na LGPD, em diversas passagens em que trata, na sua obra, da responsabilidade na legislação de proteção de dados pessoais, o jurista preconiza uma responsabilidade independente de dolo e de culpa.

Assim, ao passo que Miragem (2021, p. 495) dispõe sobre o dever de segurança atribuído aos agentes de tratamento, ele afirma que na avaliação da responsabilidade desses pelo tratamento irregular de dados pessoais, não deve ser

considerado o dolo ou a culpa, mas apenas a ocorrência do tratamento irregular, indicando implicitamente a adoção de uma responsabilidade objetiva:

> Em relação aos danos causados em relação ao tratamento indevido de dados pessoais, é necessário que se compreenda a existência de um dever de segurança imputável aos agentes de tratamento (controladores e operadores de dados), que é segurança legitimamente esperada daqueles que exercem a atividade em caráter profissional, e por esta razão presume-se que tenham a expertise suficiente para assegurar a integridade dos dados e a preservação da privacidade de seus titulares. Daí porque a responsabilidade dos agentes de tratamento decorre do tratamento indevido ou irregular dos dados pessoais do qual resulte o dano. Exige-se a falha do controlador ou do operador, que caracteriza o nexo causal do dano. Contudo, não se deve perquirir se a falha se dá por dolo ou culpa, senão que apenas sua constatação é suficiente para atribuição da responsabilidade, inclusive com a possibilidade de inversão do ônus da prova em favor do titular dos dados, nas mesmas hipóteses de hipossuficiência e verossimilhança que a autorizam no âmbito das relações de consumo (art. 42, § 2º, da LGPD). (MIRAGEM, 2021, p. 495)

Conforme entendimento de Bruno Miragem supra colacionado, a LGPD imporia um dever se segurança aos agentes de tratamento, exigindo-se a falha do controlador ou do operador, para configuração do nexo causal. No entanto, seria prescindível a comprovação de dolo ou culpa, bastando apenas prova da falha do controlador ou operador.

Confirmando seu posicionamento quanto à responsabilidade objetiva na legislação, na descrição das condições de imputação da responsabilidade dos agentes de tratamento, Miragem mais uma vez ressalta a dispensabilidade da demonstração do dolo ou culpa, afirmando categoricamente sobre seu posicionamento, sem adentrar em debates doutrinários:

> As condições de imputação de responsabilidade do controlador e do operador pelos danos decorrentes do tratamento indevido dos dados serão: a) a identificação de uma violação às normas que disciplinam o tratamento de dados pessoais; e b) a existência de um dano patrimonial ou extrapatrimonial (moral) ao titular dos dados. Para a imputação de responsabilidade de ambos não se exigirá a demonstração de dolo ou culpa (é responsabilidade objetiva). [...] (MIRAGEM, 2021, p. 496)

A mesma tese é defendida por André Luis Mota Novakoski e Samyra Haydêe Dal Farra Naspolini. De acordo com os autores, a o artigo 42 da LGPD deveria ser interpretado em sistemática com a previsão do art. 927, parágrafo único, de modo a considerar a responsabilidade na LGPD como objetiva:

> Sendo o Código Civil a fonte última irradiadora de princípios e regras de direito privado, a interpretação do art. 42 da LGPD deve ser realizada de forma coerente e sistemática ao disposto no art. 927, § único, do Código Civil, que adotou a teoria da responsabilidade objetiva fundada no risco da atividade exercida pelo agente da atividade potencialmente lesiva, eliminando a situação de socialização do prejuízo na qual a vítima era forçada a suportar o dano em razão da dificuldade (prática, financeira, probatória) de provar a culpa [...] (Novakoski; Naspolini 2020, p. 168).

Na mesma perspectiva é o entendimento de Caitlin Mulholland, a qual também fundamenta a adoção da responsabilidade objetiva no fato de que por serem os possíveis danos decorrentes da atividade de risco significativamente graves, por si só, justificaria o acolhimento de referida modalidade responsabilidade. Em suas palavras:

> [...] apesar do uso de expressões diversas em sua redação, tanto o artigo 42, quanto o artigo 44, da LGPD, adotam o fundamento da responsabilidade civil objetiva, impondo aos agentes de tratamento a obrigação de indenizar os danos causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador. Fundamenta esta conclusão o fato de que a atividade desenvolvida pelo agente de tratamento é evidentemente uma atividade que impõe riscos aos direitos dos titulares de dados, que, por sua vez, são intrínsecos, inerentes à própria atividade e resultam em danos a direito fundamental. Ademais, 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*)

Ainda de acordo com Mulholland (2020, *online*), o fundamento da responsabilidade objetiva também se encontraria nos princípios orientadores da LGPD, com destaque para o princípio da segurança, da prevenção, e da responsabilização e prestação de contas, dispostos no artigo 6º, incisos VII, VIII e X, respectivamente.

Outro argumento invocado pela doutrina orientada pela responsabilidade objetiva reside nas semelhanças da legislação consumerista com a legislação de proteção de dados, de modo que “[...] não haveria motivo para o legislador ter seguido os mesmos moldes do CDC se sua intenção, ao final, não era a de estipular um regime que se aproximasse das relações consumeristas [...]” (SANTOS; SILVA; PADRÃO, 2021, p. 24).

Entre as semelhanças elencadas, destacam-se o caput do art. 43 da LGPD, com o §3º dos artigos 12 e 15 do CDC; a similitude do art. 43, inciso III da LGPD com o artigo 12, §3º, inciso III da legislação consumerista; bem como a

simetria entre o artigo 43 da lei de proteção de dados com o art. 12, §3º, inciso I do Código de Defesa do Consumidor. (TEPEDINO; TERRA; GUEDES, 2020, p. 286).

No mesmo ângulo, Divino e Lima também fundamentam uma responsabilidade objetiva na legislação de proteção de dados, a partir de uma interpretação do art. 43 da lei citada. Em suas palavras:

> Com relação à aplicação dessas teorias na LGPD, o legislador considerou o risco que a atividade carrega consigo, já que direcionada em sua grande parte a direitos da personalidade, mas relativizou as hipóteses de responsabilidade, positivando algumas excludentes de ilicitude e consagrando a Teoria do Risco Objetivo no art. 43 da referida legislação [...] (DIVINO; LIMA, 2020, p. 19)

Desta feita, através de diversos argumentos, esta corrente abarca como fundamento da responsabilidade civil na LGPD um sistema de baseado no risco, utilizando como embasamento legal a disposição do art. 927, parágrafo único, *in fine*, do Código Civil (BRASIL, 2002), a partir de uma leitura sistemática da legislação, considerando os objetivos e princípio da lei de proteção de dados.

3.2.4.2. Natureza subjetiva da responsabilidade civil na LGPD

Quanto à corrente defensora de uma natureza subjetiva da responsabilidade disciplinada na LGPD, essa também traz inúmeros argumentos relevantes.

Uma das premissas norteadoras dessa corrente diz respeito a não previsão da objetivação da responsabilidade na LGPD. Nas palavras de Fernando Tasso (2020, p. 107):

> Em todas as situações jurídicas em que o legislador excepcionou a regra da responsabilidade subjetiva no direito privado, o fez de modo expresso e inequívoco, a exemplo do emprego da expressão “independentemente da existência de culpa” nos artigos 12 e 14 do Código de Defesa do Consumidor ou singelamente se referindo à obrigação de reparar o dado “independentemente de culpa”, como na cláusula geral do artigo 927, parágrafo único do Código Civil. Não há na Lei Geral de Proteção de Dados qualquer artigo que se valha da expressão “independentemente de culpa” ou “independentemente da existência de culpa”, a indicar de modo inequívoco que o regime jurídico adotado fora o da responsabilidade objetiva.

Outro critério constantemente apresentado pela corrente subjetivista da responsabilidade guarda relação com a série de deveres impostos pelo legislador aos agentes de tratamento de dados pessoais, denominados como standard de

condutas. Sobre referidos encargos, apontam Tepedino, Terra e Guedes (2020, p. 289):

> Além disso, a LGPD tem todo um capítulo dedicado a "segurança e boas práticas". Trata-se do Capítulo VI, que é dividido em duas seções: (i) Seção I – Da segurança e do sigilo de dados e (ii) Seção II – Das Boas Práticas e da Governança. Nessas seções, a LGPD criou uma série de deveres que devem ser observados pelos agentes de tratamento de dados. O legislador estabeleceu, então, verdadeiro standard de conduta que deve ser seguido pelos agentes de tratamento de dados para evitar incidentes de segurança, chegando mesmo ao ponto de determinar, na Seção II, que os agentes poderão, no âmbito de suas competências, traçar as normas de boas práticas e de governança. Também na Seção II é possível notar a preocupação do legislador com a conduta dos agentes, assim como com o cumprimento de programas, políticas internas, procedimentos, mecanismos de supervisão (internos e externos), padrões técnicos etc.

Considerando esse *standard* de condutas, essa corrente doutrinária aponta que não haveria coerência na fixação desse rol de deveres pelo legislador, se ainda que os agentes as cumprissem, ainda corressem o risco de serem responsabilizados objetivamente:

> Assim sendo, caso o sistema de responsabilidade civil fosse da modalidade objetiva, a prescrição exaustiva e detalhada dos deveres seria algo absolutamente inócuo, sobretudo porque redundaria na conclusão de que de nada adiantaria o cumprimento dos deveres se, qualquer que fosse o incidente, a responsabilidade pela reparação estivesse configurada, o que é um contrassenso (TASSO, 2020, p. 108):

Outro argumento fortemente debatido pela doutrina que defende a natureza subjetiva da responsabilidade civil prevista na LGPD remete ao histórico de tramitação de projeto dessa Lei. Em sua redação original, o projeto de lei nº 5.276/2016 previa expressamente em um de seus dispositivos, a responsabilidade objetiva e solidária dos agentes de tratamento. Como aduzem Tepedino, Terra e Guedes (2020, p. 288):

> O único dispositivo da LGPD que remetia para a responsabilidade objetiva foi retirado no trâmite legislativo, o que é um dado significativo para a interpretação da lei. O próprio histórico de tramitação do projeto de lei que deu origem à LGPD evidencia, portanto, a opção do legislador pela responsabilidade subjetiva. A versão inicial do Projeto de Lei n.º 5276 trazia, no Capítulo sobre "Transferências internacionais de dados", uma regra geral expressa de responsabilidade solidária e objetiva desses agentes pelos danos causados em virtude do tratamento de dados (art. 35). Além disso, na Seção sobre "Responsabilidade e Ressarcimento de danos", havia uma abordagem ampla sobre os sujeitos obrigados a reparar o dano ("todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais causar a outrem dano") (art. 42), e outra regra igualmente ampla

> prevendo a solidariedade entre todos os agentes da cadeia de tratamento, sem qualquer distinção entre controlador e operador (“[n]os casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesma obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos causados”) (art. 44).

Nesse ângulo, Tepedino, Terra e Guedes (2020, p. 289) apontam que essa previsão foi retirada das versões posteriores do projeto, não permanecendo na versão final da LGPD. Ademais, o artigo 42 da legislação discutida teria sofrido uma alteração importante durante a tramitação do projeto:

> [...] ainda no período de tramitação do projeto, o caput do art. 42 da LGPD sofreu uma alteração importante: a expressão “em violação à legislação de proteção de dados pessoais” foi acrescentada, o que também evidencia a opção do legislador pela responsabilidade subjetiva. Os agentes de tratamento não responderão em toda e qualquer situação em que causarem danos a terceiros, mas apenas quando isso ocorrer em violação à legislação de proteção de dados pessoais, ou seja, quando a sua conduta não se adequar ao standard estabelecido pelo próprio legislador. (TEPEDINO, TERRA E GUEDES; 2020, p.289).

Visando combater os argumentos apresentados pela doutrina que defendem a responsabilização objetiva dos agentes de tratamento, a corrente subjetiva enuncia diferenças da LGPD com o CDC, que também indicariam a opção legislativa na LGPD pela responsabilidade subjetiva.

