UNIVERSIDADE DE TAUBATÉ

Jessica Aparecida Ferreira Galhardo

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: DESAFIOS E PERSPECTIVAS DE SUA IMPLEMENTAÇÃO NO BRASIL

Taubaté -SP
2022

Jessica Aparecida Ferreira Galhardo

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: DESAFIOS E PERSPECTIVAS DE SUA IMPLEMENTAÇÃO NO BRASIL

Trabalho de Conclusão de Curso apresentado como exigência parcial para o desenvolvimento do Trabalho de Graduação necessário para a obtenção do diploma de Bacharel em Direito no Departamento de Ciências Jurídicas da Universidade de Taubaté.

Orientador: Prof. Dr. Júnior Alexandre Moreira Pinto

Taubaté -SP
2022

Grupo Especial de Tratamento da Informação - GETI
Sistema Integrado de Bibliotecas - SIBi
Universidade de Taubaté - UNITAU

G155l Galhardo, Jessica Aparecida Ferreira

Lei geral de proteção de dados pessoais : desafios e perspectivas de sua implementação no Brasil / Jessica Aparecida Ferreira Galhardo. -- 2022.

60f.

Monografia (graduação) - Universidade de Taubaté, Departamento de Ciências Jurídicas, 2022.

Orientação: Prof. Dr. Junior Alexandre Moreira Pinto, Departamento de Ciências Jurídicas.

1. Dados pessoais. 2. Responsabilidade civil. 3. Proteção de dados - Legislação. 4. Risco - Direito. I. Universidade de Taubaté. Departamento de Ciências Jurídicas. Curso de Direito. II. Título.

CDU - 342.7:004(81)

Ficha catalográfica elaborada pela Bibliotecária Regina Márcia Cuba – CRB 8ª/7416

Jessica Aparecida Ferreira Galhardo

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: DESAFIOS E PERSPECTIVAS DE SUA IMPLEMENTAÇÃO NO BRASIL

Trabalho de Conclusão de Curso apresentado como exigência parcial para o desenvolvimento do Trabalho de Graduação necessário para a obtenção do diploma de Bacharel em Direito no Departamento de Ciências Jurídicas da Universidade de Taubaté.

Orientador: Prof. Dr. Júnior Alexandre Moreira Pinto

Trabalho de Graduação defendido e aprovado em _____/_____/_____ pela comissão julgadora:

_____
Professor Dr. Júnior Alexandre Moreira Pinto

_____
Professor (a), Universidade de Taubaté

Taubaté -SP
2022

AGRADECIMENTOS

Agradeço a Deus; sem ele não teria capacidade de alcançar esta tão sonhada graduação, ao meu marido Paulo, desde que você passou a fazer parte da minha vida que vivencio uma espiral construtiva, esta é uma das muitas conquistas ao seu lado e minha filha Alice, que ao logo destes anos acompanhou minha luta, idas e vindas para a faculdade, não há exemplo maior de dedicação do que o da nossa família.

Aos meus colegas de turma, por compartilharem comigo momentos de descobertas e aprendizado e por todo o companheirismo.

Agradeço também a todos os professores que me acompanharam durante a graduação, em especial ao Prof. Júnior Alexandre Moreira Pinto responsável pela realização deste trabalho.

“Aparte-se do mal, e faça o bem; busque a paz, e siga-a.
Porque os olhos do Senhor estão sobre os justos,
E os seus ouvidos atentos às suas orações;
Mas o rosto do Senhor é contra os que fazem o mal.”
1 Pedro 3:11,12

RESUMO

O presente estudo tem como objetivo analisar a implementação da Lei nº 13.709/2018 (LGPD) no Brasil e sua efetividade para a tutela do direito fundamental à proteção de dados pessoais na internet e identificar o papel e os desafios observados pela LGPD, além de investigar o risco de vazamento de dados pessoais sensíveis e sua responsabilização no ordenamento jurídico nacional. O advento tecnológico viabilizou um fluxo de dados pessoais desmedido, onde a utilização inadequada de tais dados se compreende em uma grave ameaça aos direitos da personalidade, com ênfase ao direito à privacidade, haja vista a possibilidade de violação, disseminação e comercialização dos dados, sendo estes tratados como uma nova mercadoria. Nesse sentido, a pesquisa explana a relevância da proteção de dados pessoais no ordenamento jurídico brasileiro, sendo estes elevados ao status de direito fundamental, com base no entendimento do Supremo Tribunal Federal exaurado em 2020. Para tanto, será abordada a criação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), os dados pessoais sensíveis, previsto no art. 5º, II, da LGPD, os tratamentos que devem ser observados com esses dados, os atos discriminatórios que podem ocorrer com o vazamento desses dados e a importância da responsabilização pelo vazamento ocorrido, a fim de afastar a discriminação. A técnica de pesquisa utilizada no presente trabalho é a bibliográfica, sendo o método dedutivo empregado, a fim de adequar ideias ou descobrir intuições sobre a temática abordada.

Palavras-chave: Dados pessoais. Responsabilidade civil. Lei Geral de Proteção de Dados. Vazamento. Riscos.

ABSTRACT

The present study aims to analyze the implementation of Law No. the risk of leakage of sensitive personal data and its liability in the national legal system. The technological advent has made possible an excessive flow of personal data, where the inappropriate use of such data is understood as a serious threat to the rights of the personality, with emphasis on the right to privacy, given the possibility of violation, dissemination and commercialization of data, being these treated as a new commodity. In this sense, the research explains the relevance of the protection of personal data in the Brazilian legal system, which are elevated to the status of a fundamental right, based on the understanding of the Federal Supreme Court exhausted in 2020. To this end, the creation of Law No. 13,709 will be addressed. /2018 (General Personal Data Protection Law - LGPD), sensitive personal data, provided for in art. 5, II, of the LGPD, the treatments that must be observed with this data, the discriminatory acts that can occur with the leak of this data and the importance of accountability for the leak that occurred, in order to remove discrimination. The research technique used in the present work is the bibliographical one, being the deductive method used, in order to adapt ideas or discover intuitions about the theme addressed.

Keywords: Personal data. Civil responsability. General Data Protection Act. Leak. Scratchs

SUMÁRIO

INTRODUÇÃO

O presente estudo almeja analisar as dificuldades e as perspectivas no tocante à Lei nº 13.709/2018 (LGPD) pois, com a elevada expansão das novas tecnologias da informação na sociedade contemporânea, verifica-se o aumento do uso da internet pelos usuários, que frequentemente estão gerando dados no plano online. Nos dias atuais, os supracitados dados são capazes de movimentar a Economia, pautados na tecnologia e na informação. Tal conjuntura se encontra diretamente conectada ao Poder Econômico no intento de garantir direitos como a proteção de dados, a proteção do direito à intimidade e à privacidade, demonstrando-se a necessidade de fiscalização a fim de regular o espaço cibernético.

Assim, a presente pesquisa se concentra nos seguintes problemas: Com a implementação da LGPD no Brasil, é possível aferir que nosso ordenamento jurídico apresenta medidas efetivas para a tutela do direito fundamental à proteção de dados pessoais na internet? Qual o papel e os desafios observados pela LGPD?

Sob tais situações, a LGPD foi editada com o objetivo de regulamentar o tratamento dado aos dados pessoais da pessoa. Seja pessoa jurídica, física ou até o ente estatal, todos devem respeitar o que é tipificado no texto normativo. Porém, com a inovação legislativa, é visível alguns institutos que podem prejudicar o titular dos dados, haja vista seu tratamento ser realizado com o escopo de segurança jurídica ou defesa nacional. Acepção essa que contém vasta amplitude hermenêutica, permitindo uma margem arbitrária prejudicial para a segurança dos dados e, consequentemente, ao direito à privacidade das pessoas.

Pelo arranjo das competências aferidas a ANPD pela LGPD, resta nítido a sua relevância dentro da atual conjuntura legislativa, uma vez que a ANPD é a figura central para a aplicação LGPD, em uma realidade onde os agentes de tratamento de dados pessoais, tanto no âmbito público quanto no privado, estarão à mercê de sua função regulatória, sobretudo na seara sancionatória, com a possibilidade de sanções.

As variáveis que poderão influir no processo de pesquisa e elaboração do trabalho são as legislações constitucional, no que tange aos direitos fundamentais do indivíduo, bem como a legislação infraconstitucional (Lei nº 13.709/2018), com ênfase na área do Direito Digital, assim como as possíveis regulamentações ou alterações de entendimento no âmbito dos Tribunais brasileiros.

No que se refere à relevância pessoal, tem-se conhecimento que dados são informações relacionadas à pessoa em si, possuindo características próprias, devendo, o usuário, protegê-las contra possíveis ameaças com a má administração dessas informações. Têm-se o conhecimento, também, de que alguns dados se encontram em uma esfera ainda mais delicada, os dados pessoais sensíveis, sendo esses, ao terem seu sigilo quebrado, podem acarretar na difamação e preconceito quanto à sociedade.

O tema escolhido mostra-se relevante socialmente, tendo em vista que a população brasileira ainda carece de muita instrução e estudo quando o assunto é proteção de dados pessoais. Vivemos em uma sociedade em que a tecnologia cresce desenfreadamente e, com isso, a exposição de dados pessoais fica cada vez maior através de mecanismos sociais. O uso dessas informações de maneira errônea, ou até mesmo a publicação excessiva de informações pessoais acarretam em consequências gravosas.

Na seara jurídica, a proteção de dados vem ganhado cada vez mais força. As informações que antes eram semeadas em leis infraconstitucionais autônomas, hoje se reuniram em um só texto, Lei Geral de Proteção de Dados, com o objetivo de promover maior celeridade e segurança jurídica. Assim, faz-se necessária a observância sobre a legislação vigente, para uma análise mais técnica das respostas da problemática abordada neste projeto.

Acerca da metodologia utilizada, a pesquisa será bibliográfica, a mesma que se desenvolve tentando explicar um problema por meio de teorias publicadas em doutrinas ou artigos do gênero. A finalidade desse tipo de pesquisa consiste em reconhecer e a analisar as principais contribuições teóricas existentes sobre um determinado tema, tornando-se uma ferramenta fundamental para qualquer pesquisa.

No que se refere ao método de abordagem, a pesquisa se pautará no método indutivo, que corresponde aquele responsável pela generalização, ou seja, parte-se de algo particular para uma questão mais abrangente, geral. A finalidade do método indutivo se pauta em alcançar as conclusões mais amplas do que o conteúdo determinado pelas premissas nas quais encontra-se fundamentado. Portanto, nota-se que o método indutivo é fundamental para a verificação do dado particular, bem como de sua utilização de modo geral, através de uma experimentação ampla para que a generalização alcançada seja considerada verdadeira.

1 A EVOLUÇÃO HISTÓRICA SOBRE O DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS

1.1 DIREITO À PRIVACIDADE

A fim de adentrar a privacidade de proteção de dados se faz necessário realizar uma breve recapitulação da história, pois, o Direito à privacidade surgiu a partir da necessidade de garantir os direitos fundamentais das pessoas através dos dados coletados, tornando-os um direito fundamental, sujeito a proteção jurídica do Estado. Assim, o estudo delineará uma breve história da evolução tecnológica e das conquistas obtidas durante a evolução da informatização.

Desse modo, verifica-se no curso da história que o homem sempre procurou superar as intempéries e limitações impostas pela natureza, buscando sempre meios de sofisticar a matéria que tinha à sua disposição para torná-la útil para si e lhe trazer mais conforto e comodidade (BORGES, 2014).

A tecnologia é uma conquista do homem em face das dificuldades que a natureza sempre lhe proporcionou. Por essa razão, percebe-se que em cada momento histórico, com suas descobertas, o aperfeiçoamento de técnicas ou a invenção de outras para vencer estes obstáculos sempre gozaram de ampla aceitação, mormente pelos benefícios à humanidade (COTS, 2014).

Em face de tudo isso, destaca-se, no entanto, que o mau uso dos progressos da humanidade já resultou mais de uma vez em problemas diversos, decorrendo disso a necessidade de disciplina de seu uso, muitas das vezes através das normas, o que vem ocorrendo no caso do ambiente virtual, objeto que suscita cada vez mais profundas disposições normativas sobre o seu uso.

A Constituição Federar de 1988 traz no seu art. 5.º, inciso X, XI, XII, o direito à privacidade demonstrado logo abaixo:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou

> desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (BRASIL, 1988)

Nesse contexto, observa-se que a privacidade constitui uma maneira do indivíduo preservar sua honra e imagem. Compreende-se também, em um direito da personalidade, cuja a inviolabilidade está garantida no texto constitucional, em seu artigo 5°, inciso X. Assim sendo, Mota (2000, p. 149) afirma que esse fenômeno denomina-se na “vocação de abertura do tradicional direito geral de personalidade” e que, “sincrônica e diacronicamente ele permite a tutela de novos bens face à renovadas ameaças à pessoa humana”.

Nesse sentido, o primeiro texto legal a versar sobre a tutela do direito à privacidade foi a Declaração dos Direitos e Deveres do Homem na cidade de Bogotá, no ano de 1948, compreende-se no primeiro acordo internacional sobre direitos humanos. Após a menção na Declaração, somente dezoito anos depois, o Pacto Internacional dos Direitos Civis e Políticos preceituou matéria de cunho correspondente acerca da privacidade e seus desdobramentos.

Para chegar ao nível de inviolabilidade à intimidade, à vida privada, à honra e à imagem das pessoas, é assegurando o direito aos danos materiais e morais decorrentes da violação, sendo perceptível que as consolidações das garantias da privacidade são tuteladas e, para chegar a esse ponto transcorreu-se uma evolução histórica de violações da dignidade da pessoa humana, cujo resgate se deu ao longo do tempo e, atualmente, tem-se os institutos que protege a privacidade do indivíduo contra condutas que afrontam o cidadão, sejam estas praticadas pelo particular ou pelo próprio Estado.

Portanto, o direito à privacidade é uma matéria de importância mundial, uma vez que a violação da intimidade acarreta ao indivíduo sensação de insegurança e instabilidade. A preservação da intimidade e privacidade proporciona ao ser humana uma ávida sensação de liberdade, onde o mesmo pode colocar seu desempenho e convicções em prática e manter vínculos sociais sem estar sendo vigiado. Sendo assim, a seção posterior trará uma breve evolução histórica da proteção de dados pessoais.

1.2 BREVE HISTÓRICO DA PROTEÇÃO DE DADOS PESSOAIS NO MUNDO

Com a propagação do princípio da dignidade humana pelas Constituições em todo o mundo, principalmente com o término da Guerra Mundial de 1939 e com a Declaração Universal de Direitos Humanos do ano de 1948, os interesses essenciais da existência humana passaram a ser prioridade nas discussões dos juristas (COTS; OLIVEIRA, 2019).

Para Bauman (2011, p. 8), crítico da pós-modernidade, o mundo líquido moderno que muda constantemente o ser humano permitiu que hoje pudesse dispor de algo até então inimaginável, a Internet, a web mundial, “as autoestradas de informação que nos conectam de imediato, em tempo real, a todo e qualquer canto do planeta”, podendo tudo isso ser transportado nos bolsos através dos pequenos smartphones.

Diante do viés de crescentes evoluções dos meios digitais no século XX, as relações sociais se apresentam como uma nova vertente, para eliminar obstáculos, conectar-se rapidamente para trocas de informações online, as interseções sociais passam a estar cada dia mais presentes e sua exposição mais aparente. Diante desse panorama, será apresentada a noção geral sobre dados pessoais relacionando-a com o direito à privacidade e suas tutelas.

O termo proteção de dados pode ser entendido tanto como o desempenho da liberdade do indivíduo, quanto como algo que se encontra interno a este sujeito, de modo que faz parte da sua natureza enquanto ser humano. De acordo com Cancelier (2016, p. 85) “ter privacidade é fundamental ao indivíduo, não apenas em oposição ao público, mas numa relação interna, visto que não será possível a assunção de seus desejos sem a construção de seu espaço íntimo.”

Assim, se tem como características principais a liberdade e a transparência como viés primordial, a primeira lei de proteção geral de dados foi criada na Alemanha em 1970, onde se notou a necessidade de maior proteção dos dados pessoais, visto que constituem uma proteção da personalidade do indivíduo, fazendo jus da proteção por parte do Estado jurisdicional. Em 1980 que a Organization for Economic Cooperation and Development (OECD), através do Comitê, publicou uma diretriz que estabeleceria princípios básicos em relação à proteção de dados e sobre o fluxo de informações entre os países que já possuíam sua lei (COTS; OLIVEIRA, 2019).

Em 1981 foi aprovado o Data Protection Convention, o primeiro instrumento legal internacional, que buscava proteger o indivíduo contra a coleta e o processamento de dados pessoais de forma abusiva ou inadequada, proibindo-se o processamento de dados confidenciais sobre raça, política, saúde, religião, vida sexual, antecedentes criminais, dentre outras informações. Também se consagrava o direito do indivíduo de saber quais informações são armazenadas sobre ele e, se fosse o caso, corrigi-las (COTS; OLIVEIRA, 2019).

O Brasil obteve os seus primeiros instrumentos legais tendo alcance na proteção de dados pessoais no ano de 1990, sendo possível citar o início no Código de Defesa do Consumidor (Lei 8.078/1990), que previa o direito de o consumidor acessar suas informações existentes em cadastros, registros e consumo registrado sobre ele. Posteriormente, em 1996 foi criada a Lei de Interceptação Telefônica e Telemática (Lei 9.296/1996).

Em seguida, a Lei do Habeas Data (Lei 9.507/1997), regulou o rito de acesso e a correção de informações pessoais e se tornou um direito constitucional. No ano de 2002, o Código Civil Brasileiro trouxe um capítulo sobre os Direitos da Personalidade, para coibir a violação da vida privada das pessoas, revendo a privacidade como um direito subjetivo de cada um e não focando no âmbito de propriedade.

Em 2011 foi aprovada a Lei de Acesso à Informação (Lei nº 12.527/2011) que, dentre outras questões, definia a informação pessoal como aquela relacionada à pessoa natural identificada ou identificável, determinando aos órgãos e entidades do Poder Público a proteção da informação sigilosa e pessoal, observando-se a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. Ademais, eram ressaltados alguns princípios, liberdades e garantias individuais, que seriam consagradas, também, na futura Lei Geral de Proteção de Dados (LGPD), como o princípio da transparência, vida privada, honra, respeito à intimidade e imagem das pessoas.

Outra lei que vale destaque é a Lei 12.737/12 - Lei Carolina Dieckmann, que criminalizou a invasão de dispositivos de informática, evidenciando em um dos seus dispositivos:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três)

> meses a 1 (um) ano, e multa. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave (BRASIL, 2012).

Diante dos fatos ocorridos no ano 2013, o mundo se viu diante de um impacto nas legislações relativas à proteção e ao tratamento dos dados pessoais. Veio à tona a existência de um software denominado PRISM e outros que eram utilizados para monitorar e coletar de forma massiva as trocas de informações no mundo, vigiando não apenas os terroristas, mas também espionando países e grandes empresas estrangeiras.

O Brasil se viu obrigado a colocar em tramitação a PL 2126/11, que dizia respeito do Marco Civil da Internet, mesmo não trazendo em seu corpo qualquer tipo de proteção prática quanto às espionagens internacionais, contudo, continha conceitos e princípios a respeito privacidade e da proteção dos dados pessoais, o Marco Civil foi votado e aprovado, entrando em vigor no ano de 2014, passando pela primeira vez constar a palavra privacidade, dando ênfase à necessidade da proteção dos dados pessoais, marcando-a como princípio fundamental. O Marco Civil da Internet (Lei nº 12.965/2014) trouxe consigo, como, por exemplo, o artigo 3º, que abordou o princípio da proteção da privacidade e dos dados pessoais:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...]
> II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei.," bem como o artigo 7º no inciso VII, VIII e X: VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; (BRASIL, 2014)

Assim, não se pode esquecer que todos esses princípios e regramentos seriam posteriormente implementados na Lei Geral de Proteção de Dados, ficando transparente a importância dos mesmos para elaboração da LGPD no país.

De forma geral, segundo Bioni (2019, p. 67), “é possível dividir a história da criação das leis de proteção de dados pessoais em quatro gerações.” A primeira geração seria o momento em que aparece a preocupação com o processamento massivo dos dados pessoais na esfera do governo, na conjuntura da formação do Estado Moderno, possuindo o seu foco na esfera governamental.

Nesse momento, foram estabelecidas normas rígidas, que regulavam o uso das tecnologias, no tocante ao processamento e à coleta de dados pessoais das pessoas componentes do governo. A segunda geração tinha como centro uma mudança regulatória, não se preocupava apenas com os dados pessoais das pessoas governamentais, mas, também, dos indivíduos da esfera privada, transferindo-se, assim, para os próprios titulares dos dados, a responsabilidade de mantê-los protegidos. Em outras palavras, decidiam-se quais informações poderiam ser coletadas, usadas e compartilhadas, tudo com o seu devido consentimento, dando uma maior autonomia para o indivíduo, em gerir as suas informações pessoais (BIONI, 2019).