Um dos dispositivos apontados pela corrente subjetiva é o artigo 43, inciso II, que segundo Tepedino, Terra e Guedes (2020, p.291), não diria respeito a uma hipótese de relação de causalidade, mas sim induziria à ideia de culpa presumida como fundamento da responsabilidade civil. Os autores também lecionam as significativas diferenças do mencionado dispositivo, com o art. 12, §3º, inciso II, do CDC. Assim:

> O inciso II reflete, portanto, o regime subjetivo de responsabilidade, adotado pela LGPD, porque está intrinsecamente vinculado ao elemento culpa e, exatamente por isso, sua redação não se assemelha à do Código de Defesa do Consumidor. Enquanto o Código de Defesa do Consumidor isenta de responsabilidade o fornecedor que demonstrar que o defeito inexiste, que é um parâmetro mais objetivo, a LGPD exime do dever de indenizar o agente de tratamento que não tiver violado a lei. (TEPEDINO; TERRA; GUEDES, 2020, p. 292)

Este é, inclusive o entendimento de Fernando Tasso, que se referindo ao inciso II do art. 43 da LGPD, defende:

> Enquanto as hipóteses dos incisos I e III de ambos os artigos se equivalem, este coloca como excludente a não colocação do produto no mercado, o

> que consiste num fato de objetividade binária, enquanto a Lei Geral de Proteção de Dados prevê mais um dever ao agente de tratamento de dados, qual seja a observância de uma conduta diligente que, em sendo observada é causa de elisão da responsabilidade civil. (TASSO, 2020, p. 109)

Outrossim, cabe colocar em evidência o entendimento de Tepedino, Terra e Guedes (2020, p. 293) quanto ao fundamento da responsabilidade civil na LPGD na culpa presumida.

Segundo os autores, a redação do art. 43 não seguiria o modelo da cláusula geral de risco adotada pelo Código Brasileiro, mas sim se trataria de enunciado legal semelhante ao adotado pelo Código Civil Português e o Código Civil Italiano, os quais enunciam um sistema da culpa presumida. Nesse sentido, a culpa do agente de tratamento, em caso de danos aos titulares de dados pessoais, seria presumida, sendo afastada, no entanto, se o agente de tratamento provar em nenhum momento ter violado a LGPD, seguindo o standard de conduta preconizado pela legislação. A adoção do modelo de culpa presumida, segundo os autores, teria sido ressaltada pela previsão do artigo 44.

Aliás, destaca-se o entendimento de Fernando Tasso (2020, p. 109) que “o dever sucessivo da responsabilidade civil decorre da infringência a um dever originário, o de adotar as medidas de segurança previstas na Lei”, o que se coaduna com o sistema da responsabilidade fundamentada na culpa presumida, apesar de não ter o magistrado assumido essa posição expressamente.

Seguindo essa corrente, Tasso (2020, p. 112) afirma que a LGPD deve ser interpretada em consonância com o Código Civil, no qual prevalece a regra da responsabilidade subjetiva, nos termos do art. 186 e 187, aplicando-se a responsabilidade objetiva apenas em hipóteses específicas ou em caso de exercícios de atividade de risco, em função do artigo 927, parágrafo único do Código Civil. Destarte, a responsabilidade objetiva pela violação da LGPD só poderia ser utilizada como fundamento em caso de atividades essencialmente de risco, incidindo nessas circunstâncias a cláusula geral de responsabilidade previsto no art. 927. Segundo referido entendimento, a atividade de tratamento de dados, em sua natureza, não seria considerada atividade de risco.

Como último argumento utilizado por parte da corrente subjetiva, e que sofre severas críticas da doutrina objetiva, está relacionado à previsão do art. 45 da LGPD.

Segundo Tepedino, Terra e Guedes, reconhecer o fundamento objetivo da responsabilidade seria tornar a previsão do dispositivo citado inócua.

Elucida os autores que tendo instituído a LGPD um regime de responsabilidade objetiva, seria este mais severo do que o próprio CDC. Desta feita, ao prever que nas relações de consumo a responsabilidade se submeteria ao regime previsto na legislação consumerista, significaria dizer que mesmo diante da disparidade existente nas relações de consumo, a essa seria aplicada um regime menos gravoso. Nesse sentido:

> Por fim, se a LGPD tivesse adotado o modelo objetivo de responsabilidade, então a remissão ao Código de Defesa do Consumidor no art. 45 seria inócua, para dizer o mínimo. Isto porque, nesta hipótese, a LGPD teria instituído um regime de responsabilidade até mais rigoroso do que o do próprio Código de Defesa do Consumidor, que pelo menos exige a existência de um "defeito" para a configuração da responsabilidade. Assim, diante de uma relação de consumo, a responsabilidade dos agentes de tratamento se submeteria a um regime, por assim dizer, menos rigoroso do que o instituído pela LGPD, que seria aplicável às relações paritárias, o que parece não fazer sentido. (TEPEDINO; TERRA; GUEDES, 2020, p. 293)

Sem prejuízo dos demais argumentos apresentados para fundamentar uma possível responsabilidade subjetiva, os fundamentos apresentados por Gustavo Tepedino, Aline Terra e Gisela Cruz, bem como pelo magistrado Fernando Tasso, permeiam as discussões doutrinárias.

3.2.4.3. Natureza proativa da responsabilidade na LGPD

Corrente doutrinária que também merece ênfase é a capitaneada por Maria Celina Bodin de Moraes.

De acordo com a autora, a responsabilidade prevista na LGPD não seria objetiva ou subjetiva, mas sim guardaria uma nuance especial, que a mesma denomina de responsabilidade proativa.

Consoante entendimento de Bodin de Moraes (2019, p. 05), a responsabilidade prevista na LGPD estaria ligada ao princípio da prestação de contas, preceituado no artigo 6º, inciso X da LGPD, de modo que o simples cumprimento da lei não seria mais suficiente, devendo o agente de tratamento de dados pessoais demonstrar que tomou "proativamente" todas as medidas necessárias para prevenir a ocorrência de possíveis danos.

Nesse sentido, em artigo elaborado em 2019, antes da entrada em vigor pleno da legislação de proteção de dados, Maria Celina Bodin leciona:

> [...] A partir de 2020, quando a lei entra em vigor plenamente, qualquer organização a ela sujeita terá que 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 v) exige esse mesmo cumprimento responsável de seus funcionários e na sua cadeia de terceirização. (MORAES, 2019, p. 05)

Ainda complementa Moraes que a legislação previu uma séria de consequências em razão do descumprimento da legislação e do dever de prestação de contas. Assim, segundo a professora:

> Em termos práticos, estes novos princípios requerem que as empresas analisem os dados que tratam, com que finalidade o fazem e que tipo de operações de tratamento levam a cabo. Exigem-se, em síntese, atitudes conscientes, diligentes e proativas por parte das empresas em relação à utilização dos dados pessoais. Assim, a partir de agosto de 2020, quando entra em vigor a LGPD, qualquer empresa que processe dados pessoais não apenas terá que cumprir a lei, mas também deverá provar que está em conformidade com a Lei. Caberá às empresas, e não mais (apenas) à Administração Pública, a responsabilidade de identificar os próprios riscos e escolher e aplicar as medidas apropriadas para mitigá-los. (MORAES, 2019, p. 06)

Em razão dessa cognição, Bodin de Moraes (2019, p. 06) conclui que, não obstante o legislador ter guardado semelhanças com o regime de responsabilidade subjetivo, criou um sistema fundamento no risco objetivo, objetivando ir além da prevenção, adotando um sistema que visa justamente evitar a ocorrência de danos. A esse novo sistema, Moraes denomina Sistema de Responsabilização Proativa.

3.2.4.4. LGPD: um sistema de culpa presumida embasado no dever de segurança e na prestação de contas

Em verdade, as divergências existentes no tocante ao fundamento da responsabilidade civil na LGPD decorrem de um fato mais complexo: a realidade moderna, em razão da sua conjuntura, já não sustenta apenas a regra genérica de responsabilidade subjetiva, excecionando apenas hipóteses casuísticas da responsabilidade objetiva como fundamento para dever de indenizar e uma cláusula geral de risco em termos genéricos.

Cada vez mais se está diante de novas situações ensejadoras de danos à sociedade, como causa dos avanços tecnológicos, firmando-se como as “novas pretensões” abordadas pela professora Giselda Hironaka (2005, p. 128), e já colacionadas no início deste trabalho.

Na sociedade hodierna, em um ordenamento jurídico que tem como elemento norteador a Dignidade da Pessoa Humana, se mostra insuficiente focar a Responsabilidade civil na ideia de que a conduta ilícita que decorreu de culpa do agente deve ser vista como hipótese principal orientadora do dever de indenizar:

> [...] Hoje, todos os esforços se concentram na busca da reparação, tendo-se radicado em nossa consciência coletiva a ideia de que a vítima merece ser ressarcida, ainda que não tenha havido conduta culposa ou dolosa (isto é, ilícita) por parte do autor do dano. (MORAES, 2019, p. 02)

Dessa forma, a análise da responsabilidade objetiva focada na reparação efetiva do dano, em detrimento da análise do elemento culpa, demonstrar-se-ia mais pertinente.

No entanto, a Teoria do Risco como inserida no ordenamento jurídico brasileiro, nos termos do art. 927, parágrafo único, não transparece efetiva segurança, uma vez que atribui a responsabilidade objetiva apenas às situações casuísticas elencadas pelo ordenamento jurídico, e às atividades essencialmente de risco, nas hipóteses assim entendidas pela jurisprudência.

Conforme afirma Giselda Hironaka sobre a necessidade de um sistema que tenha como objetivo a diminuição das hipóteses de irressarcibilidade (2005, p. 106):

> Hodiernamente, há uma significativa participação humana na assunção de riscos e, consequentemente, haverá de ocorrer assunção, também, da responsabilização que daí decorre. O cerne da preocupação dos atuais dias desenvolve-se no sentido de não mais restar “irresarcido” nenhum dano ao qual estejamos, todo nós, expostos, em consequência da atividade por outrem desempenhada. Ou, pelo menos, que haja uma progressiva, mas incessante e sensível, diminuição das hipóteses de “irresarcibilidade”.

O sistema de responsabilidade civil vigente no ordenamento jurídico atual não se mostra totalmente compatível com o elemento norteador da Carta Magna Brasileira: a dignidade da pessoa humana.

Diante da Constitucionalização do Direito Civil, muitos são os doutrinadores que tem defendido nos últimos anos um fundamento para o instituto focado essencialmente na indenização da vítima e proteção efetiva desta, e não na

culpa em si, tendo como intuito objetivar o sistema da responsabilidade pátrio. Como ponderam Tepedino, Terra e Guedes (2020, p. 08):

> A rigor, a revolução por que passa, ainda hoje, a responsabilidade civil decorre, em grande medida, da alteração da própria função do instituto, que deixa de ser, definitivamente, a moralização ou a punição de condutas, e passa a ser a proteção da vítima, de acordo com a máxima segundo a qual, verificado o dano injusto, a vítima não deve ficar irressarcida. Volta-se a responsabilidade civil para as consequências do dano, não já para suas causas.

De tal feita, diversas teses doutrinárias surgiram nesse sentido, com destaque para a Teoria da "Responsabilidade Pressuposta" defendida por Giselda Hironaka. Sustenta a professora, como conclusão de tese para aquisição de seu título de livre docente:

> Assim construída, a regra idealizada portaria o atributo equivalente a um fundamento geral da responsabilidade civil contemporânea, se sorte a se instalar não apenas além da concepção de culpa, mas também da própria concepção de risco, tal como consagrada até agora, na doutrina nacional e alienígena. Instalar-se-ia uma tal regra – como princípio fundamente de caráter geral da responsabilidade civil, independente de culpa de quem quer que seja, cuja auto-sustentabilidade se daria apenas pela efetiva produção do dano injusto, em desfavor da vítima, ancorando-se para além da pontuação legal casuística de responsabilização objetiva e revelando, como causa final almejada, a concretização dos paradigmas do justo e do equânime. (HIRONAKA, 2002, p. 354)

Em síntese, a Teoria da Responsabilidade Pressuposta capitaneada por Giselda Hironaka sustenta a criação de uma responsabilidade que fosse pressuposta pelo próprio ordenamento jurídico, fugindo dos contornos clássicos da culpa e rico, e embasando-se em um princípio fundante da responsabilidade que visasse centralizá-la na efetiva reparação da vítima.

Citada teoria orienta-se pelo reconhecimento dos riscos da sociedade pós - moderna. Segundo Hironaka (2005, p. 106), diante de uma assunção de riscos pela sociedade em razão de suas atividades, essa também deve arcar com os riscos que dela recorrerem.

A obra de Giselda Hironaka é um grande marco no sentido de se reconhecer a insuficiência da Teoria da Culpa como regra no ordenamento jurídico.

Assim como a dinamicidade da sociedade fez aflorar a teoria objetiva, imagina-se que, em um breve intervalo de tempo, a base fundante da responsabilidade será novamente reformada. Enquanto isso, a doutrina tenta dar

seus primeiros passos no sentido de identificar esse “fundamento adequado da responsabilidade”, através de sistemas intermediários de responsabilidade.

Cabe observar que o fundamento da responsabilidade objetiva da LGPD encontra certo diálogo com o motivo de ser da Teoria da Responsabilidade Pressuposta, haja vista referida corrente defender a responsabilidade objetiva dos agentes de tratamento independente de culpa, isto é, independente de qualquer violação pelos agentes de tratamento da legislação de proteção de dados, orientando-se a partir do risco e da necessidade de efetiva reparação à vítima.