A terceira geração se trata de regulamentos, que dão ao indivíduo a prerrogativa na participação de todo o processo, desde a coleta até o compartilhamento das informações, ou seja, deu-se uma autonomia maior para a pessoa titular daquelas informações. Na quarta geração entra novamente o Estado, regulamentando certos tipos de dados pessoais que seriam considerados sensíveis, tirando da autonomia do indivíduo a prerrogativa de auto escolha, passando para o Estado a prerrogativa de gerir tais informações, com base nos regulamentos das leis de proteção de dados (BIONI, 2019).

1.3 CONTEXTO HISTÓRICO DA PROTEÇÃO DE DADOS PESSOAIS NA EUROPA

A proteção de dados pessoais se compreende em um dos direitos fundamentais da pessoa, disposto na Declaração Universal de Direitos Humanos Europeia, com vigência desde o ano de 1948. A temática sobre a regulamentação da proteção de dados pessoais está em destaque há mais de duas décadas em solo europeu, tendo como movimento precursor a Convenção 108 de 1981, editada recentemente pelo Conselho da Europa. Após a supracitada Convenção, verificou-se a elaboração da Diretiva 95/46/CE, também abordando o assunto, atualmente

revogada pelo Regulamento Europeu de Proteção de Dados (2016/679), todavia, com as principais acepções conservadas (GDPR, 2016).

Nessa conjuntura, na seara europeia, passaram a originar autoridades nacionais, como é o caso da autoridade francesa CNIL na década de 1980, que atualmente encontra disposição no GDPR, detendo poderes informacionais independentes, de certificação e de sanção no tocante à proteção de dados pessoais. As mencionadas autoridades colaboram na adaptação de organizações nos ditames da proteção almejada, tendo em vista que ofertam diretivas às organizações, controladores, operadores, assim como pode solucionar determinados conflitos inerentes ao tema (GDPR, 2016).

Desse modo, as lições de Polido et. al. (2018, p. 34) aferem que:

> Tal Regulamento trouxe inovações que começaram a valer a partir de 25 de maio de 2018. Seu direcionamento procurou unificar a proteção de dados na União Europeia com uma regra que fosse válida para todos os Estados-Membro, sem a necessidade de internacionalização das regras para que fosse válida em cada localidade. Tal situação representa uma evolução no contexto regulatório da privacidade e proteção de dados, pois até então, na Diretiva 95/46/CE, cada Estado-Membro da União Europeia necessitava internalizar na sua legislação doméstica, e isto acabava por suscitar diferentes garantias à proteção de dados nos países europeus.

Assim, o GDPR trouxe consigo um amplo rol de alterações, traduzidas em disposições que procuraram tratar dos assuntos trazidos pelos novos modelos elevados na Revolução Tecnológica, bem como o desenvolvimento de novos meios tecnológicos e como eles se relacionam com as pessoas. O regulamento pode ser tido, dessa forma, como uma adequação legislativa na seara da UE, que já detinha uma vasta cultura e jurisprudência em torno da privacidade e da proteção de dados pessoais (POLIDO et. al., 2018, p. 35).

Outrossim, além de determinar os pilares para uma estrutura funcional de proteção a dados pessoais, o GDPR consiste em um documento que ultrapassa o básico, almejando levantar minuciosamente as paredes de um refinado edifício de tutela de direitos. E, mesmo com complexidades, a redação deixa lugar para uma possível complementação pelos Estados-membros. Isso foi admitido pois, a legislação anterior, a Diretiva Europeia 95/46, já havia ampliado o caminho para o pleno tratamento da questão, aferindo os marcos efetivos à abordagem da matéria.

Todavia, foi ficando cada vez mais evidente que as acepções para a proteção de dados pessoais determinadas na Diretiva 95/46 necessitariam de

complementações, sendo igualmente indiscutível que o processo tecnológico e a quantidade exorbitante de dados em circulação reclamavam alto grau de atenção legal.

Como verificado no GDPR, era necessário gerar confiança para a operacionalização da economia digital (considerando n. 07 e 09):

> Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrônica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades econômicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE (GDPR, 2016).

Por sua vez, a frequência cada vez mais elevada de incidentes envolvendo o vazamento de dados culminaram o aprofundamento da matéria no que tange a instrumentos de responsabilização mais enérgicos. Colocados tais motivos como fundamentação, o GDPR almejou ser preciso na elaboração de mecanismos preventivos e repressivos. Assim, o referido se mostrou altamente exigente no que diz respeito à transparência das informações dispostas aos consumidores (SOPRANA; CORONATO, 2017).

O produto de todas essas pesquisas e discussões é concretizado por meio de um texto extenso e coeso, disposto em duas principais divisões: Considerandos e Texto Normativo propriamente dito. Distintamente das tradicionais exposições de motivos verificadas no Brasil, os considerandos da GDPR possuem os notáveis intentos – por meio da descrição de 173 tópicos, servir-se de parcela didática introdutória ao documento, estruturando as normas, expondo os valores que as englobam e, consequentemente, simplificando a sua compreensão e aplicação.

Nos considerandos iniciais, por exemplo, verificam-se os parâmetros detalhados da regra do consentimento prévio para coleta e manuseio de dados pessoais, que transpassa todo o texto do Regulamento. Conforme dispõe o considerando nº 42, o consentimento prévio deve ser muito bem definido, pois:

> Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Em conformidade com a Diretiva 93/13/CEE do Conselho (10), uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. (...) Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado. (GDPR, 2016)

Outra constatação de explicações importantes nessa primeira parte do material pode ser verificada nos comentários relativos à anonimização de dados, denominada no GDPR como pseudonimização (considerando nº 28). Em consonância às explanações expostas, a medida não é particular e deve ganhar evidencia na conjuntura protetiva narrada nos considerandos de nº 51 e 75 (GDPR, 2016).

Portanto, observa-se que a parte introdutória do mencionado Regulamento – consolidada por meio de seus considerandos e com mais tópicos do que o texto regulamentar, exprime um valioso material para elucidação teológica do documento, sendo hábil a servir de instrumento para nortear o seu cumprimento.

1.4 CONCEITO DE DADOS PESSOAIS

A fim de estimular o entendimento sobre a responsabilidade civil na LGPD, mostra-se indispensável, inicialmente, explanar a conceituação de “dados pessoais”. Em conformidade aos estudos de Mendes (2014, p. 54) “o sistema jurídico de proteção de dados depende, espontaneamente, do que se considera um dado pessoal e quais as espécies de processamento de dados estão englobadas pela regulação”. Assim, a observância a tais conceitos é essencial para estabelecer o alcance e as balizas da proteção jurídica.

Nesse panorama, para que se alcance a supracitada qualificação, deve-se ponderar a definição no plano jurídico de informação e dado. De acordo com as lições de Lacombe (2003, p. 490), os dados são conceituados como um emaranhado de registros sobre fatos, factíveis de serem examinados, ordenados e pesquisados para se atingir conclusões, “à medida que estes são ordenados adequada e

significativamente para propósito de compreensão e análise, são denominados de informações.”

Sendo assim, verifica-se que o dado consiste na fase primitiva da informação, tendo em vista que não é algo que por si só adiciona conhecimento. Outrossim, adicionando-se a expressão “pessoais” aos dados, eleva-se uma personalização de sua definição, de modo que os dados pessoais são caracterizados como o emaranhado de registros relativos à uma pessoa. Nessa toada, as lições de Castro (2005, p. 75) apontam que os dados pessoais são “toda e qualquer informação gráfica, acústica, fotográfica, alfabética, independente do suporte, relativa ao indivíduo identificável ou identificado.”

Sobre o conceito de dados pessoais no cerne da legislação nacional, somente elevou-se uma conceituação legal do termo no ano de 2016, por intermédio do Decreto nº 8.771, que dispõe regulações sobre o Marco Civil da Internet, comportando, em seu art. 14 que “dado pessoal é aquele relativo à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa” (BRASIL, 2016).

Desse modo, é possível observar a relevância dos supracitados conceitos, tendo em vista que os dados pessoais se encontram estritamente ligados à personalidade e à dignidade humana do indivíduo, se tornando elemento de garantia por intermédio de outros direitos fundamentais, pois são informações de inquestionável valor, que não podem ser sujeitas a condutas arbitrárias por parte dos agentes controladores (SILVA, 2019, p. 70).

No que diz respeito à latente necessidade de se respaldar os dados sociais, tal matéria desponta na sociedade contemporânea por meio de um anseio de proteger a personalidade da pessoa contra os perigosos riscos a serem ocasionados pela ausência do tratamento adequado de dados pessoais. Evidencia-se que sua finalidade não é a proteção dos dados propriamente ditos, mas sim da pessoa que figura o papel de titular.

Assim, levando-se em consideração que as informações pessoais consistem em uma relação entre o indivíduo e o meio social, a personalidade de uma pessoa pode ser substancialmente ferida com a incorreta disseminação e utilização de informações armazenadas sobre esta. Desse modo, os dados pessoais podem ser entendidos como parcela da personalidade de uma pessoa, carecendo, assim, proteção jurídica com o propósito de garantir a isonomia e a liberdade.

Em consonância às lições de Mendes (2014, p. 166), na conjuntura contemporânea de desenvolvimento tecnológico, o direito à privacidade ganha evidência para aferir surgimento à matéria sobre a proteção de dados pessoais no ordenamento jurídico brasileiro, de maneira a se readequar aos óbices encontrados por tal avanço.

Nesse enfoque, pode-se aferir que a tutela de dados alcança uma seara muito mais ampla. Inicialmente, passa a ser entendida como um vasto fenômeno que atinge toda a coletividade, ao passo em que os danos aferidos pelo processamento inadequado de dados pessoais são, naturalmente, difusos, demandando igualmente uma proteção jurídica coletiva. Em segundo, a privacidade, outrora entendida como direito negativo de ser esquecido passa a readaptar ainda o controle dos dados pessoais pelo próprio titular, que possui o poder de decidir o momento, como e onde seus dados devem transitar.

Posto isso, verifica-se que a tutela de dados pessoais, mediante a essencial proteção demandada pelo advento tecnológico, utilizou-se da privacidade para edificar um novo direito fundamental, imprescindível a uma sociedade democrática contemporânea, com premissas na personalidade e na dignidade da pessoa humana. Viabilizando às pessoas, dessa forma, a determinação acerca de seus dados pessoais, reestabelecendo a sua remota ligação com a sociedade.

2 ASPECTOS GERAIS SOBRE A LEI DE PROTEÇÃO DE DADOS PESSOAIS

2.1 A NECESSIDADE DE UMA REGULAMENTAÇÃO ESPECÍFICA NO BRASIL

O presente tópico almeja verificar quais são os fundamentos para o direito fundamental à proteção de dados na CF/88 e a necessidade de uma regulamentação específica nesse sentido, o que demonstra uma evolução dessa definição e quais são os efeitos do reconhecimento desse direito fundamental (BRASIL, 1988).

Através do surgimento da sociedade da informação, se elevam relevantes desafios para o sistema jurídico e seus operadores, sobretudo para a proteção da personalidade e da vida privada do ser humano. Para assentar a solução compatível aos desafios sociais permeados contemporaneamente, é necessário que a teoria do direito se reorganize e se reinterprete a ponto de discernir e resolver os novos problemas encontrados pela sociedade na Era da Informação.

Esse desafio se demonstra ainda mais visível no plano constitucional, pois, a vitalidade e a continuidade da CF/88 dependem de sua capacidade de se readequar às transformações históricas e sociais ocorridas, viabilizando um amparo dos indivíduos contra novas maneiras de poder que se elevam socialmente.

Nessa conjuntura habita uma tensão oriunda ao conceito de Constituição: por um lado, ela deve exprimir continuidade, estabilidade, permanência e segurança e, por outro, ela deve expressar maleabilidade, abertura de interpretação e atualização para a contínua consolidação dos direitos e princípios nela dispostos. A contradição reside no fato de que a continuidade da Constituição apenas é possível “se nela o passado e o futuro se vincularem” (OLIVEIRA, 2018, p. 16).

Com base na análise normativa e jurisprudencial pátria, demonstra-se uma vasta experiência constitucional em trâmite, que reconheceu a evolução do termo privacidade, de maneira a incluir a proteção de dados pessoais do indivíduo em nosso sistema jurídico. A partir de tais vivências e da experiência institucional relativa à proteção de dados no país, sendo possível compreender que atualmente e reconhece um direito fundamental à proteção de dados pessoais, como uma extensão da inviolabilidade da intimidade e da vida privada, dispostos constitucionalmente.

Nesse sentido, as lições de Martins (2014, p. 62) apontam que:

> As tecnologias da informação contribuíram para que a informação pessoal se tornasse algo capaz de extrapolar o próprio indivíduo. A facilidade de sua coleta, armazenamento e a sua utilidade para diversos fins tornou-a um bem em si, ligado ao indivíduo, mas capaz de ser objetivado e tratado longe e mesmo a despeito dele – não é por outro motivo que a informação pessoal é o elemento fundamental em uma série de novos modelos de negócios típicos da Sociedade da Informação. Por esse motivo a proteção de dados pessoais é tida em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e é considerada como um direito fundamental.

Desta feita, ao assentar a inviolabilidade da intimidade e da vida privada, em seu dispositivo 5º, X, a CF/88 não limita a aplicação desse conceito a nenhum caso específico. Ou seja, se extrai desse artigo uma vasta proteção da personalidade e da vida privada do indivíduo, nas várias situações em que este se encontra. Nessa toada, não faria sentido eliminar especialmente as situações em que a sua vida privada está passível de violação, como, por exemplo, na situação do processamento de dados pessoais (BRASIL, 1988).

Muitas vezes o tratamento de dados compreende, atualmente, uma ameaça muito mais severa à intimidade e à vida privada do indivíduo do que as complexidades habituais, que ensejaram o surgimento desse direito. Dessa forma, se é visível que o texto constitucional de 1988 não poderia negar-lhe o amparo constitucional mediante os bancos de dados, que compreendem riscos contínuos para todos os cidadãos.

Dessa forma, verifica-se a relevância de uma legislação específica sobre dados pessoais para assegurar os direitos dispostos no texto constitucional. Em 2016, Raminelli e Rodegheri (2016, p. 98) evidenciaram a necessidade de se elaborar uma legislação específica para proteger o direito à privacidade, “uma vez que este é amparado genericamente pelas constituições.”

Posto isso, em observância ao controle de dados pessoais, especialmente os dados sensíveis tão valiosos para seu titular, tendo este, o direito de evitar que suas informações sejam usadas de modo que lhe possa acarretar danos, fundado no princípio da dignidade humana, é possível aferir que o manuseio de tais dados por pessoas jurídicas de direito público e/ou privado carecem regulamentação própria que direcione e restrinja a atuação de controladores e operadores (RAMINELLI; RODEGHERI, 2016, p. 99).

Por ser extensa a dimensão do plano digital, se demonstra ainda mais complexo o controle dos dados pessoais na internet, onde, geralmente, são disseminadas informações de bancos de dados, o que ocasiona muita insegurança

ao titular no que tange ao rumo que será colocado a tais informações de ordem pessoal, íntima e privada.

Portanto, com o advento da Lei Geral de Proteção de Dados no Brasil, foi possível verificar a ação adotada pelo legislador pátrio em benefício da transparência, liberdade e proteção jurídica relativa aos direitos fundamentais da personalidade. Apresentando artigos que tornam a relação do titular com os agentes de tratamento ainda mais clara e eivada de boa-fé. Assim, a LGPD coloca o Brasil em pé de igualdade com outros países que já dispunham de legislação específica, sendo suprimidos problemas como a ausência de jurisdição em estabelecidos casos em que os dados são requeridos e não são alcançados sob o fundamento de não existir norma específica.

2.2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD), SEUS OBJETIVOS E A CRIAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD

Com o advento da Lei nº 13.709/2018, reconhecida como a Lei Geral de Proteção de Dados – LGPD, o Brasil passou a compor, com determinado atraso, a gama de países que possuem uma lei específica de proteção a dados pessoais. As consequências da demora na elaboração da supracitada lei são antagônicas, uma vez que, por um lado, a lei viabilizou que o tratamento de dados pessoais se comportasse em uma verdadeira “terra sem lei” e, por outro lado, admitiu ao legislador pátrio verificar a experiência internacional para constituir uma lei mais coesa e efetiva, mesmo que tenha que contemplar o cenário político e cultural brasileiro (BRASIL, 2018).

Dessa forma, no cotidiano brasileiro, quando se deixava de utilizar determinada plataforma virtual, acreditava-se que com a desabilitação os provedores deixavam de deter os dados do usuário. Todavia, o verdadeiro contexto é que ainda excluídas as contas, os dados continuam disponíveis ou armazenados na plataforma. Com o advento da proteção de dados pelo Marco Civil da Internet, e com a ratificação pela Lei Geral de Proteção de dados, o usuário poderá solicitar a exclusão definitiva de seus dados pessoais ofertados à aplicação na seara digital, demanda esta que deverá ser suprida pelo provedor nos ditames da legislação (PEREIRA, 2018, p. 3).

Com base na intensa e elevada utilização da seara virtual pelos indivíduos, a circulação contínua de dados na rede se desenvolve em velocidade assustadora. O

uso de smartphones e outros meios tecnológicos, possibilitado pela Internet das Coisas, o fluxo de informações e dados são expandidos e facilmente alcançados por organizações.

Para efetuar compras no mercado eletrônico, é necessário obter a disponibilização de relevantes dados pessoais, cartões de crédito, endereços, etc. Desse modo, as redes sociais possuem as mais variadas informações, preferências e posições dos usuários. As organizações, em geral, acumulam tais dados com determinadas informações, como nome, profissão, origem, transações profissionais, dentre outras informações de caráter sigiloso (SAMODOSSI, 2018, p. 122).

Nessa toada, o entendimento de Pereira (2018, p. 4) sustenta que:

> Para fins de aplicação prática, os dados pessoais coletados por estas empresas são todas e quaisquer informações, como nome, CPF, RG, nacionalidade, estado civil, profissão, escolaridade, dentre outras. Dado pessoal sensível é 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. Distintamente de Dado anonimizado, relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

A LGPD no Brasil, objetiva regular no plano público e privado, a utilização, proteção e transferência de dados pessoais, além de estabelecer quem são os sujeitos envolvidos e seus domínios de responsabilidade por incidentes. A supracitada Lei acarreta impactos diretos em organizações do ramo, tendo em vista que pode estabelecer multas por descumprimentos fundados no grupo econômico que a organização infratora se encontra incluída (PEREIRA, 2018, p. 4).

Nessa perspectiva, a LGPD possui também como finalidade assegurar as garantias e os direitos fundamentais dispostos no texto constitucional de 1988, sobretudo os que tangem à privacidade, à liberdade e ainda o desenvolvimento econômico e tecnológico. Todavia, evidencia-se em seus princípios o da transparência da finalidade, segundo o qual os dados só devem ser usados para objetivos específicos para os quais foram recolhidos e previamente informados aos seus titulares. (SAMODOSSI, 2018, p. 124).

A LGPD, em seu artigo 5º, conceitua dado pessoal como sendo “a informação relacionada a pessoa natural identificada ou identificável”, e toda intervenção da

operação envolvida, apontando os conceitos de titular, operador, controlador, transferência, compartilhamento etc. (BRASIL, 2018)

O texto normativo estabelece que estão passíveis à aplicação da LGPD, sobretudo no plano digital, as pessoas naturais ou jurídicas de direito público ou privado que estejam localizadas em solo pátrio ou que possuam por objetivo o oferecimento de produtos ou serviços no Brasil, devendo a partir da LGPD deter o consentimento expresso do usuário para tal feito.

Sobre a definição de consentimento, compreende-se ao pé da lei, que é toda manifestação livre, informada e inequívoca do titular dos dados, apontando expressamente a sua concordância com o tratamento de seus dados pessoais para um objetivo específico, não sendo acatadas autorizações genéricas, sendo restrito o tratamento de dados, caso a autorização tenha sido alcançada mediante vício de consentimento. (SAMODOSSI, 2018, p. 126)

No tocante ao consentimento, este transparece como a principal questão na conjuntura normativa, e a LGPD elenca diversos requisitos para sua validade. Dentre os referidos, verificam-se as informações sobre o tratamento de dados, como, por exemplo, a identificação do controlador e a relação dos dados obtidos, a responsabilidade dos agentes de tratamentos, objetivos e duração.