Norteando-se por essa lição, infere-se que em razão dos riscos proporcionados pela atividade de tratamento de dados pessoais, os danos consequentes ao titular ou terceiros deveriam ser indenizados pelo agente de tratamento, independente da existência de culpa por parte deste, fazendo valer a ideia de que o instituto de Responsabilidade civil tem como função principal a reparação.

Logo, em um diálogo com a Constituição Federal, a responsabilidade deveria ser norteada pela dignidade da pessoa humana, e, portanto, o titular de dados pessoais deveria ser reparado a partir da lógica da Responsabilidade Objetiva.

Sem embargo, a teoria liderada por Hironaka, apesar de ter sido elaborada na primeira década do século XXI, ainda demonstra ser uma realidade distante do ordenamento jurídico hodierno, considerando a complexidade de migrar de um ordenamento jurídico que tem como regra a teoria da culpa, para uma objetivação completa da responsabilidade, ou mesmo para um sistema de responsabilidade pressuposta, que reconhece como insuficiente os dois sistemas anteriores.

Essa reforma necessária do ordenamento jurídico no concernente ao sistema de responsabilidade, porém, é apontada por diversos civilistas, entre eles Rui Belfort Dias (2006, p. 52), em obra adaptada de José Dias Aguiar:

> Evidente que o Direito não vem se mostrando alheio a essas alterações, mas está longe ainda o tempo em que deixará de ser usado como instrumento de manutenção dos privilégios e das garantias de mudanças tópicas e graduais e, se possível, não invasivas das prerrogativas dos que detém o poder.
> No processo de alteração do direito, um homem novo, preocupado com o destino da humanidade e com o mundo que deixaremos para os nossos descentes, preocupado com as injustiças sociais, com a visão voltada para

> a construção de uma sociedade mais igualitária, em que valores éticos sejam resgatados e efetivamente empregados nos dilemas presentes, deve ser o ponto de partida dessa evolução da responsabilidade civil.

Não obstante a essa responsabilidade idealizada por Hironaka, e desejada por outros civilistas, que reconhecem a insuficiência do sistema de responsabilidade civil atualmente vigente, não se pode ignorar esse sistema, que se encontra em vigor e que deve ser interpretado em sistemática com a Lei Geral de Proteção de Dados.

Conforme já exposto no presente trabalho, haveria a coexistência no ordenamento jurídico vigente da responsabilidade subjetiva e objetiva. A subjetiva estaria inerente ao dever de cuidado a ser observado, enquanto, nos termos do que preceitua o art. 927 do Código Civil, em seu parágrafo único, a responsabilidade objetiva estaria presente nas hipóteses tipificadas pelo legislador, “ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem” (BRASIL, 2002).

Como pontuado por Rosenvald, Farias e Netto (2019, p. 629), as hipóteses de atividades que implicariam em risco estariam dependentes da interpretação judiciária.

Por uma interpretação sistemática do ordenamento jurídico, nota-se, no entanto, que as hipóteses decorrentes de risco com destaque e recorrentes na sociedade contemporânea foram objetivadas pelo próprio legislador, citando-se como exemplo a relação de consumo, deixando ao Estado Juiz apenas a interpretação de hipóteses casuísticas e excepcionais de atividade de risco.

Concernente ao defendido pela corrente doutrinária objetiva, de fato, há diversas semelhanças entre a legislação consumerista e a de proteção de dados. O que causa estranheza é diante da importância e impacto da LGPD à sociedade, assim como causou o CDC na década de 90, o legislador ter deixado a cargo da jurisprudência a objetivação dessa responsabilidade, por uma interpretação da atividade de tratamento como de risco nos termos do art. 927, parágrafo único, que, conforme já ressaltado, deveria ser utilizado em situações excepcionais, não antecipadamente previstas pelo legislador.

Essa questão ganha ainda mais relevância considerando o trâmite legislativo do projeto de lei. Como já apontado nesta pesquisa, e sendo este um dos princípios argumentos da corrente subjetiva, o Projeto de Lei nº 5276/2016, no

Capítulo sobre “Transferências internacionais de dados”, trazia previsão em seu artigo 35 de responsabilidade solidária e objetiva dos agentes pelos danos causados em virtude de tratamento de dados. (TEPEDINO; TERRA; GUEDES, 2020, p. 288). Essa redação, no entanto, foi retirada da versão final da LGPD, não subsistindo nenhuma disposição semelhante.

Cabe enfatizar que a LGPD é um verdadeiro *standard* de condutas que devem ser seguidas pelos agentes de tratamento. Um dos meios de efetivação de referidas disposições seria justamente a responsabilidade civil pelo tratamento irregular de dados, depreendendo a importância de respectivo instituto dentro do aparato normativo da Lei Geral de Proteção de Dados.

Logo, se o legislador, em diversos dispositivos que dizem respeito à responsabilidade civil pelo tratamento de dados pessoais no âmbito privado na LGPD, teve clara inspiração na legislação consumerista, como apontam os próprios defensores da responsabilidade objetiva, não faria sentido ele deixar de prever a responsabilização objetiva dos agentes de tratamento , assim como o fez o Código de Defesa do Consumidor, sobretudo considerando a função social e o impacto causado pela legislação, se realmente tivesse o intuito criar como regra fundante na GDPR brasileira referida responsabilidade.

De mais a mais, é incoerente imaginar que o legislador, em uma hipótese de grande complexidade, como a Lei Geral de Proteção de Dados, deixasse a cargo de a jurisprudência interpretar todos os casos envolvendo tratamento de dados como atividade de risco, com base no art. 927, parágrafo único, *in fine*.

Se de fato fosse o objetivo do legislador ter previsto como regra a responsabilidade objetiva na LGPD, teria assim disposto expressamente, assim como no CDC, não abrindo margens para insegurança jurídica decorrente de interpretações judiciárias casuísticas.

Esse raciocínio lógico leva à conclusão de que a regra na legislação de proteção de dados não seria a responsabilidade objetiva, haja vista a importância da LGPD e sua previsão de responsabilidade.

Quando o legislador deixou de prever a objetivação de responsabilidade como regra, o fez propositalmente, provavelmente considerando as casuísticas que envolvem cada caso concreto, diante da ampla gama de atividades que realizam o tratamento de dados pessoais como atividade meio.

Deste modo, não se mostraria totalmente razoável a objetivação da responsabilidade como regra absoluta na legislação de proteção de dados, com fundamento exclusivo no risco, visto que o risco zero nunca existirá (OLIVERA *et al*.; 2021, p. 153).

Entender não se tratar de uma responsabilidade objetiva, sem embargo, não significa afirmar ser essa uma responsabilidade subjetiva em seu sentido originário, considerando que "[...] que responsabilidade subjetiva e objetiva são extremos dentro de um espectro contínuo." (ROSENVALD; FARIAS; NETTO, 2019, p. 241).

Essa conclusão parte do fato de que, não obstante o risco zero não existir, também não se pode ignorar os riscos decorrentes das atividades de tratamento, elemento norteador da corrente objetiva. Dessa forma, conclui-se não ser a responsabilidade subjetiva em seu extremo a regra da responsabilidade civil na LGPD. A responsabilidade civil nessa legislação, na verdade, estaria delimitada no espectro entre os dois extremos: responsabilidade civil objetiva e subjetiva.

Maria Celina Bodin de Moraes (2019, p. 05), por sua vez, afirma ter essa responsabilidade como base fundante a proatividade, embasando-se no dever de prestação de contas imposto aos agentes de tratamento de dados pessoais.

Diante da realidade colocada pela LPGD, imprescindível que essa proatividade seja levada em consideração, estabelecendo-se uma responsabilidade intermediária na LGPD.

Comporta enfatizar que essa responsabilidade intermediária não seria nova no ordenamento jurídico brasileiro, e a rigor da redação dos dispositivos legais da legislação, configuraria uma espécie de responsabilidade já conhecida: a culpa presumida.

Nesse sentido, inclusive, foi a análise conclusiva de Gustavo Tepedino, Aline Terra e Gisela Guedes, defensores da responsabilidade subjetiva sob o viés da culpa presumida, em análise comparativa com a redação dos artigos que adotam a culpa presumida nos Códigos Civis Francês e Português (2020, p. 193).

Sobre o instituto da culpa presumida, sustentam Rosenvald, Farias e Netto (2020, p. 241):

> Pode-se conceituar a presunção de culpa como uma técnica processual de inversão de ônus da prova. Ou seja, em hipóteses previstas pela lei, não mais caberia ao ofensor a hercúlea missão de provar o erro de conduta

> moralmente imputável ao agente – o brocardo actori incumbit probatio- , pois em princípio a demonstração do fato ilícito (antijuridicidade + imputabilidade) já equivaleria a um atestado de culpa. Portanto, o ofensor deveria demonstrar que o dano não decorreu de sua falta de diligência e prudência, porém de uma causa estranha ao seu comportamento, tal como força maior, fato exclusiva da vítima ou fato de terceiro.

De acordo com o ensinamento dos autores, a culpa presumida seria um sistema intermediário entre responsabilidade subjetiva e a responsabilidade objetiva, no qual bastaria ao indivíduo lesado demonstrar o fato ilícito e o dano sofrido. Uma vez demonstrado, haveria presunção de culpa em relação ao ofensor. Essa presunção, no entanto, seria relativa, podendo o suposto ofensor demonstrar que não ocorreu nenhuma falta de diligência ou prudência, mas sim que o fato ilícito foi ocasionado por uma causa estranha ao seu comportamento.

Esse raciocínio adequa-se perfeitamente a disposição da responsabilidade civil na LGPD. Caberia ao lesado pelo tratamento irregular de dados pessoais apenas demonstrar o ato ilícito, estruturado no fato de ter seu direito à proteção de dados pessoais violada, e o dano. A partir dessa demonstração, já haveria presunção de culpa em desfavor do agente de tratamentos.

Em contrapartida, ao agente de tratamento de dados pessoais a quem é atribuído o ato ilícito, caberia afastar a presunção de culpa que existe em seu desfavor, produzindo prova no sentido de que em nenhum momento houve violação à Lei Geral de Proteção de Dados, bem como que teria adotado uma postura ativa para evitar a ocorrência de dano, através da prestação de contas, preconizado no art. 6º, inciso X da LGPD, cumprindo seu dever de segurança. Essa última parte do entendimento, inclusive, se coaduna com a Responsabilidade Proativa defendida por Maria Celina Bodin de Moraes.

No mesmo sentido, o Tribunal de Justiça de São Paulo (São Paulo, 2021) tem reconhecido a responsabilidade pelos agentes de tratamento pela falha do dever de segurança, o que fortalece o entendimento de uma responsabilidade fundada na culpa presumida e orientada pelo dever de segurança e prestação de contas Assim:

> DANO MORAL – VAZAMENTO DE DADOS – CÓDIGO DE DEFESA DO CONSUMIDOR – DEVER DE SEGURANÇA. 1 – Reconhecida a falha no sistema, ante a invasão por terceiros, ocasionando o vazamento de dados pessoais do consumidor, patente o dever de indenizar pelos danos morais sofridos; 2 – Indenização por danos morais fixada no montante pleiteado, ou seja, em R$ 10.000,00, corrigidos do arbitramento e acrescido de juros de mora de 1% ao mês, a partir da citação. RECURSO PROVIDO (TJSP;

> Apelação Cível 1000144-71.2021.8.26.0405; Relator (a): Maria Lúcia Pizzotti; Órgão Julgador: 30ª Câmara de Direito Privado; Foro de Osasco - 1ª Vara Cível; Data do Julgamento: 25/08/2021; Data de Registro: 13/09/2021)

Frisa-se que o sistema da culpa presumida parece encontrar perfeito embasamento no art. 43, inciso II da LGPD, que dispõe que os agentes de tratamento só não serão responsabilizados quando provarem que, embora tenham realizado o tratamento de dados pessoais, não houve qualquer violação à lei de proteção de dados (BRASIL, 2018). Nesse sentido:

> Nesse inciso II, o legislador afirma, a grosso modo, que, ainda que exista nexo causal entre a conduta do agente e o dano, se ele conseguir provar que cumpriu todos os deveres impostos pela LGPD, tomando as medidas de segurança recomendadas (cumprindo programas, políticas internas, procedimentos, mecanismos de supervisão, internos e externos, padrões técnicos etc.), não será responsabilizado. Nessas circunstâncias, o agente terá demonstrado que observou o standard esperado e, se o incidente ocorreu, não foi em razão de sua conduta culposa. (TEPEDINO; TERRA; GUEDES, 2020, p. 292)

Desta feita, o sistema de culpa presumida encontraria pleno cabimento diante das disposições e finalidades da LGPD. Precipuamente, pois ao passo que não objetiva totalmente a responsabilidade civil, também não desprotege o titular de dados pessoais, reconhecendo os riscos inerentes à atividade de tratamento de dados, presumindo-se a culpa do agente de tratamento de dados.