Por ser um assunto que eleva várias dúvidas, verifica-se ainda o procedimento de revogação do consentimento no uso de dados pela plataforma que não sejam condizentes aos requisitos informados. A LGPD ainda dispõe o direito dos usuários ao acesso e alcance, conforme requisição, de todos os dados que foram manuseados e o adequado tratamento e retificação de informações, haja vista constituir em dever dos agentes manter os dados sempre corretos. (OLIVEIRA, 2018, p. 85)

A lei em comento, ainda, cria a Autoridade Nacional de Proteção de Dados (ANPD), o órgão federal encarregado de fiscalizar os procedimentos e de editar as normas relacionadas à proteção de dados pessoais. Dentre um vasto rol de competência proveniente ao órgão em comento, localizado inicialmente no art. 55-A, incluído pela Lei nº 13.853/2019, frisa-se a obrigação de zelar pela integridade e proteção dos dados pessoais; fiscalizar e aplicar as sanções previstas na lei; promover a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; a edição de regulamentos e procedimentos sobre a proteção de dados pessoais e privacidade; celebrar em qualquer turno o compromisso com agentes de

tratamento sobre a erradicação de irregularidades; e garantir que o tratamento de dados seja oportunizado na forma mais simples e coesa possível (BRASIL, 2018).

Todavia, em 13 de junho de 2022, mediante a Medida Provisória nº 1.124/2022, a Autoridade Nacional de Proteção de Dados passou a ser uma autarquia de natureza especial. O órgão está sujeito ao regime autárquico especial, com patrimônio próprio e com sede e foro no Distrito Federal.

A Medida Provisória de 2022 repõe o teor original da Lei 13.709/2018, que dispunha a respeito da criação de uma agência reguladora, autarquia especial com personalidade jurídica própria, componente da administração pública indireta. É um serviço autônomo, com patrimônio e receita próprios, para desempenhar atividades para as quais se demande, para seu adequado funcionamento, gestão administrativa e financeira descentralizada (BRASIL, 2018).

As agências reguladoras têm função normativa, fiscalizadora e sancionatória, podendo edificar disposições infralegais para demandar seu cumprimento e punir sua eventual violação, fundamentada no perfil técnico de seus dirigentes, todos com especialização na área. No que diz respeito ao regime de pessoal, é proibido exonerar ad nutum, isto é, atribui maior segurança ao dirigente para cumprir seu mandato, sem depender de possíveis pressões políticas. Viabiliza uma independência técnica mais profunda, intencionando um adequado desempenho para o setor que representa; e não propriamente aos interesses partidários (PSCHEIDT, 2022, p. 2).

Até então, o modelo praticado, criado pela Lei nº 13.853/2019, era um órgão público sem personalidade jurídica própria, que integrava a Administração Pública direta. Ele era composto por serviços que faziam parte da estrutura administrativa da Presidência da República e dos Ministérios, mas não tinha autonomia técnica, financeira ou fontes de receitas próprias, sendo totalmente subordinado ao Presidente da República. O órgão sofria influência política e partidária direta, pois estava habituado, ligado e compromissado com planos de governos e de partido. Não obstante, a própria Lei 13.853/2019 assinalava que cabia ao Presidente da República estabelecer o afastamento preventivo, caso houvesse necessidade, e articular o julgamento acerca dos trabalhos dos componentes do Conselho Diretor (PSCHEIDT, 2022, p. 2).

Consequentemente, a MP nº 1.124/2022 retifica uma distorção jurídica, que intencionava conferir autonomia em um local onde esta não existia. Na implementação de um "mero" órgão, o Poder Executivo possuía total controle regulamentar, o que

determinava diretrizes a respeito da proteção de dados de acordo com o plano de governo. Isso minorava alguns conflitos, mas tornava qualquer regulamento consecutivo ainda mais suscetível a questões políticas, o que era uma grande fonte de inquietação.

Sendo assim, chega-se à conclusão de que as considerações expostas acima obstam o andamento de qualquer entidade fiscalizatória. Não é de hoje que muitos ocupantes do Poder Executivo são respaldados (nos mais diversos sentidos) por grandes instituições privadas; e estas sem dúvidas exigiam sua contrapartida. Atualmente, com a edição da supracitada MP, o cenário está diferente, pois a ANPD conquista força, robustez e independência para finalmente efetivar as regras da LGPD.

2.3 OS DADOS PESSOAIS COMO DIREITO FUNDAMENTAL E SEU RECONHECIMENTO NO BRASIL

No Brasil, o texto constitucional de 1988, ainda que faça menção, em seu art. 5º, XII, ao sigilo das comunicações de dados, não engloba expressamente um direito fundamental à proteção e livre disposição de dados pelo seu referido titular, sendo o reconhecimento de tal direito um assunto que suscita muitas dúvidas no sistema jurídico brasileiro (BRASIL, 1988).

A proteção dos dados pessoais, por seu turno, além da menção ao sigilo da comunicação de dados, ainda encontra amparo parcial mediante a previsão de *habeas data*, com fulcro no artigo 5º, LXXII, da CF/88, ação constitucional, com status de direito-garantia fundamental autônomo, que rigorosamente almeja garantir ao indivíduo o conhecimento e até mesmo a viabilidade de alcançar a retificação de dados que permeiam os registros ou banco de dados de entidades governamentais ou de viés público, “ao mesmo tempo em que se trata de uma garantia procedimental do exercício da autodeterminação informacional.” (MENDES, 2018, p. 185)

Através do reconhecimento de um direito material de proteção de dados pessoais no texto constitucional de 1988, elevam-se novas possibilidades para o exercício dessa ação, de maneira a viabilizar uma compreensão de sua aplicação compatível com a relevância da proteção de dados pessoais no atual contexto informatizado. Sob este viés, verifica-se que as hipóteses dispostas no art. 5º, LXXII, da CF/88 são somente algumas das formas processuais de proteção da privacidade,

não esvaindo, desse modo, todos os mecanismos constitucionais de tutela. (BRASIL, 1988)

Dessa forma, constata-se que o *habeas data* detém características não desvendadas, cuja revelação dependerá estritamente da adequada aplicação do direito fundamental à proteção de dados, assim como da extensão da interpretação sobre as condições processuais dessa ação. Assim, o habeas data se demonstra uma ferramenta poderosa, cujo potencial ainda não foi totalmente averiguado pela interpretação constitucional.

No tocante ao reconhecimento dos dados pessoais como direito fundamental pelo Supremo Tribunal Federal, verifica-se que nos dias 06 e 07 de maio de 2020, a Suprema Corte proferiu uma decisão importante para o exercício da proteção de dados pessoais no Brasil. Através da maioria de dez votos favoráveis, o STF referendou a Medida Cautelar conferida pela Ministra Rosa Weber, relatora da ADI 6.387. Nesse sentido, a Suprema Corte cessou a eficácia da MP nº 954/2020, a qual, em seu art. 2º estabelecia que as organizações de telecomunicações partilhassem com o Instituto Brasileiro de Geografia e Estatística – IBGE, os dados de seus consumidores. (STF, 2020)

A Suprema Corte edificou, desse modo, uma tutela constitucional mais extensa e abstrata do que o direito à inviolabilidade da seara íntima e da vida privada. A mencionada tutela poderá ser aferida em diversos casos posteriores que comportam o compartilhamento, a coleta e o processamento de dados pessoais em solo pátrio. A matéria desse direito fundamental exorbita o indivíduo protegido pelo direito à privacidade, uma vez que não se restringe somente aos dados íntimos ou privados, muito pelo contrário, diz respeito a qualquer dado capaz de identificar uma pessoa. De acordo com o entendimento do Ministro Gilmar Mendes:

> Trata-se de direito autônomo e com contornos próprios, extraído de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa. (STF, 2020)

Desse modo, é possível verificar que o reconhecimento desse direito fundamental, no campo de argumentação dos diversos votos enunciados, é uma

grande evolução no que diz respeito à tutela constitucional dos dados pessoais no sistema jurídico pátrio. Será necessário, todavia, demarcar suas nuances, tanto na jurisprudência quanto na doutrina brasileira.

Sendo assim, se demonstra essencial no cenário brasileiro, além da LGPD, outras legislações que tratem sobre o assunto, a fim de permear a necessidade de não somente primar pela consistência constitucional do marco normativo infraconstitucional, como também de propiciar sua integração e harmonia produtiva, de maneira a superar possíveis problemas e garantir ao direito fundamental à proteção de dados, sua plena concretização e efetividade.

O Direito Civil aborda os dados pessoais na proteção do direito da personalidade, no art. 12 do CC/2002 e quando dispõe a regulação geral dos direitos da personalidade dos artigos 11 ao 21 do mesmo Diploma. Especificamente, o dispositivo 12 supracitado protege o titular dos dados pessoais contra possíveis atividades de tratamento capazes de ferir qualquer destes direitos, ao atribuir a ele os direitos de “exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.” Desta feita, a LGPD possui dentre as suas finalidades o pleno desenvolvimento da personalidade da pessoa natural (art. 1º e 2º, VII) e respalda a personalidade no direito de revisão das decisões automatizadas (CARDOSO, 2020, p. 3).

2.4 DISTINÇÕES ENTRE DADOS PESSOAIS, PESSOAIS SENSÍVEIS E ANONIMIZADOS

Imperioso trazer à lume, as distinções entre os dados pessoais, dados pessoais sensíveis e dados anonimizados, previstos na Lei nº 13.709/2018. Os dados pessoais são aqueles relacionados a nome, CPF, RG, e-mail, data de nascimento, telefone, endereço residencial, cartão bancário, localização via GPS, todos os dados que permitam identificar, direta ou indiretamente, uma pessoa natural (física). Sendo assim, não existem dados pessoais de pessoas jurídicas, no entanto, isso não quer dizer que estas não produzem ou não podem ser titulares de dados, mas somente que estas não se enquadram como dados pessoais protegidos pela LGPD (BRASIL, 2018).

Com base nesse conceito, os dados podem ser entendidos como elementos que não necessariamente possuem significado inteligível isoladamente, enquanto a

informação consiste em dados ordenados para gerar e transferir conhecimento. Desse modo, os dados são processados para gerar informações que, por seu turno, produzem conhecimento e, em última análise, valor econômico. Por conseguinte, a informação é extraída dos dados (inclusive de sua relação a uma pessoa), e não o contrário. Portanto, pode-se dizer que os dados são a matéria-prima da informação (MENDES, 2014, p. 88).

Por exemplo, nomes, endereços de e-mail e números de telefone são dados pessoais, pois são relativos a uma pessoa natural. O conhecimento de que todos esses dados pertencem à uma mesma pessoa é informação. Além disso, saber que o nome e o endereço de e-mail pertencem à mesma pessoa, mas o número de telefone não pertence à mesma pessoa, também é informação (distinta da anterior).

Depois do dado pessoal, a LGPD define em seu inc. II do art. 5 o que são dados pessoais sensíveis:

> [...] 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.

As técnicas legislativas empregadas na definição conceitual foram inicialmente inadequadas, pois o inciso I conceitua dados pessoais, à medida que o inciso II do art. 5º da LGPD não define dados pessoais sensíveis, somente se limita a elencar exemplos. A LGPD possui uma classificação parcial, que cria uma distinção entre os dados, mas define somente um lado dessa distinção, razão pela qual os conceitos opostos são delineados por exclusão (BRASIL, 2018).

Primeiramente, os dados que não se enquadram no conceito legal de dados pessoais (artigo 5º, inc. I) são considerados dados não pessoais e não são abrangidos pela LGPD. Na última hipótese, por exemplo, se enquadram dados de pessoas jurídicas (que não podem ser relacionados a pessoas físicas). Em segundo lugar, os dados relativos a pessoas naturais que não se enquadrem no conceito jurídico de dados pessoais sensíveis (artigo 5.º II) são considerados dados pessoais em sentido estrito, ou não sensíveis (BRASIL, 2018).

Sendo assim, o assunto é polêmico e não há conformidade na doutrina pátria, uma vez que também se defende que o rol é taxativo para aferir segurança jurídica

aos agentes de tratamento e afastar questionamentos sobre quais são os dados pessoais sensíveis.

Por último, os dados anonimizados, previstos no art. 5º, III, da Lei nº 13.709/2018, são referentes aos dados relativos ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Estes, no entanto, só serão protegidos pela LGPD se puderem ser revertidos e tornarem a identificação possível (BRASIL, 2018).

2.5 APLICABILIDADE DA LGPD NO ÂMBITO PÚBLICO E PRIVADO

No que diz respeito ao setor privado, as organizações empresariais, como vislumbrado, deverão elevar esforços para desenvolver suas atividades em conformidade à Lei Geral de Proteção de Dados Pessoais, empregando-se um sistema capaz de mapear e classificar informações em sua propriedade, aferindo-se o grau equivalente de segurança e limitação de acesso, demandando investimentos no treinamento contínuo de todos seus funcionários e dirigentes. A disposição é que a LGPD alcançará, sobretudo, os âmbitos de recursos humanos, escritórios de advocacia, hospitais, dentre outros, tendo em vista o extenso fluxo de armazenamento de informações de outros indivíduos.

No plano virtual privado, ações como a permissão de termos de uso e políticas de privacidade de complexa assimilação com somente um clique será foco da reestruturação da LGPD, uma vez que o consentimento deve ser fundado na permissão de informações totalmente compreensíveis e, quando for possível, ser requerido de maneira gradual, conforme sua necessidade e objetivo.

Desta feita, dados pessoais como, por exemplo RG, CPF, endereço, telefone e dados sensíveis deverão observar estritamente os deveres de tratamentos dispostos pela LGPD, especialmente relativo ao sigilo, gestão e segurança de tais informações. Nesse sentido, a ação de estabelecimentos como farmácias pedirem dados pessoais para a venda de produtos que não envolvem medicamentação, passou a ser uma prática inapropriada.

Por sua vez, as redes sociais denotam maior atenção por parte de seus usuários, à medida em que a superexposição ocorrida não é tutelada pela legislação. Isto é, a livre propagação de informações pessoais em tais plataformas, por exemplo, pode ocasionar drásticos efeitos quando não se verificar o real consentimento do

titular. Cumpre destacar que as redes sociais se valem da monetização de dados pessoais para viabilizar seu acesso, assim, estas também passam por adequação no cerne da LGPD em relação aos termos de uso e políticas de privacidade para torná-los mais nítidos e finalísticos ante que o usuário permita o pleno acesso a informações de natureza substancialmente pessoal, como vídeos, fotos, localizações, dentre outros (FRAZÃO, 2018, p. 56).

Estas são apenas algumas exemplificações de âmbitos que estão sendo impactados pela adequação à legislação de dados. Ademais, vale evidenciar que a LGPD trouxe consigo uma diversidade de contribuições como a viabilidade do livre fluxo de dados com nações signatárias do Regulamento Europeu, ampliando, assim, a competitividade das empresas nacionais e simplificando a internacionalização de iniciativas do Brasil (SOUZA, 2018, p. 115).

Ainda, destaca-se a transparência trazida ao mercado como elemento que impulsiona a confiança de titulares de dados nos mercados em conformidade à LGPD, tendo em vista a certeza do controle do usuário sobre as informações que lhe dizem respeito e, também, a distinção substancial em mercados muito competitivos, onde a organização por intermédio do compliance com a LGPD será levada em consideração em comparação a outra empresa que não apresenta cuidados com as informações pessoais de seus clientes.

Desse modo, o entendimento de Frazão sustenta que vislumbrar a LGPD como um caminho (mesmo que complexo) é muito mais benéfico do que combatê-la como se inimigo fosse. A inovação consiste na criação de modos de se solucionar impasses ou de superar empecilhos, desde que em conformidade às regras do jogo. Se o contrário ocorresse, a inovação se tornaria automaticamente ilícita e nociva não apenas para o malfeitor, mas para o mercado como um todo (FRAZÃO, 2018, p. 58).

Em suma, a LGPD possui o intento de concretizar adequadamente o contrário, trabalhando para o impulsionamento da inovação responsável e para o incentivo de edificação de modelos negociais não apenas factíveis no viés comercial, como também sob o enfoque da privacidade de todos os seus usuários (FRAZÃO, 2018, p. 58).

No cerne do setor público, verifica-se que seria infactível que o próprio Poder Público ignorasse uma legislação que versa sobre a privacidade e a proteção de dados de seus próprios administrados, sendo o ente estatal o possuidor de um big data incomparável e o principal agente de tratamento das supracitadas informações.

Assim, a aplicação da legislação de dados ao cerne do Poder Público e Privado, consubstancialmente de modo indistinto, mesmo que observadas algumas diferenças, é uma grande empreitada, que se não for verdadeiramente superada, coloca em questão a *ratio legis* da Lei, que é tutelar os dados pessoais e a privacidade dos indivíduos contra abusividades e aferir maior controle do titular dos dados sobre suas informações, durante todo o processo de tratamento, independentemente da natureza da organização empresarial (MIGUEL, 2019, p. 256).

Um fator frequentemente encontrado em termos e condições no setor público e privado, diz respeito às cláusulas genéricas e o colhimento indiscriminado de dados pessoais. Nesse diapasão, o dispositivo 6º da LGPD coíbe condutas que almejam o colhimento de excedentes informacionais, o condicionando aos princípios da necessidade e finalidade, que serão expostos em tópico específico. (BRASIL, 2018)

Em outro enfoque, verifica-se a elevada utilização da tecnologia na governança pública em nível global, a título de exemplificação nota-se a Estônia que viabilizou aos indivíduos o acesso a todo e qualquer serviço público em plataforma virtual. Utilizando-se da identidade digital, as pessoas conseguem ter acesso, por exemplo, aos serviços relativos à Previdência Social, como agendamentos de consultas, registros de empresas e licenciamentos, dentre outros (SOUZA, 2018, p. 88).

Portanto, verifica-se que nosso país também transita nesse sentido, o de desburocratizar a adequada utilização da tecnologia em benefício da eficiência da Administração Pública e na qualidade de vida dos administrados, ainda que gradativamente. Mesmo que o Brasil ainda não tenha disposto um documento digital único, já foram viabilizados documentos como a Carteira Nacional de Habilitação digital, a Carteira de Trabalho e o Título de Eleitor, por exemplo. Assim, retira-se deste fato a latente necessidade de investimentos nos campos de segurança da informação e proteção de dados pessoais, para que as supracitadas soluções não se tornem um problema no país.

2.6 AGENTES DE TRATAMENTO

No que tange aos agentes de tratamento, com base nas inovações apresentadas pela LGPD e com fulcro em seu dispositivo 5º, inc. IX, estes são compreendidos em controlador e operador. A priori, para que se possa definir

adequadamente a relevância dessa inovação legislativa, Oliveira realiza uma pertinente analogia, ao equiparar tais figuras com o consumidor e o fornecedor, elevados pela Lei nº 8.078/1990 (COTS; OLIVEIRA, 2019).

O autor aponta, inicialmente, que mesmo que existam dissemelhanças a respeito de seus conceitos, oriundas da condição de determinados indivíduos em alguns casos concretos, se o supracitado Código não trouxesse tais conceituações, a complexidade seria ainda maior. Desta feita, igualmente à legislação consumerista, a LGPD também edificou as figuras do operador e do controlador, a fim de delinear direitos e obrigações, deixando mais nítido o status de cada indivíduo que participa do tratamento de dados pessoais. Para tanto, o doutrinador conceitua o controlador como "aquele que decide sobre o tratamento de dados, à medida que o operador é quem trata dos dados por ordem do primeiro indivíduo" (OLIVEIRA, 2018, p. 254).

O autor ainda sustenta que a conceituação será de muita utilidade no cerne da responsabilidade dos agentes, o que demandará que as organizações empresariais no geral determinem muito bem a função que anseiam revestir no tratamento de dados pessoais. A título de exemplificação, nota-se que se uma organização almeja deliberar sobre os dados alcançados, investirá a função de controlador e responderá - de modo direto - pelos danos aferidos ao titular, "de maneira solidária com os demais controladores constantes na mesma relação." (OLIVEIRA, 2018, p. 255)

Todavia, se a organização almeja tão-somente prestar serviços abalizados em contratos comerciais, sem o envolvimento em processos decisórios que englobam o tratamento de dados pessoais, a supracitada organização será classificada na figura do operador, "respondendo somente pelos danos que aferir causa por inobservância da lei ou do instrumento contratual." (OLIVEIRA, 2018, p. 255)

Evidencia-se que tal baliza possui o intento de coibir o compartilhamento indiscriminado dos dados pessoais, tendo em vista que o controlador não viabilizará mais que seus operadores se utilizem das bases de dados alcançadas pelo seu contratante, como outrora era corriqueiro. Sendo assim, tais premissas viabilizam que não exista mais um compartilhamento de dados do titular em uma conjuntura nunca almejada por este.

Prosseguindo com a definição de agentes de tratamento elevada pela LGPD, nota-se que esta obteve nítida influência do GDPR. Em consonância ao seu dispositivo 5º, a LGPD conceitua como controlador "a pessoa natural ou jurídica, de

direito público ou privado, a quem competem as deliberações relativas ao tratamento de dados pessoais", revelando-se em comparação ao conceito de *data controller* do dispositivo 4º, item 7, da GDPR. Por sua vez, no que tange ao operador, a LGPD o conceitua como "a pessoa natural ou jurídica, de direito público ou privado, que efetua o tratamento de dados pessoais em nome do controlador", demonstrando-se tal definição em consonância ao art. 4, item 8, da GDPR, que trata sobre o *data processor* (MALDONADO; BLUM, 2018, p. 200).