Todavia, considerando e privilegiando o *standard* de condutas dispostos na legislação, caberia ao agente de tratamentos afastar a presunção de sua culpa provando que todas os deveres impostos pela legislação foram cumpridos, inclusive as obrigações inerentes ao dever de segurança e prestação de contas, preconizados pela professora Bodin de Moraes, de modo a evitar qualquer ocorrência do dano ao titular.

Desta feita, nos casos de afastamento da presunção de culpa, o agente prova que se o dano ocorreu, foi por motivos alheios às suas responsabilidades impostas por lei, as quais foram cumpridas, com destaque para o dever de segurança e prestação de contas.

Aliás, como destacam Tepedino, Terra e Guedes (2020, p. 293), as semelhanças do art. 43, inciso II, da LGPD, com os dispositivos legais que adotam o sistema de culpa presumida nas legislações civis italiana e francesa são latentes.

Nesse sentido, segundo o art. 2050 do Código Civil (ITÁLIA, 1942): "*Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, e tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*."[9]

Nesta perspectiva, a redação do art. 493, "2" do Código Civil Português[10] apregoa que:

> Quem causar danos a outrem no exercício de uma actividade, perigosa por sua própria natureza ou pela natureza dos meios utilizados, é obrigado a repará-los, excepto se mostrar que empregou todas as providências exigidas pelas circunstâncias com o fim de os prevenir. (PORTUGAL, 1966)

Assim, em ambas as legislações alienígenas, o exercício de atividade perigosa invoca o sistema de responsabilidade fundado na culpa presumida, sendo esta presunção afastada se o agente provar que tomou todas as medidas diligentes para evitar o dano.

Com esse mesmo raciocínio, é a redação do art. 43, inciso II da LGPD, que ensina que os agentes de tratamento serão responsabilizados, exceto se provarem que não houve qualquer violação da LGPD no tratamento de dados pessoais, isto é, que adotaram todo o *standard* de condutas estipulados pela legislação, inclusive a prestação de contas e dever de segurança, visando evitar a ocorrência de danos ao titular de dados e a terceiros.

Vale frisar que o reconhecimento do sistema da culpa presumida não tornaria a previsão do art. 42, §2º, quanto à possibilidade de inversão do ônus da prova, ineficaz.

Ainda que a culpa do agente de tratamento seja presumida, cabendo este provar que cumpriu a lei e tomou todas as diligências necessárias para evitar o dano, ainda restaria ao lesado demonstrar o fato ilícito e o dano. Neste caso, em sendo identificada a hipossuficiência do lesado, caberia ao juiz também inverter o ônus da prova no tocante à demonstração do fato ilícito e do dano, isto é, além de provar o cumprimento do *standard* de condutas dispostas pela LGPD, o agente de

---

[9] "Quem causar dano a outrem no exercício de atividade perigosa, pela sua natureza ou pela natureza dos meios utilizados, é obrigado a repará-lo, se não provar ter tomado todas as medidas adequadas para evitar o dano". (tradução nossa)

[10] "Aquele que causar dano a outrem no exercício de uma atividade perigosa por sua própria natureza, ou pela natureza dos meios utilizados, fica obrigado a repará-lo, salvo se demonstrar que empregou todas as providências cabíveis". (tradução nossa)

tratamento também teria de demonstrar que não houve fato ilícito e nem dano decorrente da atividade de tratamento discutida.

Inclusive o art. 44, parágrafo único da LGPD leciona que ao deixar de adotar as medidas de segurança previstas no art. 46 da respectiva lei, o agente de tratamento der causa ao dano, será responsabilizado. Assim, se provar que adotou as medidas previstas no art. 46, isto é, as medidas diligentes necessárias, o agente de tratamentos não será responsabilizado. Trata-se de mais um indício de que a LGPD teria adota o Sistema da Culpa Presumida. Consoante lições de Tepedino, Terra e Guedes (2020, p. 293):

> O parágrafo único do art. 44, que trata dos incidentes de segurança, também seguiu o mesmo modelo de responsabilidade subjetiva, ao afirmar que "[r]esponde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano". Assim, também na hipótese de incidente de segurança, a opção do legislador não foi a de responsabilizar o agente independentemente de culpa, mas apenas quando ele não conseguir demonstrar que adotou as medidas de segurança previstas em lei. Aqui também o legislador evidenciou a sua preocupação com a conduta dos agentes de tratamento, adotando redação semelhante à do art. 493, "2", do Código Civil português e do art. 2.050 do Código Civil italiano, que criaram sistemas de presunção de culpa.

Por consequência do que foi apresentado, a partir de uma interpretação legal da LGPD e seus objetivos, bem como pela por uma análise comparativa com as codificações civis italiana e francesa, entende-se que a legislação de proteção de dados teria adotado um sistema de responsabilidade fundado na culpa presumida. Contudo, caberia interpretar esse sistema de culpa presumida em diálogo do que foi defendido por Maria Celina Bodin de Moraes na defesa de uma Responsabilidade Proativa, devendo-se considerar para a exclusão da responsabilidade do agente de tratamento o cumprimento do dever de segurança e de prestação de contas preconizados na legislação.

À vista disso, a LGPD simultaneamente teria levado em conta os riscos decorrentes da atividade de tratamento, tal como compreenderia a valorização do cumprimento do *standard* de condutas aduzidos pela legislação, de modo a não tornar as previsões da LGPD inócuas.

Assim sendo, a culpa presumida seria um sistema intermediário entre dois extremos, a responsabilidade subjetiva e a responsabilidade objetiva, comprovando-se que o legislador não se encontra desvinculado aos avanços da pós-modernidade e seus impactos na responsabilidade civil, mas, com efeito, estaria

dando passos lentos no sentido de migrar de um sistema fundado na responsabilidade subjetiva, para um sistema embasado na reparação efetiva da vítima do dano.

Cabe dar ênfase que o Ordenamento Jurídico tende a avançar no instituto da responsabilidade civil nos próximos anos, em vista da realidade hodierna que se apresenta, o que leva a crer que, em um futuro não muito distante, esse sistema de culpa presumida orientado pelo dever de segurança e prestação de contas, disposto na LGPD, possa ser alterado, bem como o sistema de responsabilidade civil previsto pela própria legislação civilista.

4 RESPONSABILIDADE CIVIL NO COMÉRCIO ELETRÔNICO NA PESPECTIVA DA PROTEÇÃO DE DADOS PESSOAIS

Após estudo quanto ao regime jurídico da responsabilidade civil prevista na Lei Geral de Proteção de Dados, importa ser analisado os principais desdobramentos de aludida lei sobre o comércio eletrônico, sendo este, de longe, um dos setores mais atingidos pelas regulações trazidas pela LGPD.

Considerando o alavanque da economia digital na última década, sobretudo após a pandemia do Covid-19, realiza-se uma delimitação das principais particularidades da responsabilidade civil pelo tratamento inadequado de dados pessoais no âmbito do comércio eletrônico, através da aplicação das premissas do da Teoria do Diálogo de Fontes.

Aludido estudo possui como escopo enfatizar as peculiaridades existentes no regime jurídico que rege a responsabilidade civil pelo tratamento em inobservância à LGPD quando este ocorrer na perspectiva do e-commerce.

Isto porque, embora a fixação de citado regime jurídico se valha de importantes previsões normativas da lei de proteção de dados, a ocorrência do tratamento de dados no âmbito consumerista culmina em notórias especificidades em face da adequação ao CDC, mormente no que diz respeito ao fundamento a responsabilidade civil a ser aplicada.

4.1. Os Efeitos da Pandemia no *E-Commerce* e a Intensificação da Vulnerabilidade do Consumidor

A evolução do comércio ao longo da história sempre manteve estrita relação com as necessidades da respectiva sociedade. Diante disso, as modalidades de transações que surgiram baseadas no escambo, evoluíram ao ponto de possibilitar respectivos negócios por via eletrônica.

O comércio eletrônico é resultado da evolução tecnológica das últimas décadas. Na era digital, na qual relações se tornaram cada vez mais virtuais, o *e-commerce* era algo impreterível.

Importante trazer a lume que o comércio eletrônico na segunda década do século XXI ainda era visto com cautela pelos consumidores, que guardavam uma predileção pelo comércio físico, em razão das maiores vulnerabilidades e desconfianças trazidas pelo *e-commerce*.

No entanto, o que era uma alternativa, tornou-se uma necessidade a partir do início de 2020, com a Pandemia do SARs-Cov-2 (Covid-19).

As incertezas trazidas pelo cenário pandêmico tiveram como principal efeito a adoção de medidas que objetivavam o distanciamento entre pessoas, de modo a diminuir a contaminação que se alastrava. Como consequência, vários comércios físicos tiveram suas portas fechadas durante grande período, só permanecendo abertos os serviços considerados essenciais pelo governo.

A realidade de *Lockdown*, contudo, trazia uma outra problemática: a necessidade dos consumidores por adquirir determinados produtos, assim como a imprescindibilidade de os comerciantes realizarem sua atividade econômica.

Em vista desse panorama, o empreendedorismo novamente se reinventou. Desde pequenos empresários de lojas físicas, a grandes redes de lojas, passaram a ter o *e-commerce* como seu principal mecanismo de lucro. O comércio eletrônico, que até então era visto como meio alternativo para os consumidores, passou a ser o principal meio de compra.

Como apontam Rezende, Marcelino e Miyaiji (2020, p. 63):

> O cerceamento do direito constitucional de ir e vir trouxe, por um lado, limitações físicas à realização de vendas e à geração de receita para as empresas, mas, por outro, alavancou a expansão do e-commerce que já apresentava uma trajetória de crescimento ao longo dos últimos 5 anos.

Sobre o aumento dessa modalidade de Comércio, pesquisa realizada pela ABComm e Neotrust, e divulgada pelo site de notícias G1, em matéria produzida por Darlan Alvarenga, indica que :

> [...] o crescimento nas vendas foi de 68% na comparação com 2019, elevando a participação do e-commerce no faturamento total do varejo, que passou de 5% no final de 2019 para um patamar acima de 10% em alguns meses do ano passado.” (ALVARENGA,2021).

A intensificação do e-*commerce* durante a Pandemia do Coronavírus, além de fundamental em vista do cenário pandêmico, é fato inerente aos benefícios trazidos por esse meio de transação. Sobre referidas benesses, leciona Tarcísio Teixeira (2015, p. 30 e 31):

> [...] manter a hospedagem e o funcionamento de um estabelecimento virtual é proporcionalmente bem menos oneroso do que um estabelecimento físico, haja vista: a redução do custo com a manutenção de estoque, que pode ficar a cargo de fornecedores encarregados de despachar as mercadorias

> direta- mente aos clientes da loja virtual, por meio de comunicação eletrônica enviada pelo servidor desta; a diminuição da mão de obra; a redução das despesas com locação etc. Além disso, teoricamente, na internet não há limitação geográfica para se vender, tudo vai depender do valor do frete, da legislação aplicável, da carga tributária e alfandegária e da diferença de idiomas. Mesmo pequenas empresas podem comercializar seus bens para clientes localizados nas mais distantes e variadas localidades, com custos relativamente baixos, o que seria praticamente inviável se não fosse a rede mundial de computadores.

Ainda de acordo com Teixeira (2015, p.31), o comércio eletrônico possibilitaria a redução da cadeia produtiva dos bens, proporcionando a realização de compras sem limitação temporal, e a ascensão da atividade comercial em razão do Marketplace.

Sobrevém que, a vulnerabilidade do consumidor, indissociável da relação consumerista, torna-se mais latente no *e-commerce*. Isso porque, na grande maioria das vezes, a formação de aludida relação por via eletrônica está vinculada a um contrato de adesão.

Sobre os desdobramentos da supramencionada espécie de contrato, Cláudia Lima Marques (2002, p. 59) elucida que em aludidos casos, os consumidores adquirirão uma relação contratual “pronta e regulamentada”, sendo-lhes eliminado a faculdade de negociar de modo efetivo os termos e condições relevantes do contrato.

Essa unilateralidade na elaboração contratual por parte do fornecedor, somado com a mera adesão do consumidor, guarda maiores riscos no comércio eletrônico.

Os contratos de adesão eletrônicos são submetidos ao consumidor através dos termos de uso. Esses termos, em generalidade, são compostos por um extenso texto, com cláusulas redigidas em linguagem extremamente técnica, e outras de grande importância, que importam em renúncia a direitos e, sobretudo, em permissão pelo uso de dados pessoais.