Com base nas considerações realizadas, é possível concluir que o controlador se demonstra a figura principal quando se trata da tutela dos direitos dos titulares, isto é, consiste no indivíduo que toma as decisões concernentes aos dados pessoais. Decorrente disso, a maioria das responsabilidades pela consonância com a LGPD recai sobre tal figura, possuindo como encargo, desse modo, controlar a finalidade e as formas gerais de como os dados devem ser utilizados.

Assim, verifica-se que é o controlador que delibera o porquê do colhimento dos dados do titular; como será realizado seu tratamento, por intermédio das hipóteses permissivas do art. 7º da LGPD; sobre quais pessoas irá realizar a coleta de dados; quais dados pessoais serão alcançados (conteúdo); o objetivo ou propósito para os quais os dados pessoais serão utilizados; e a decisão em divulgar, compartilhar, transferir e por quanto tempo estes serão retidos. (BRASIL, 2018)

Por sua vez, quando se trata do operador de dados pessoais a delimitação de suas tarefas se demonstra complexa, tendo em vista que está restrito ao processamento de dados em conformidade às instruções e o objetivo aferido pelo controlador, não sendo possível exercer controle sobre os dados ou modificar o propósito de seu tratamento. (HOSKEN, 2018, p. 45)

Contudo, tal figura possui como responsabilidade promover garantias para instauração de medidas organizacionais e técnicas apropriadas, de maneira que o processamento alcance os requisitos dispostos na legislação e de segurança. Isto é, o operador possui a liberdade de utilizar o conhecimento técnico para deliberar como serão realizadas determinadas atividades em nome do controlador, mas não impõe decisões sobre o que é realizado com os dados (HOSKEN, 2018, p. 46).

Portanto, tem-se que o dispositivo 39 da LGPD deixa nítida a determinação de que o operador apenas tratará os dados pessoais em consonância às instruções apresentadas pelo controlador, sem realizar qualquer modificação nestas. No entanto, verifica-se que isso não isenta o operador de empregar medidas técnicas e

organizacionais relativas à segurança, com fulcro no art. 46 do mesmo Diploma (BRASIL, 2018).

3 O VAZAMENTO DE DADOS PESSOAIS SENSÍVEIS PREVISTOS NA LEI GERAL DE PROTEÇÃO DE DADOS E SUA RESPONSABILIZAÇÃO

3.1 PRINCÍPIOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

Através das disposições contidas na CF/88 e na LGPD, é factível observar uma imposição de princípios norteadores que deverão ser obedecidos no uso da informática aferido ao tratamento de dados, sobretudo no que tange aos direitos fundamentais e à ordem constitucional do Estado Democrático de Direito.

Evidenciam-se, no art. 6º da LGPD, os seguintes princípios que operam como mandamentos do ordenamento: o princípio da boa-fé (caput), o princípio da finalidade (inciso I), o princípio da adequação (inciso II), o princípio da necessidade (inciso III), o princípio do livre acesso (inciso IV), o princípio da qualidade dos dados (inciso V), o princípio da transparência (inciso VI), o princípio da segurança (inciso VII), o princípio da prevenção (inciso VIII), o princípio da não discriminação (inciso IX) e o princípio da responsabilização e da prestação de contas (inciso X) (BRASIL, 2018).

O dispositivo 6º da supracitada Lei estabelece que as atividades concernentes ao tratamento de dados pessoais deverão respeitar o princípio da boa-fé. A boa-fé objetiva compreende deveres de condutas contratuais, de natureza secundária, instrumental, anexa ou lateral, tais quais os de informação adequada, esclarecimento, lealdade etc., encontrando-se disposta nos arts. 4º, III e 51, IV do CDC, que estabelecem um diálogo com as disposições gerais dos arts. 113, 187 e 422 do Código Civil de 2002.

A denominada boa-fé contratual é oriunda da acepção de obrigação como processo, e denota uma conduta de cooperação, lealdade e expectativas verdadeiras das partes, sobretudo o titular, face ao controlador (art. 10 da LGPD), o que se revela a partir das circunstâncias reais em que se deu o consentimento, o objetivo de utilização e o tratamento de dados pertinente, bem como as informações prévias dispostas. A premissa da confiança do consumidor engloba tanto a crença nas informações fornecidas quanto de que aquele que possua acesso aos seus dados, em razão do consentimento aferido, não se porte de maneira divergente a elas e observe a vinculação ao objetivo de uso (MIRAGEM, 2019, p. 105).

A boa-fé, além de ser considerada direcionadora das atividades que envolvem o tratamento de dados pessoais, inclusive na sua utilização secundária; além de

disposta no art. 6º, caput, é também mencionada no art. 7º, 3º, que aduz “o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização”, assim como compreende baliza e critério para a aferição de sanções administrativas, com fulcro no art. 52, § 1º, II, da LGPD (BRASIL, 2018).

Assim, o princípio da boa-fé contratual, que engloba a principal seara de atuação da boa-fé objetiva, consiste em uma verdadeira e legítima expectativa por parte do consumidor do produto ou serviço, que deve portar razões para confiar na contraparte (NORONHA, 1994, p. 255).

Por seu turno, no que tange ao princípio da finalidade, verifica-se que todo procedimento conexo ao sistema de tratamento de dados, sendo este automatizado ou não, deve ser efetuado sempre e estritamente no sentido de alcançar as finalidades propostas para o sistema. Sendo assim, é necessário verificar os critérios de proporcionalidade e adequação entre os meios e as finalidades, em todas as fases do processamento de informações, que se materializam em requisitos de limitação: do colhimento e do armazenamento; da conservação, da utilização e da comunicação dos dados (SAMPAIO, 1998, p. 312).

A finalidade deve alcançar seu reconhecimento antes da realização de coleta dos dados, sendo especificada, especialmente, na relação entre os dados coletados e seu propósito, além do seu uso não abusivo e na extirpação ou anonimização dos dados que não forem mais úteis e necessários (RODOTÀ, 2008, p. 90).

O dispositivo 6º, I, da LGPD conceitua o princípio da finalidade, ligando-o à “realização do tratamento para objetivos legítimos, específicos, explícitos e informados ao titular, sem a viabilidade de tratamento futuro de maneira desarmônica com tais finalidades.” Em observância ao referido princípio, demonstra-se embasada a limitação da transferência de dados pessoais a terceiros, além de se poder, por intermédio deste, organizar um critério para valorar a razoabilidade do uso de determinados dados para um certo fim (MIRAGEM, 2019, p. 107).

O dispositivo 7º da LGPD, como demonstrado, estabelece as finalidades legítimas para o tratamento de dados pessoais. No tocante aos dados sensíveis, as supracitadas finalidades são delineadas de maneira mais estrita, no art. 11 da mesma Lei. Isso embasa uma limitação do colhimento e armazenamento de dados, de maneira que tais processos devem sempre se abalizar às informações puramente necessárias ao fim da operação. Similarmente, a qualidade dos dados ressalta a

obediência ao supracitado princípio, pois os dados devem ser completos, exatos, pertinentes e importantes às finalidades almejadas (BRASIL, 2018).

Assim, o indivíduo que almeja alcançar o consentimento do titular dos dados obriga-se a se sujeitar expressamente às finalidades para as quais pretende usar os dados, conectando-se aos termos desta sua expressão pré-negocial. Desta feita, a finalidade consiste na restrição temporal do tratamento de dados, de maneira que as informações colhidas e armazenadas não devem permear os bancos de dados por um lapso maior do que o essencialmente indispensável ao alcance das finalidades elencadas. Portanto, o dispositivo 15 da LGPD dispõe as situações da cessação do tratamento de dados pessoais (BRASIL, 2018).

Em seguida, a adequação é determinada no dispositivo 6º, II, da LGPD pela "compatibilidade do tratamento com as finalidades expostas ao titular, em consonância ao contexto do tratamento." O mencionado princípio possui como base o foco no procedimento executado para se alcançar o objetivo pretendido. Seu propósito consiste na conservação da ligação indispensável entre a finalidade e o uso dos dados informado ao titular e seu concreto atendimento na realização do tratamento de dados (COTS; OLIVEIRA, 2019, p. 199).

Liga-se de maneira direta ao consentimento aferido pelo titular para o tratamento dos dados ou às demais finalidade legais permitidas, que deverão ser expostas, lado a lado com a situação de confiança que se edifica a partir do correto e estrito atendimento nos termos da informação prévia ao consentimento ou ao uso informado (COTS; OLIVEIRA, 2019, p. 200).

Passando ao princípio da necessidade, o dispositivo 6º, III, da LGPD aduz que "da limitação do tratamento ao mínimo necessário para a concreção de suas finalidades, com amplitude dos dados apropriados, proporcionais e não excessivos em relação às finalidades do tratamento." A utilização dos dados pessoais, dessa forma, deve se limitar ao mínimo necessário que supra os objetivos de consentimento do titular e a finalidade legítima, verificada a adequação entre meios e fins, de maneira correta, proporcional e não excessiva (BRASIL, 2018).

Com base na LGPD em seu art. 6º, IV, compreende o livre acesso na "garantia, aos titulares, de consulta simplificada e gratuita sobre a forma e duração do tratamento, assim como sobre a integralidade de seus dados pessoais." O mencionado princípio demonstra-se conexo à publicidade e seu propósito é o de amparar a efetiva participação dos titulares de dados em seu tratamento, exprimida

na obrigação de consentimento e na viabilidade de conhecimento sobre a maneira e amplitude em que se desenvolve tal procedimento. Engloba, sobretudo, a possibilidade de alcançar a cópia dos registros existentes, assim como retificar informações incorretas ou sem precisão, podendo ainda adicionar dados legítimos que possam beneficiar seu interesse (RODOTÀ, 2008, p. 92).

Como bem elucida Miragem, a violação do direito de acesso aos dados pode se configurar não apenas pela mera recursa, mas sim na dinâmica contemporânea do mercado pela colocação de óbices ao acesso, demandando que o consumidor se direcione a distintos indivíduos ou setores para alcançar a informação, “aferindo morosidade injustificada em seu acesso e deixando de simplificar o exercício do direito” (MIRAGEM, 2019, p. 110).

Acerca do princípio da qualidade dos dados a LGPD, em seu dispositivo 6º, V, garante aos titulares a nitidez, exatidão, importância e atualização dos dados, em consonância à sua necessidade e para a realização da finalidade de seu tratamento. (BRASIL, 2018)

Assim, os mencionados princípios se demonstram que muita relevância para a adequada proteção aos dados pessoais, sendo, o mais importante destes, a transparência, pois é o mecanismo pelo qual os indivíduos se utilizam para alcançar maior nitidez e clareza sobre como tais informações serão tratadas.