Como aclara Cíntia Rosa Pereira de Lima (2014, p. 03):

> Entretanto os fornecedores de produtos e serviços disponibilizados através da internet veiculam contratos extremamente longos, com uma linguagem técnica (que não é de domínio comum) e misturam no meio de tantas cláusulas de estilo (boilerplates rules) outras cláusulas importantes e imprevisíveis, tais como a utilização dos dados pessoais dos usuários, a cláusula compromissória ou cláusula eletiva, a limitação da responsabilidade do fornecedor, dentre outros.

Não se ignorando a conveniência de que os consumidores virtuais lessem referidos termos de uso em sua totalidade e com cautela, na realidade, sabe-se que não é o que ocorre na prática. Primordialmente, em razão da linguagem extremamente técnica utilizada nesses termos de uso, de difícil compreensão para pessoas leigas, violando o princípio da transparência aduzido no artigo 6º, inciso VI, da LGPD, segundo o qual, deve ser garantido aos titulares dos dados pessoais "[...] informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;" (BRASIL, 2018).

Ademais, levando em consideração a sociedade da Pós- Modernidade, não se pode olvidar da imediatidade e rapidez que marca os atos humanos.

Assim, na maioria das vezes, os consumidores virtuais realizam compras visando a facilidade, pensando nas consequências presentes daquela compra, e não nas futuras. Por conseguinte, na maioria das ocasiões, esses consumidores restringem-se a apresentar concordância ao termo de uso, sem nem mesmo tomar conhecimento de seu teor e pensar nos efeitos dessa adesão, e tampouco refletir que acaba de celebrar um contrato de compra e venda eletrônico.

À luz dessas ponderações, sem embargo ao dever do consumidor de ler o contrato eletrônico, há que ser sopesada sua vulnerabilidade.

Imprescindível rememorar que um dos princípios orientadores do Código de Defesa do Consumidor é justamente o dever de informação do fornecedor. Nos termos do que ensina o art. 46 da legislação consumerista, *ipsis litteris*:

> Os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo, ou se os respectivos instrumentos forem redigidos de modo a dificultar a compreensão de seu sentido e alcance. (BRASIL, 1990)

Como se observa, o dispositivo supracitado trata do dever de oportunizar a informação sobre o conteúdo do contrato. Ganha relevância nesta discussão a segunda parte da norma, que dispõe que os contratos não vincularão os consumidores caso tenham sido elaborados visando dificultar a compreensão de suas cláusulas.

De acordo com Lima Marques (2002, p. 668), cabe realizar a interpretação do que seria a dificuldade de compreensão, que, segundo a

professora, seria entendido pelos tribunais como “conhecimento jurídico do consumidor médio, isto é, de homem atento, mas sem formação específica”.

Nesse sentido, de forma a concretizar o direito da proteção do consumidor, o Código de Defesa do Consumidor e o Código Civil trouxeram diversos dispositivos com o intuito de equilibrar a relação contratual consumerista, sobretudo nos contratos de adesão.

Merece destaque a previsão quanto à nulidade das cláusulas consideradas abusivas em seu artigo 51. Na mesma linha de raciocínio, disciplina o Código Civil no artigo 424 que “Nos contratos de adesão, são nulas as cláusulas que estipulem a renúncia antecipada do aderente a direito resultante da natureza do negócio.” (BRASIL, 2002)

Por sua vez, tanto o art. 423 do Código Civil e art. 47 do Código de Defesa do Consumidor preveem a interpretação mais benéfica ao aderente de cláusulas em contrato de adesão.

De modo evidente, tanto o legislador consumerista quanto o civil objetivaram proteger o consumidor diante dos contratos de adesão. Conseguintemente, considerando a própria finalidade do legislador brasileiro, a mera aceitação dos termos de uso em um contrato eletrônico não vincula por completo o consumidor, devendo ser tomado como parâmetro para análise a forma que esses termos são redigidos.

Cabe pontuar que a proteção do consumidor também deve estar em diálogo com o dever deste de se informar. Isto é, para que de fato haja a vinculação do consumidor ao contrato eletrônico, imprescindível se faz que as cláusulas sejam redigidas em linguagem acessível ao homem médio.

De mais a mais, compete também ao fornecedor colocar em destaque cláusulas que ganham considerável importância naquela relação contratual, como cláusulas restritivas de direitos ou aquelas que disponham sobre o consentimento para o uso de dados pessoais. Como elucida Bruno Miragem (2019, p, 18):

> Neste caso, só é reconhecido como eficaz o consentimento quando aquele que manifesta vontade teve as condições plenas de compreender o conteúdo da sua decisão e de que modo ela repercute em relação aos seus interesses pressupostos. Consentimento daquele que decide a partir de informações incorretas ou incompletas não é reconhecido como tal, de modo a tornar ilícita, no âmbito do tratamento dos dados pessoais, quaisquer operações que venham a se basear nele.

Estando os termos de uso em conformidade à legislação consumerista, não pode o consumidor invocar sua vulnerabilidade na hipótese de este não ter se atentado aos termos de uso. Como ensina Cíntia Rosa Pereira de Lima (2014, p.12):

> Isto porque o usuário não pode se beneficiar de sua própria torpeza, alegando a ausência de consentimento fundamentada no fato dele mesmo não ter lido o contrato, dando ensejo à aplicação da vedação de comportamentos contraditórios *("venire contra factum proprio")*. Por outro lado, o fornecedor deve empregar em suas práticas comerciais uma técnica tal que obtenha a manifestação expressa da anuência do usuário como condição *sine qua non* para a validação desta transação eletrônica.

Desta feita, ainda ponderando os mecanismos legais de proteção do consumidor, conclui-se que estes não são capazes de estancar sua vulnerabilidade, sobretudo no *e-commerce*.

A mera concordância com os termos de uso, sem ter conhecimento do que nele está previsto, pode trazer danos irreparáveis ao consumidor eletrônico, que na maioria das vezes tem sua privacidade violada por sua própria anuência, a qual é viciada. Com a pandemia, essa vulnerabilidade e violação da privacidade do consumidor eletrônico têm se tornado constante na vida dos consumidores.

4.2. O Impacto da LGPD no Comércio Eletrônico

Como já ressaltado, a Lei Geral de Proteção de Dados foi uma legislação imprescindível à Pós-modernidade. A sociedade da economia informacional passou a ter sua privacidade extremamente violada, sobretudo, pela utilização de dados pessoais por terceiros. Como lecionam Tepedino, Terra e Guedes (2020, p. 283):

> O desenvolvimento eletrônico das relações humanas – hoje considerada realidade irreversível – torna inafastável o fornecimento de informações pessoais. A ausência de instrumentos para disciplinar o uso e a integridade dos dados de cada pessoa, sobretudo aqueles considerados sensíveis, impede o pleno exercício da liberdade, diante do papel predominante da informação para as escolhas individuais. Uma lei geral de proteção de dados pessoais que leve em conta os diversos valores existenciais alcançados pela circulação das informações, prevendo ferramentas específicas de controle, afigurava-se, por isso mesmo, indispensável para garantir – e fomentar – essa nova face da privacidade.

Nessa perspectiva, comporta ênfase que, decerto, um dos principais desdobramentos do desenvolvimento tecnológico das últimas décadas é o comércio

eletrônico. Tal qual foi exposto no tópico anterior, a pandemia do Covid-19 alavancou exponencialmente o *e-commerce*, que já vinha crescendo em ritmo acelerado nos últimos anos, o que, indubitavelmente, tem se tornado tendência.

O crescimento do *e-commerce* foi paralelo ao início da vigência da LGPD. Sem dúvidas, ainda que não houvesse pandemia, a modalidade virtual de comércio seria uma das mais afetadas pela legislação de proteção de dados. Sem embargo, com o crescimento significativo dessas transações, a LGPD passou a impactar desde pequenos comerciantes eletrônicos a grandes empresas nesse ramo.

Ao realizar uma simples compra pela internet, o consumidor é instado a fornecer uma série de dados pessoais, como nome, número de R.G. e CPF, endereço, número de cartão de créditos, dentre outras informações. Esses dados, geralmente, são repassados para outros envolvidos na cadeia do comércio eletrônico, como transportadores, empresas especializadas em pagamento, dentre outros.

Sucede-se também que, ao navegar pela internet, visando realizar determinada compra, por exemplo, em poucos minutos o consumidor é surpreendido por diversos anúncios relacionados ao objeto de compra pretendido. Isso é consequência de uma mera aceitação dos termos denominados cookies, em uma caixa de diálogo. Como ensina Lima (2014, p. 14):

> Assim, os cookies (registros de acesso dos sites pelos quais navega o usuário) e o spyware (programa de computador espião que armazena as senhas de segurança de uma conta de email ou outros serviços) podem ser instalados no computador de um usuário, com a sua própria “concordância” tácita, porque clicou em uma caixa de diálogo que leu e concorda com todos os termos do contrato, dentre os quais a cláusula que autoriza o fornecedor a instalar cookies e spyware na máquina do usuário.

Os cookies, de forma genérica, são arquivos que ficam salvos no computador do usuário e registram sua atividade na rede. Na mesma linha do que foi discutido sobre os termos de uso, os consumidores eletrônicos aceitam esses cookies, sem nem mesmo saber o que são. Insta salientar que, na maioria dos casos, o termo de aceitação de cookies é apresentado ao usuário da *web* como forma de facilitar sua navegação, omitindo sua óptica negativa, qual seja, o rastreamento da navegação do indivíduo.

Diante da realidade na qual, através da captação desses dados de visitação de sites, é possível criar um perfil do consumidor, direcionando-o anúncios conforme seu suposto caráter de consumo, esses perfis adquirem grande valia no comércio eletrônico, sendo, inclusive, comercializados. Existem empresas especializadas no armazenamento e venda de dados, configurando-se o denominado mercado de dados pessoais.

Como definem Silveira, Avelino e Souza (2016, p. 219/2020), o mercado de dados pessoais consubstancia-se nas trocas econômicas destinadas ao comércio de informações relativas a uma pessoa identificada ou identificável, e se nortearia perante as necessidades de referidos dados por empresas, e instituições públicas. Assim, de acordo com os autores, a interceptação de dados pessoais seria um bem econômico de grande valia, funcionando, em suas palavras, como "[...] moeda paga pelo uso gratuito de plataformas, sites e serviços online."

Os cookies também demonstram sua imprescindibilidade para marketing digital, de modo a direcionar anúncios e propagandas. Nessa perspectiva, ao navegar pela *web*, o *ciberconsumidor* tem sua movimentação registrada pelos navegadores, que criam um perfil de sua navegação. Com esse perfil criado através de coletas de dados pessoais, que muitas vezes são vendidos para os fornecedores virtuais, é possível direcionar ao consumidor eletrônico uma série de anúncios e propagandas, aumentando as chances da aquisição do produto vendido, o qual, usualmente, nem mesmo é necessário ao consumo naquele momento. Em outras hipóteses, esses cookies são coletados pelos próprios fornecedores. Incontestável o valor dos dados pessoais nesse contexto.

Segundo, Basan e Faleiros Júnior (2020, p. 08) "Essa nova realidade apresenta particularidades, tendo em vista que a publicidade incessante cria expectativas e comportamentos orientados ao consumo, se tornando irresistíveis [...]".

À vista disso, observa-se que a interceptação de dados pessoais é inerente ao comércio eletrônico, sobretudo em razão da coleta de referidos dados em uma compra e venda virtual, pelo comércio de dados pessoais coletados por *cookies*, bem como pela utilização desses dados por fornecedores para o direcionamento de publicidade a um público- alvo.

O fornecimento desses dados pessoais pelo *ciberconsumidor* se dá com base no Princípio da Confiança, o qual, em inúmeras ocasiões, é violado pelos

fornecedores eletrônicos. Não raras as vezes são exigidos do consumidor dados além do necessário para a realização de uma compra, objetivando criar um banco de dados em relação a ele, prática a qual deve ser combatida em razão do princípio da finalidade, orientador do tratamento de dados, nos termos já ressaltados nesta pesquisa.

Tendo em consideração todo o exposto, imprescindível a proteção especial do consumidor nos contratos de compra e venda do *e-commerce*.

Neste ângulo, de modo evidente, adequa-se o consumidor eletrônico no que a Lei Geral de Proteção de Dados trata como titular de dados pessoais, enquanto o fornecedor dessa relação comercial, e outros envolvidos na cadeia da respectiva modalidade de comércio, como agentes de tratamento.

Partindo dessa premissa, infere-se que a coleta, tratamento e descarte desses dados pessoais pelos agentes de tratamento envolvidos na cadeia de comércio por via virtual deve ser dar em perfeita adequação ao que dispõe a LGPD, podendo estes estarem sujeitos à responsabilização civil ou sanções administrativas, nos termos do que preconiza a lei nº 13.709/2018.

Em vista do relatado, o mero consentimento para o tratamento desses dados pessoais no comércio eletrônico pode ser viciado, nos moldes da discussão do subtópico anterior, não podendo ser considerado como absoluto.

Muitas vezes a cláusula de permissão para o uso desses dados é mesclada em um texto complexo, ou apresentada como aceitação de cookies que, supostamente, teria único objetivo de facilitar a navegação do consumidor, sendo que, em verdade, não é o que advém, rompendo-se a confiança depositada pelo consumidor no fornecedor eletrônico. Verifica-se, de forma latente, um desvio da finalidade da cláusula de aceitação dos *cookies*.

Nessa perspectiva, aplica-se na construção do raciocínio último vetor interpretativo fixado no tópico “2.4” desta pesquisa, sob análise de julgamento firmado pelo Tribunal de Justiça da União Europeia (UNIÃO EUROPEIA, 2021, p. 56) no qual este entendeu pela não validade do consentimento dado por uma opção pré-validada fixada em razão de *cookies* , extraindo-se deste julgado a imprescindibilidade do consentimento expresso e específico para o tratamento de dados.

.Assim, a LGPD torna-se um mecanismo imperioso para efetivar o direito à privacidade e à proteção de dados pessoais no *e-commerce*, aplicando-se

essa a todos que realizam o tratamento de dados pessoais. Desta feita, observa-se a imprescindibilidade da observância do dever de segurança dispostos no artigo 46 e seguintes da legislação. Segundo leciona Tarcísio Teixeira (2021, p. 94):

> As boas práticas deverão fazer parte da rotina dos empregados, dos prestadores de serviço e de quaisquer outras pessoas que tratem dados, a fim de evitar o acesso não autorizado de dados, situações acidentais ou ilícitos de destruição. Percebe-se que a lei não exclui a responsabilidade do agente nesses casos; pelo contrário, o coloca como ator na prevenção de tais incidentes, sendo sua obrigação adotar as medidas previstas no caput do art. 46.

Considerando a complexidade das obrigações impostas pela legislação de proteção de dados, é inestimável a importância de profissionais habilitados na área para evitar possível descumprimento das disposições legislativas, podendo incorrer os agentes de tratamento em responsabilidade civil e submeter-se em penalidades administrativas.

Nessa sistemática, mostra-se indispensável um programa de *compliance* em empresas que tratam de dados pessoais, devendo estas adaptarem suas políticas de privacidade, tal como frequentemente retificar seu programa de governança, a fim de que estejam em conformidade com a legislação (TEIXEIRA, 2021, p. 95).

Infere-se que através de mecanismos efetivos, os envolvidos na cadeia de *e-commerce* devem respeitar, em todos os atos realizados, o direito à privacidade e à proteção de dados pessoais, estruturando suas respectivas atividades às disposições da LGPD, sob pena de serem responsabilizados civilmente e administrativamente.

Por consequência, constata-se que a LGPD é mais um ponto influenciador a adoção de programas de *compliance* em empresas, sejam elas de pequeno ou grande porte, considerando enquadraram-se como agentes de tratamento nos termos da legislação de proteção de dados.

4.3. Responsabilidade Civil no Comércio Eletrônico à Luz da Legislação de Proteção de Dados: uma Interpretação Sistemática entre as Normas

À letra do que foi pontuado sobre o impacto da Lei nº 13.709/2018 no comércio eletrônico, ganha ênfase a previsão do art. 45 de referida legislação, que preconiza que a responsabilidade civil dos agentes de tratamento em razão das

violações à LGPD, no âmbito da relação de consumo, deve ser disciplinada pelo Código de Defesa do Consumidor (BRASIL, 2018).

Inicialmente, cabe sublinhar que citada disposição não deve ser interpretada *ipsis literris*, considerando a necessidade de diálogo de fontes no ordenamento jurídico. Assim, a interpretação sistemática do art. 7º do CDC com o art. 64 da LGPD leva à tese de que os direitos dos titulares de dados previstos em ambas as normas, devem ser cumulados e compatibilizados (MIRAGEM, 2019, p.04).

Por esse raciocínio, salienta-se que o art. 43 do Código de Defesa do Consumidor (BRASIL, 1990) que trata sucintamente “Dos Bancos de Dados e Cadastros de Consumidores”, ganha novos contornos com a lei de proteção de dados.

. Em face dessas ponderações, observa-se que diante de uma violação do direito à proteção de dados pessoais, no âmbito do consumo, além das previsões pertinentes no CDC, devem ser aplicadas as disposições da LGPD, sendo sempre utilizada a interpretação mais benéfica ao consumidor. Conforme ensinamento de Fernando Tasso (2020, p. 113):

> Identifica-se que, no atual panorama Constitucional e infralegal, a relação entre os microssistemas não é de mera intersecção, mas de continência, na medida em que a toda e qualquer violação de direito do consumidor deve-se atribuir, dentre os regimes jurídicos elegíveis, o que melhor atenda à defesa do consumidor.

De mais a mais, mostra-se que o vazamento de dados pessoais tem elevada probabilidade de incidência na perspectiva das relações consumeristas, razão pela qual se faz imprescindível a análise do regime jurídico da responsabilidade civil pelo tratamento de dados pessoais neste âmbito.

Aliás, há de se enfatizar que a própria LGPD reconhece em vários dispositivos a necessidade de proteção do consumidor no âmbito de referida lei. A exemplificar-se, pontua-se que entre os fundamentos da LGPD, está a proteção do consumidor, prevista no art. 2º, VI da lei citada (BRASIL, 2018).

No mesmo sentido, existe previsão no art. 18, §8º da lei de dados sobre a competência dos órgãos de defesa do consumidor para atuar, através de requerimento do titular dos dados pessoais, nas hipóteses de infração de seus direitos pelo controlador. Também há no art. 5- K, parágrafo único, a lei discutida

enuncia o dever de articulação entre a Autoridade Nacional de Proteção de Dados e outros órgãos titulares de competência afeta a proteção e dados, como exemplo os órgãos de defesa do consumidor (MIRAGEM, 2019, p. 02).

Anota-se que o principal impacto da previsão do art. 45 diz respeito à natureza da responsabilidade civil nos casos de violação de proteção de dados do titular no âmbito consumerista, seja no comércio eletrônico ou físico, que, a rigor, será considerada objetiva, afastando-se as divergências doutrinárias existentes na LGPD em referido tema.

Como já abordado, é defendido por Tepedino, Terra e Guedes (2020, p. 293) que a previsão do artigo 45 da LGPD seria irrelevante no caso de reconhecimento de uma responsabilidade objetiva em respectiva lei. Todavia, apesar de concordar-se com os autores no sentido do fundamento da responsabilidade civil na legislação de proteção de dados não ser objetiva, referido argumento não prospera, considerando que a redação de citado artigo implica em diversas consequências legais, e não apenas na migração de um sistema de culpa presumida para o de responsabilidade objetiva.

A regulação da responsabilidade civil pelo Código de Defesa do Consumidor, em se tratando de danos no âmbito da LGPD em relações consumeristas traz, além do fundamento objetivo da responsabilidade, implicações no regime de solidariedade, no prazo prescricional, entre outas inferências.

Em princípio, cabe destacar que, em caso de danos oriundos do tratamento inadequado de dados, estar-se-á, inequivocamente, diante de um fato do serviço, e as disposições legais dele decorrentes. Como leciona Bruno Miragem (2021, p. 498):

> Tratando-se de danos a consumidores decorrentes do tratamento indevido de dados, contudo, o art. 45 da LGPD, ao dispor que “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”, conduzem tais situações ao regime do fato do serviço (art. 14 do CDC). Neste caso, controlador e operador de dados respondem solidariamente assim como outros fornecedores que venham intervir ou ter proveito do tratamento de dados do qual resulte o dano. Incidem tanto as condições de imputação da responsabilidade pelo fato do serviço (em especial o defeito que se caracteriza pelo tratamento indevido de dados, ou seja, desconforme à disciplina legal incidente para a atividade), quanto as causas que porventura possam excluir eventual responsabilidade do fornecedor (art. 14, § 3º), que estão, porém, em simetria com o disposto no próprio art. 43 da LGPD.

Assim, imprescindível colacionar a redação do artigo 14, caput do CDC, que dispõe:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. [...] (BRASIL, 1991)

Em complementação, o legislador consumerista define no art. 14, §1º, inciso II, como serviço defeituoso aquele que não oferece a segurança que dele legitimamente se presume, considerando, entre outras hipóteses, o uso e os riscos que razoavelmente dele se esperam. (BRASIL, 1991)

O tratamento inadequado de dados pessoais é, indubitavelmente, um defeito relativo à prestação de serviços do fornecedor, ora agente de tratamento. Cabe ao fornecedor, que é considerado como agente de tratamento, observar o *standard* de condutas disciplinados pela legislação.

No caso de tratamento de dados em inobservância aos ditames da LGPD na perspectiva das relações consumeristas, denota-se a ocorrência de grave falha na prestação de serviços ao consumidor, considerando a violação ao princípio da confiança, bem como o descumprimento do dever de segurança preconizado pela lei de proteção de dados.

Esse raciocínio encontra embasamento no art. 14, §1º, inciso II, da legislação (BRASIL, 1990), pois haveria a fato do serviço por esse não oferecer a segurança que dele se imaginava, tomando como norte os usos e os riscos que dele razoavelmente se esperam, isto é, ao fornecer seus dados pessoais para a realização de uma compra, o consumidor imagina que esses dados estejam protegidos.

No entanto, o possível o vazamento desses dados transparece o descumprimento do fornecedor/agente de tratamento ao *standard* de condutas preconizadas pela legislação de tratamento de dados, falhando com o dever de segurança imposto pela LGPD. Ressalta-se que o artigo citado, no que tange ao dever de segurança do fornecedor, deve ser interpretado em consonância com o art. 44 da Lei Geral de Proteção de Dados.

Nesse raciocínio, segundo leciona Miragem, a análise desses riscos está estritamente relacionada com as tecnologias de informação disponíveis à época do tratamento:

> Em outros termos, trata-se de situar, em relação à responsabilidade pelos danos causados em relação ao tratamento indevido de dados, qual o lugar dos riscos do desenvolvimento, considerando, neste caso, a própria previsibilidade de uma atualização e avanço técnico em atividades vinculadas à tecnologia da informação, mais veloz do que em outras atividades econômicas. (MIRAGEM, 2019, p, 36)

Uma vez adequado o vazamento de dados pessoais como fato do serviço, comporta ênfase que nesta ocorrência, os fornecedores responderão objetivamente em relação aos danos ocasionados aos titulares, ora consumidores, nos termos do art. 14, *caput*, primeira parte do CDC (BRASIL, 1990), considerando ser o vazamento de dados pessoais defeito relativo à prestação de serviços, de modo que essa deveria ter observado o *standard* de condutas e dever se segurança impostos pela legislação de tratamento de dados.

Salienta-se que o fato do serviço em razão do vazamento de dados pessoais implica na responsabilidade entre todos aqueles considerados como fornecedores, nos termos do artigo 3º, caput, da Lei nº 8.078/90 (BRASIL, 1990).

Ademais, como dispõe o art. 7º, parágrafo único, do Código de Defesa do Consumidor: “Tendo mais de um autor a ofensa, todos responderão solidariamente pela reparação dos danos previstos nas normas de consumo.” (BRASIL, 1990)

Infere-se, portanto, que como mais um meio de tutela efetiva dos titulares dos dados pessoais, além da solidariedade prevista na LGPD no art. 42, §1º (BRASIL, 2018), nada impede a aplicação, em se tratando de relação consumerista, da solidariedade prevista no CDC.

Considerando a previsão do art. 45 da Legislação de Proteção de Dados, presumir ia-se a aplicação das hipóteses de excludente de responsabilidade do art. 14, §3º, do CDC, que dispõe, *in verbis*:

> Art. 14. [...]
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
> I - que, tendo prestado o serviço, o defeito inexiste;
> II - a culpa exclusiva do consumidor ou de terceiro.
> (BRASIL, 1990)

Ocorre que, em sintonia com o preconizado por Fernando Tasso, já colacionado acima, ainda que se tratando de relações consumeristas, sempre deve ser considerado a interpretação mais benéfica ao consumidor. Assim sendo, demonstra-se mais adequado a aplicação das excludentes previstas no art. 43, inciso I a III, da LGPD, considerando ser um rol mais específico, ao mesmo tempo que inspirado no próprio CDC. De acordo com Tasso (2020, p. 113):

> No que concerne às hipóteses excludentes de responsabilidade, contudo, o sistema a ser seguido deve ser, necessariamente, o do artigo 43 da Lei Geral de Proteção de Dados em detrimento daquele previsto no artigo 12, §3º do Código De defesa do Consumidor.

Essa análise conclusiva partiria da premissa de que as previsões dos incisos I e III do art. 43 da LGPD seriam equivalentes às hipóteses descritas no art. 14,§ 3º do CDC, ao passo que o inciso II do citado artigo 43 corresponderia a uma diferenciação entre os sistemas de responsabilidade civil previsto na legislação consumerista e na Lei de Proteção de Dados, sendo nesta última um regime de responsabilidade subjetiva (TASSO, 2020, p. 113).

Outra implicação do art. 45 da LGPD é a adoção do prazo prescricional quinquenal relativo ao fato do serviço, previsto no art. 27 do Código de Defesa do Consumidor. Segundo Bruno Miragem (2021, p. 498):

> Outro efeito prático da remissão do art. 45 da LGPD ao regime de reparação próprio da legislação de proteção do consumidor será a submissão de eventuais pretensões de reparação dos consumidores ao prazo prescricional previsto no seu art. 27 do CDC, de cinco anos contados do conhecimento do dano ou de sua autoria.

Nesta conjuntura, constata-se que diante do vazamento de dados pessoais no âmbito consumerista, ou outra violação da LGPD pelo agente de tratamento, o titular lesado terá o prazo de 5 (cinco) anos para demandar o ofensor, a conta da data do conhecimento do dano, ou de sua autoria.

Mister observar ainda que, no caso de violação do dever de proteção de dados no âmbito consumerista, a aplicação de inversão do ônus da prova *ope judices* em relação ao consumidor, por interpretação do art. 6º, inciso VIII do CDC (BRASIL,1990), com o art. 42, §2º, da LGPD, ganha maior perspectiva, tendo em vista a própria previsão do art. 4º, inciso I, da legislação consumerista quanto ao reconhecimento da vulnerabilidade do consumidor (BRASIL, 1990)

Resta evidente pelo apregoado que, não obstante às previsões protetivas da LGPD quanto ao titular de dados, a disposição do art. 45 de referida lei, realizando uma interpretação sistemática entre a lei nº 13.709/18 com o CDC, atribui maior caráter protecional ao titular de dados como consumidor, em virtude da interpretação sistemática de duas legislações com enfoque constitucional.

5 CONCLUSÃO

Conforme exposto ao longo desta pesquisa, são imensuráveis os impactos trazidos pela Lei nº 13. 709 /18 à sociedade hodierna. A legislação, que se mostrava indispensável diante da realidade que se faz presente na economia informacional, impôs a necessidade de adequação dos agentes de tratamento de dados pessoais às suas previsões, sob pena de responsabilização administrativa, civil, e, em sendo o caso, até mesmo penal.

Fruto de um vagaroso e gradual avanço legislativo, a LGPD teve como base legislativa outro marco regulatório de grande importância no cenário normativo internacional: o Regulamento Europeu de Proteção de Dados (GDPR).

Considerando a notória similitude normativa entre os marcos regulatórios, no desenvolvimento da presente pesquisa foi possível, a partir da análise de julgados do Tribunal de Justiça da União Europeia no âmbito da proteção de dados pessoais, extrair vetores interpretativos a serem aplicados para melhor compreensão da Lei Geral de Proteção de Dados Brasil, dentre os quais, cita-se a delimitação do ato ilícito a partir da necessidade/finalidade do tratamento de dados pessoais e da ponderação de princípios.

A necessidade de uma interpretação da legislação brasileira de proteção de dados sob o viés do direito comparado se mostra fundada em dois fatos: primeiramente, em razão de sua recente vigência, de modo que os tribunais brasileiros ainda estão iniciando a fixação de entendimento jurisprudencial sobre o tema. De outro lado, embora a importância atribuída à legislação para o Ordenamento Jurídico hodierno, certamente, ela não foi capaz de esgotar a regulação sob a temática da proteção de dados pessoais, pairando discussões sobre particularidades da LGPD, as quais aos poucos vão se consolidando em âmbito doutrinário e jurisprudencial.

Nessa lógica, foi possível constatar que, de longe, a temática que guarda maior debate em sede doutrinária diz respeito às previsões quanto a responsabilidade civil na legislação.

Assim, no estudo realizado fez-se imprescindível discorrer sobre os pressupostos da responsabilidade civil no âmbito da LGPD, quais sejam, o ato ilícito, o nexo de causalidade, o dano, e, para parte da doutrina, o elemento culpa.

Em relação ao elemento dano, na perspectiva do dano moral, inferiu-se, através da análise doutrinária e jurisprudencial, que a mera violação da legislação de proteção de dados, sem a prova das consequências demonstrativas de seu condão de causar potencial prejuízo grave extrapatrimonial ao titular de dados (ou terceiro), não pode ser ensejadora, como regra, da responsabilização civil, isto é, não se pode aplicar na LGPD, de modo geral, a previsão de um dano *in res ipsa*.

Consoante análise doutrinária realizada, compreender o dano moral na legislação como presumido, sobretudo em face das proporções atuais do tratamento de dados em massa, transformaria o judiciário em uma espécie de loteria, fenômeno o qual já é observado na perspectiva do dano moral para além do microssistema da LGPD.

Digno enfatizar que aludida conclusão se deu pela da aplicação de um dos vetores interpretativos fixados no subtópico “2.4”, a partir da análise de julgado do Tribunal de Justiça da União Europeia do qual se extraiu que nem sempre a mera violação de um direito ensejará necessário prejuízo ao seu titular.

Aliás, como foi evidenciado, a tese fixada nesta pesquisa, a partir de análise doutrinária, também tem sido adotada pelo Tribunal de Justiça de São Paulo, em ações indenizatórias recentes no âmbito de proteção de dados que chegaram à sua análise, já sob o viés da LGPD.

No julgamento de mencionadas ações, o Tribunal firmou o entendimento de que a mera violação da LGPD não se consubstancia, por si só, como dano moral, pelo hipotético prejuízo, devendo este restar devidamente demonstrado.

Nesse sentido, observou-se que o dano moral *in res ipsa* na LGPD, a exemplo do que se verifica no Ordenamento Jurídico em geral, será tido como exceção, e, na maior parte das vezes, estará relacionado ao inadequado tratamento de dados sensíveis, conforme ficou implícito no julgamento da Apelação nº 1001032-45.2021.8.26.0177 pelo Tribunal de Justiça de São Paulo.

Outro ponto de relevantes divergências doutrinárias concerne ao fundamento da responsabilidade civil na LGPD, isto é, a presença ou não do elemento “culpa” como pressuposto do dever de indenizar.

Sucede-se que, ao trazer na LGPD um microssistema de responsabilidade civil em 4 (quatro) artigos, o legislador deixou de prever expressamente sobre o fundamento de referida responsabilidade.

Nessa perspectiva, com argumentos de grande pertinência, a doutrina civilista, em processo de formação sobre a temática, se divide entre três correntes principais que poderiam fundamentar a responsabilidade na legislação: a responsabilidade objetiva, a responsabilidade subjetiva e a responsabilidade proativa.

A partir da análise das previsões da LGPD, suas finalidades, e, sobretudo, da análise do cenário atual do instituto da responsabilidade civil, concluiu-se que a responsabilidade prevista na lei tenderia para um fundamento de culpa presumida, a ser norteada pelo dever de segurança dos agentes de tratamento.

Nos termos expostos, ao elencar um rol de condutas de segurança e boas práticas a serem aplicadas pelos agentes de tratamento, seria incompatível a previsão de uma responsabilidade objetiva implícita que deixasse de valorizar o cumprimento de aludidas previsões.

De toda sorte, se considerada como estritamente subjetiva a responsabilidade na legislação, estaria se ignorando estado atual da sociedade hodierna, a qual demanda uma constante assunção de riscos, mormente no âmbito da economia digital.

Dessa forma, atingiu-se a conclusão que a responsabilidade civil na LGPD estaria no ínterim entre dois extremos, de modo que a ocorrência de um dano ao titular ou terceiro no âmbito da lei de proteção de dados ensejaria uma presunção de culpa por parte do agente de tratamento, a qual seria afastada caso este demonstrasse a adoção de todas as medidas eficazes para evitar o dano, nos termos das excludentes de responsabilidade prevista no artigo 43, inciso II, da lei.

Elucida-se que, nesse caso, o ato ilícito estaria presente diante da violação do direito à proteção de dados pessoais, no entanto, restando devidamente comprovada o exercício do dever de segurança por parte do agente de tratamento, sua culpa fica afastada, e, conseguintemente, o dever de indenização.

Vale ressaltar que citado dever se segurança deve ser parametrizado conforme as disposições legais e tecnologias existentes quando do tratamento de dados objeto de análise.

No desenrolar deste estudo, também foi asseverado sobre a necessidade de interpretação da LGPD em um diálogo de fontes com o restante do ordenamento jurídico, promovendo a fixação de vetores interpretativos a partir da

relação entre o microssistema da lei geral de proteção de dados, e o sistema normativo vigente.

Desse modo, adentrou-se à delimitação do regime jurídico de responsabilidade civil aplicado a um dos setores mais impactados pela LGPD, o comércio eletrônico, apresentando suas principais peculiaridades em relação ao sistema normativo previsto pela lei de proteção de dados.

Por força da disposição do artigo 45 da lei de proteção de dados, em caso de danos ocasionados pelo tratamento de dados pessoais no âmbito consumerista, devem ser aplicadas as previsões do Código de Defesa do Consumidor.

Por consequência, a fixação dos parâmetros da responsabilidade civil no comércio eletrônico no âmbito da proteção de dados necessita de uma interpretação sistemática entre LGPD, CDC, Constituição Federal, e demais diplomas legislativos aplicáveis.

De tal feita, nestas hipóteses, tendo como norte que o tratamento de dados pessoais pelo fornecedor se configura como cristalina falha em sua prestação de serviços a qual, por orientação da LGPD, deveria se dar em observância ao dever de segurança, observou-se que estaria presente nestas hipóteses o fato do serviço, o qual traz como principal consequência, a responsabilização objetiva do fornecedor, ora agente de tratamento.

De toda sorte, constatou-se que a previsão do artigo 45 da Lei nº 13 709/2018 também traz implicações quanto à responsabilização solidária entre todos aqueles considerados fornecedores, para efeito do CDC, bem como a adoção de um prazo quinquenal para pleitear a reparação em juízo nessas relações consumeristas, a contar da data da descoberta do dano e sua autoria.

Destarte, foi possível deduzir que nas hipóteses de danos oriundos a partir do tratamento de dados pessoais nas relações consumeristas, o aspecto protecional disposto na LGPD ganha maior salvaguarda, considerando a expressa previsão legal quanto à hipossuficiência do consumidor. Referida conclusão não poderia ser diferente, considerando ser o direito à proteção do consumidor, bem como o direito à proteção de dados pessoais, elencados constitucionalmente.

Em conclusão, verifica-se que a Lei Geral de Proteção de Dados, não obstante ao avanço normativo trazido para o ordenamento jurídico brasileiro, ainda se mostra como um terreno fértil para diversas discussões doutrinárias e

jurisprudenciais, cujos posicionamentos tenderão a se formar com o tempo, sempre em adequação aos avanços tecnológicos e informacionais experimentados pela sociedade líquida.

O presente trabalho, sem o objetivo de esgotar a análise do tema, teve como escopo apresentar um panorama das divergências que já vêm se formando na doutrina sobre a LGPD, fixando possíveis posicionamentos dos tribunais pátrios, conforme delimitação realizada sob a perspectiva do direito comparado da União Europeia.

REFERÊNCIAS

A. A. de .; MARCELINO, J. A. .; MIYAJI, M. . A REINVENÇÃO DAS VENDAS: AS ESTRATÉGIAS DAS EMPRESAS BRASILEIRAS PARA GERAR RECEITAS NA PANDEMIA DE COVID-19. **Boletim de Conjuntura (BOCA)**, Boa Vista, v. 2, n. 6, p. 53–69, 2020. DOI: 10.5281/zenodo.3834095 . Disponível em: https://revista.ioles.com.br/boca/index.php/revista/article/view/113. Acesso em: 12 abr. 2022.

ALVARENGA, Darlan. Com pandemia, comércio eletrônico tem salto em 2020 e dobra participação no varejo brasileiro. **G1**, 26.fev.2021. Disponível em:https://g1.globo.com/economia/noticia/2021/02/26/com-pandemia-comercio-eletronico-tem-salto-em-2020-e-dobra-participacao-no-varejo-brasileiro.ghtml. Acesso em 12 abr. 2022.

BASAN, A. P.; FALEIROS JÚNIOR, J. L. DE M. A proteção de dados pessoais e a concreção do direito ao sossego no mercado de consumo. **civilistica.com**, v. 9, n. 3, p. 1-27, 22 dez. 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/565. Acesso em: 20 abr. 2022

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988, Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 14 ago. 2022.

BRASIL**. Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais [...]. Brasília: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 19 mai. 2022.

BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm#:~:text=DECRETO%20N%C2%BA%2010.474%2C%20DE%2026%20DE%20AGOSTO%20DE%202020&text=Aprova%20a%20Estrutura%20Regimental%20e,comiss%C3%A3o%20e%20fun%C3%A7%C3%B5es%20de%20confian%C3%A7a. Acesso em 21 ago. 2022.

BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados [...] . Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm#:~:text=DECRETO%20N%C2%BA%2010.474%2C%20DE%2026%20DE%20AGOSTO%20DE%202020&text=Aprova%20a%20Estrutura%20Regimental%20e,comiss%C3%A3o%20e%20fun%C3%A7%C3%B5es%20de%20confian%C3%A7a. Acesso em 21 ago. 2022.

BRASIL. **Lei nº 7.347, de 24 de julho de 1985**. Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente [...]. Brasília, DF, Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm. Acesso em: 19 mai. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 21 mai. 2022.

BRASIL. **Lei n º 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 21 mai. 2022.

BRASIL. **Lei nº 12.414, de 09 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento [...] . Brasília, DF, Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em 14 ago. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal[...]. Brasília, DF, Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 20 ago. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Senado Federal, 1988, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em 20 ago. 2022.

BRASIL. **Lei Nº 13.105, de 16 de Março de 2015.** Código de Processo Civil. Brasília, Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 21 mai. 2022.

BRASIL. **Lei. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 mai. 2022.

DIAS, Rui Belfort. **Da Responsabilidade Civil**. 11 ed. [Adaptado da obra de] José Dias Aguiar. Rio de Janeiro: Editora Renovar, 2006.

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: 28 de fevereiro de 2022.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In:* BIONI, Bruno (coord). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. p. 22-39. E-book.

DONEDA, Danilo. A Autoridade Nacional De Proteção De Dados E O Conselho Nacional de Proteção de Dados. *In:* BIONI, Bruno (coord). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. p.466-476. E – book.

ELER, Kalline Carvalho Gonçalves. A releitura da privacidade: do "direito de ser deixado só" ao direito à autodeterminação informativa. **Revista Internacional de Tecnología, Ciencia y Sociedad**, v. 5, n. 2, p. 185–196, 2016. Disponível em: https://journals.eagora.org/revTECHNO/article/view/1351. Acesso em 21 ago. 2022.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.

GODINHO, A. M.; QUEIROGA NETO, G. R.; TOLÊDO, R. C. M. A responsabilidade civil pela violação a dados pessoais. **Revista IBERC**, v. 3, n. 1, 3 abr. 2020. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/105 . Acesso em 24 fev. 2022.

HELMANN, Renê. O Dano Moral in res ipsa e sua dimensão probatória na jurisprudência do STJ. **Revista dos Tribunais Online**. vol. 291/2019, p. 311 – 336, Maio / 2019. Disponível em: https://www.academia.edu/39275961/O_DANO_MORAL_IN_RE_IPSA_E_SUA_DIMENS%C3%83O_PROBAT%C3%93RIA_NA_JURISPRUD%C3%8ANCIA_DO_STJ. Acesso em 01 mai. 2022.

HIRONAKA, Giselda Maria Fernandes Novaes. **Responsabilidade Pressuposta**. Belo Horizonte, Del Rey Editora, 2005.

ITÁLIA. **R.D. 16 marzo 1942, n. 262 Approvazione del testo del Codice Civile.** Disponível em: http://www.jus.unitn.it/cardozo/Obiter_Dictum/codciv/Lib4.htm . Acesso em 01 mai. 2022.

LGPD: a responsabilidade civil dos agentes de tratamento e possíveis causas de judicialização. [*S. l.: s. n*.], 2020. 1 vídeo (99min). Realizado pelo Tribunal de Justiça de Santa Catarina – TJSC. Disponível em: https://www.youtube.com/watch?v=Jg-IMDV-Q1M. Acesso em 21 jul. 2022.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. E-book.

LIMA, Cíntia Rosa Pereira de.. **O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos.** In: XXIII Congresso Nacional do CONPEDI, 2014, João Pessoa. XXIII Congresso Nacional do CONPEDI - TEMA: A Humanização do Direito e a Horizontalização da Justiça no século XXI. Florianópolis: CONPEDI, 2014.

LORENZON, Laila Neves. **ANÁLISE COMPARADA ENTRE REGULAMENTAÇÕES DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA (LGPD E GDPR) [...].** Revista do Programa de Direito da União Europeia – FGV, v. 1, p.39-52, 2021. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/article/view/83423 . Acesso em 04 set 2022.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 4 ed. São Paulo: Revista dos Tribunais, 2002.

MENDES, Laura Schertel Ferreira Mendes. **Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental.** São Paulo: Editora Saraiva, 2014. E-book.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais** | vol. 1009/2019 | Nov / 2019 DTR\2019\40668. Disponível em: https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em 15 maio 2022.

MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021.

MORAES, Maria Celina Bodin de. Conceito, função e quantificação do dano moral. **Revista IBERC**, Minas Gerais, v. 1, n. 1, p. 01 - 24, nov.-fev./2019.

MORAES, Maria Celina Bodin de. **Danos à Pessoa Humana: Uma leitura Civil-Constitucional dos Danos Morais**. Rio de Janeiro: Editora Renovar, 2003.

MORAES, Maria Celina Bodin de. **LGPD: um novo regime de responsabilização civil dito "proativo".** Editorial à Civilistica.com. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: https://civilistica.com/lgpd-um-novo-regime-de-responsabilizacao-civil-dito-proativo/. Acesso em 30 abr. 2022.

MULHOLLAND, Caitlin Sampaio. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?** MIGALHAS, 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-de-dados-pessoais--culpa-ou-risco. Acesso em 24 abr. 2022.

NOVAKOSKI, André Luiz Mota; NASPOLINI, Samyra Haydêe Dal Farra. **Responsabilidade Civil na LGPD: Problemas e Soluções.** Conpedi Law Reviex, v. 6, n. 1, p. 158174, 2020. Disponível em: https://indexlaw.org/index.php/conpedireview/article/view/7024. Acesso em 09 mar. 2022.

OLIVEIRA, Amanda Flavio de. et al. **Direito do Consumidor - 30 anos de CDC**. Rio de Janeiro: Grupo GEN, 2020. E-book.

OLIVEIRA, Ricardo. **LGPD: Como evitar as sanções administrativas**. São Paulo: Editora Saraiva, 2021. E-book.

PORTUGAL. **Decreto Lei nº 47 344, de 25 de Novembro de 1966** . Disponível em https://www.igac.gov.pt/documents/20178/358682/C%C3%B3digo+Civil.pdf/2e6b36d8-876b-433c-88c1-5b066aa93991. Acesso em 01 maio 2022.

PINHEIRO, Patrícia Peck. **PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N. 13.709/2018 (LGPD)**. São Paulo, Editora Saraiva, 2021. E-book.

REALE, Miguel. **Filosofia do Direito**, 20ª edição. São Paulo: Editora Saraiva, 2013. E-book.

RESPONSABILIDADE civil na LGPD. [*S. l.: s. n*.], 2021. 1 vídeo (96 min). Realizado pela Comissão de Proteção de Dados e Privacidade da OAB RJ. Disponível em: https://www.youtube.com/watch?v=obJEro6QjRA. Acesso em: 14 abr. 2022.

ROSENVALD, Nelson; FARIAS, Cristiano Chaves D.; NETTO, Felipe Peixoto B. **Novo Tratado de Responsabilidade Civil**. São Paulo: Editora Saraiva, 2019.

SANTOS, Camila Ferrão dos; SILVA, Jennifer Gomes da; PADRÃO, Vinicius. Responsabilidade Civil pelo Tratamento de Dados Pessoais na Lei Geral de Proteção de Dados. **Revista Eletrônica da PGE – RJ**, v. 4, n. 3 , 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/issue/view/12. Acesso em 24 abr. 2022.

SANTOS, Marcelo Vinícius Miranda dos. Critérios de Imputação da Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais. **Revista Conversas Civilísticas**, v. 1, n. 2, 31 dez. 2021. Disponível em: . https://periodicos.ufba.br/index.php/conversascivilisticas/article/view/47539. Acesso em 28 de fevereiro de 2022.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A Proteção De Dados Sensíveis No Sistema Normativo Brasileiro Sob O Enfoque Da Lei Geral De Proteção De Dados (Lgpd) – L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, *[S. l.]*, v. 26, n. 2, p. 81–106, 2021. DOI: 10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 28 ago. 2022.

SARLET, Ingo Wolfgang**.** A EC 115/22 e a proteção de dados pessoais como Direito Fundamental**. Consultor Jurídico**, 2020. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em 7 set. 2022.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Apelação Cível 1000641-85.2021.8.26.0405.** "[...] Pretensão escorada em situações hipotéticas, prejuízo potencial advindo do receio de uso futuro dos dados do consumidor em eventuais fraudes no comércio – Situação inapta a autorizar reparação [...]" Relator (a): Sá Duarte; Órgão Julgador: 33ª Câmara de Direito Privado; Foro de Osasco - 8ª Vara Cível; Data do Julgamento: 29/11/2021; Data de Registro: 30/11/2021.

SÃO PAULO**. Apelação Cível nº 1000144-71.2021.8.26.0405**. “[...]Reconhecida a falha no sistema, ante a invasão por terceiros, ocasionando o vazamento de dados pessoais do consumidor, patente o dever de indenizar pelos danos morais sofridos [...].Relator (a): Maria Lúcia Pizzotti; Órgão Julgador: 30ª Câmara de Direito Privado; Foro de Osasco - 1ª Vara Cível; Data do Julgamento: 25/08/2021; Data de Registro: 13/09/2021.

SÃO PAULO. Tribunal de Justiça de São Paulo**. Apelação Cível 1001032-45.2021.8.26.0177.** “[...] Inteligência do artigo 46 da Lei Geral de Proteção de Dados (Lei n. º 13.709/2018). Danos morais não verificados. Vazamento de dados que não ensejou dano efetivo ao requerente. Dados vazados que não estão abrangidos no conceito de dado pessoal sensível (art. 5º, II, da LGPD).[...]” Relator (a): Virgilio de Oliveira Junior; Órgão Julgador: 23ª Câmara de Direito Privado; Foro de Embu-Guaçu - Vara Única; Data do Julgamento: 01/12/2021; Data de Registro: 03/12/2021.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Apelação Cível 1014245-32.2019.8.26.0196.** “[...] Pressupostos da responsabilização civil que consistem em ato ou conduta humana, nexo de causalidade e dano. Ausência de prova segura quanto ao dano e ao nexo de causalidade. Dano moral que no caso dos autos não se constitui "in re ipsa" [...]”Relator (a): Daise Fajardo Nogueira Jacot; Órgão Julgador: 27ª Câmara de Direito Privado; Foro de Franca - 4ª Vara Cível; Data do Julgamento: 26/11/2021; Data de Registro: 26/11/2021.

SILVEIRA, S. A.; AVELINO, R.; SOUZA, J. A privacidade e o mercado de dados pessoais | Privacy and the market of personal data. **Liinc em Revista**, *[S. l.]*, v. 12, n. 2, 2016. DOI: 10.18617/liinc.v12i2.902. Disponível em: http://revista.ibict.br/liinc/article/view/3719. Acesso em: 20 abr. 2022.

TASSO, Fernando Antonio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 97-115, Janeiro-Março/2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_a_lgpd.pdf?d=637250344175953621. Acesso em 26 abr. 2022.

TEIXEIRA, Tarcisio. **A LGPD e o e-commerce**. São Paulo: Editora Saraiva, 2021.

TEIXEIRA, Tarcísio. **Comércio Eletrônico - conforme o marco civil da internet e a regulamentação do e-commerce no Brasil, 1 ª edição.** São Paulo: Editora Saraiva, 2015.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES , Gisela, Sampaio da Cruz. **Fundamentos do Direito Civil - Responsabilidade Civil - Vol. 4**. Rio de Janeiro: Grupo GEN, 2020.

THEODORO JÚNIOR, Humberto Theodoro. **Dano Moral.** 8 ed. Rio de Janeiro: Grupo GEN, 2016

UNIÃO EUROPEIA. **Directiva 95/46/CE, de 24 de Outubro de 1995, relativa à protecão das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Parlamento e Conselho Europeu, 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em 12 set. 2022.

UNIÃO EUPEIA. **General Data Protection Regulation (GDPR).** Disponível em: https://gdpr-info.eu/chapter-1/. Acesso em 04 set. 2022.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. **Ficha Temática**: proteção dos dados pessoais. Tribunal de Justiça da União Europeia, 2021. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_pt.pdf. Acesso em: 20 ago. 2022.