A transparência é conceituada pelo art. 6º, VI, da LGPD como sendo a garantia, aos titulares, de informações nítidas, precisas e facilmente alcançáveis sobre a execução do tratamento de dados e seus respectivos agentes, verificados os segredos comerciais e industriais. Verifica-se menção à transparência sobre o tratamento de dados e os indivíduos envolvidos em vários ordenamentos jurídicos, inclusive no Regulamento Europeu (BRASIL, 2018).

Conforme o princípio da transparência, todo sistema de colheita, registro, tratamento, processamento, transmissão e de banco de dados deve ser de conhecimento geral. De acordo com Cots e Oliveira (2019, p. 224):

> Isso significa que todos – ou pelo menos aqueles cujos dados tenham sido coletados, registrados, tratados, processados, transmitidos ou armazenados em bancos – devam e possam ter ciência do tipo de informação envolvida, bem como da finalidade da operação envolvida, seja através de publicações periódicas de relatórios pelas unidades de processamento, seja pela disponibilização dos dados, de forma on-line ou não, em escritórios especializados ou até mesmo em bibliotecas e livrarias.

Assim, o princípio da transparência eleva que os dados pessoais deverão ser tratados de maneira nítida e transparente entre o operador e o titular dos dados, obtendo como propósito assegurar que o titular possa ter conhecimento da maneira como seus dados estão sendo usados, havendo duas possibilidades de se flexibilizar o supracitado princípio, que são os segredos comerciais e industriais.

A segurança, por sua vez, é conceituada pelo art. 6º, VII da LGPD como a "utilização de medidas 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 difusão." Refere-se a um desdobramento da segurança demandada do fornecedor em face ao consumidor e seu patrimônio, cuja violação denota a responsabilidade objetiva pelos danos aferidos, sobretudo na situação de os dados serem acessados sem permissão ou acidentalmente, o que depreende ainda as hipóteses referidas (BRASIL, 2018).

O dispositivo 44 da LGPD sustenta que o tratamento de dados pessoais será inadequado quando deixar de respeitar a legislação ou quando não dispor a segurança que os titulares dos dados podem esperar, tendo em vista as circunstâncias relevantes, à medida que o art. 46 e os seguintes comportam normas sobre segurança e boas práticas. Outro princípio norteador da LGPD é o da prevenção, que é definido no VII do referido artigo como "a adoção de medidas para prevenir a ocorrência de danos em razão do tratamento de dados pessoais" (BRASIL, 2018).

Em seguida, o princípio da não discriminação é disposto no art. 6º, IX da mesma Lei como "a impossibilidade de realização do tratamento de dados para fins discriminatórios ilícitos ou abusivos." O benefício ocasionado pelo processamento de dados, no sentido da maior precisão da distinção e da personalização dos indivíduos, não pode servir para aferir danos, restringir ou eliminar qualquer consumidor da possibilidade de acesso ao consumo.

Assim, ilícita se demonstra a discriminação eivada em condições vedadas pela legislação para fins de distinção, cabendo uma menção ao texto constitucional de 1988 que, em seu art. 3º, IV, veda preconceitos de origem, raça, cor, sexo e idade. Similarmente, determina a Carta Magna que "ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política", em seu art. 5º, VIII. (BRASIL, 1988)

Também se demonstra situação de discriminação aquelas que em razão de critérios que não estejam em conformidade com a finalidade para qual se concretize determinada distinção, como aquela que trate de dados sensíveis, para ilustrar, a recusa de fornecimento de produto ou serviço a qualquer indivíduo em virtude de sua orientação sexual ou raça, ou ainda a cobrança de valores distintos para homens e mulheres.

Desta feita, dentre os mecanismos dispostos no art. 20 da LGPD para afastar o tratamento de dados discriminatórios se encontra a disposição do direito do titular dos dados de revisar as decisões tomadas exclusivamente com fundamento em tratamento automatizado de dados pessoais capazes de afetar seus interesses, incluindo-se as decisões norteadas a estabelecer o seu perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade (BRASIL, 2018).

Por último, o princípio da responsabilização e prestação de contas, com fulcro no art. 6º, X da LGPD, encontra sua definição na exigência de comprovação, pelo agente, da aderência de medidas efetivas e aptas de comprovar a observância e o cumprimento das disposições protetivas no cerne dos dados pessoais e, sobretudo, da eficácia de tais medidas (BRASIL, 2018).

A responsabilização e prestação de contas alcançaram eficácia principalmente no âmbito coletivo, sempre que existir interesse difuso, direito coletivo ou individual homogêneo, carecedor de proteção específica, em disposição que se conecta ao art. 6º, VI e VII do CDC. Ainda, o art. 42 da LGPD, na mesma direção, comporta a responsabilização do controlador e do operador que, em virtude do tratamento de dados, aferir a outrem dano patrimonial, moral, individual ou coletivo, em contrariedade à LGPD (BRASIL, 2018).

Portanto, como consequência de tal imperativo, a LGPD, em seu dispositivo 50, dispôs a exigência de programas de *compliance*, no tocante aos agentes de tratamento de dados, sobretudo controladores e operadores, com a aderência de um programa de governança que observe os requisitos como os pressupostos de organização, o regime de funcionamento, os procedimentos, incluindo-se reclamações e petições de titulares, as normas de segurança, as obrigações específicas de cada agente, dentre outros (BRASIL, 2018).

3.2 O VAZAMENTO DE DADOS PESSOAIS SENSÍVEIS E OS ATOS DISCRIMINATÓRIOS

O inadequado tratamento dos dados e a não utilização devida podem acarretar no vazamento de dados pessoais e por consequência gerar atos discriminatórios, práticas de *geopricing*, *geoblocking*, entre outras consequências. Importante a Lei Geral de Proteção de Dados (LGPD) trazer a responsabilização do agente 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, obrigando-o a realizar a reparação, conforme exposto em seu art. 42:

> Art. 42. 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.
> §1° A fim de assegurar a efetiva indenização ao titular dos dados:
> I- o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> §2° 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.
> §3° 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.
> §4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

A LGPD não se limita apenas à reparação por indenização no âmbito cível, traz também a previsão de sanções administrativas como multas diárias ou multas simples, as quais estão limitadas, no total de R$50.000.000,00 (cinquenta milhões de reais) por infração. Cumpre informar que a LGPD não faz referência expressa a investigações ou repressões de infrações penais. De igual modo, também não cria novos tipos penais, servindo apenas como balizadora para a conduta frente à proteção de dados (BRASIL, 2018).

Acerca dos atos discriminatórios, a priori, faz-se necessário elucidar o termo discriminação, que nega oportunidades em função de características que não são aceitas, com vistas a inferiorizar e/ou desqualificar. Normalmente, a discriminação

decorre de um preconceito ou de mais de um, significa também a negativa de direitos e outras prerrogativas em razão, de como bem já mencionado, da desqualificação que se faz sobre certo objeto (pessoas ou grupos).

Ao contrário do preconceito, a discriminação traz implicações jurídicas e em diversos casos constitui ato ilícito civil ou penal. A discriminação pode ser classificada em direta, quando alguém diz claramente ou indireta e nessa seara entram as práticas do *geopricing* e *geoblocking*.

A prática de *geopricing*, utiliza sistema de empresas de *e-commerce* algoritmos para analisar informações como, por exemplo, o endereço de IP do usuário e assim identificar a sua localização geográfica. Com a informação, o valor da oferta do produto ou serviço é definido em razão da região de origem do usuário. Já na prática de *geoblocking*, o sistema utiliza a informação para definir se a oferta de um produto ou serviço estará disponível ou não para usuários de uma determinada região.

Nessa vereda, o MP/RJ, por meio da 5ª promotoria de Justiça de Tutela Coletiva de Defesa do Consumidor e do Contribuinte da Capital, ajuizou uma ação civil pública contra a Decolar.com pela prática de *geoblocking*, isto é, bloqueio da oferta com base na origem geográfica do consumidor - e de *geopricing* - precificação diferenciada da oferta também com base na geolocalização, pela discriminação injustificada.

Entre outros pedidos, o MP/RJ requereu que a Decolar se abstenha de promover qualquer discriminação injustificada de consumidores brasileiros, bem como de permitir que hotéis discriminem quaisquer consumidores com base na origem geográfica ou nacional, tanto pela prática de *geoblocking*, quanto pela prática de *geopricing*, bem como requereu que a empresa fosse condenada a pagar danos materiais e morais a cada um dos consumidores lesados (MP/RJ, 2018).

E, em relação aos danos morais coletivos, pediu para que a Decolar fizesse a reparação no valor mínimo de R$ 57 milhões, a serem revertidos ao Fundo de Reconstituição de Bens Lesados ou à instituição que colabore para promover a recomposição dos interesses coletivos lesados (MP/RJ, 2018).

Cumpre esclarecer que o inquérito partiu de denúncia ofertada pelo escritório Dannemann Siemsen Advogados, na qualidade de representante da Booking.com., alegando o sócio do escritório que:

> As práticas de geoblocking e geopricing são abusivas, discriminatórias e lesivas aos interesses dos consumidores. Em alguns casos, a diferença de preços com base em geolocalização do consumidor alcança 400%. Tais práticas merecem ser descontinuadas, sem prejuízo das indenizações de ordem material e moral aos consumidores lesados (MP/RJ, 2018).

Afora os fatos narrados, as informações obtidas por dados pessoais ajudam a coletar dados, que podem ser utilizados para, por exemplo, saber qual tipo de sapato um determinado grupo compra, qual é o público que a venda é realizada, e essas informações trazem o empoderamento que grandes empresas almejam. Portanto, deve se ter um grande zelo com esses dados e principalmente com os dados pessoais sensíveis, que só devem ser compartilhados mediante consentimento, com fulcro no art. 5º, inc. XII, da LGPD (BRASIL, 2018).

3.3 CONCEITO E PRESSUPOSTOS DA RESPONSABILIDADE CIVIL

Rosenvald entende que “a responsabilidade civil consiste no dever de reparar os danos provocados em uma situação onde um determinado indivíduo sofre prejuízos jurídicos como consequência de atos ilícitos praticados a outrem.” Elencados no Código Civil de 2002, os pressupostos da responsabilidade civil apontam que, caso algum ato ilícito seja cometido e venha causar ou cause danos à integridade física, à honra ou a um bem de outro ser, este dever-se-á ser ressarcido de forma proporcional (ROSENVALD, 2017, p. 34).

Desta forma, a responsabilidade civil trata-se da aplicação de deliberações para compelir um indivíduo a indenizar o dano, patrimônio ou conduta ofensiva causada a terceiros, em virtude de ação praticada por si mesmo, por terceiro a quem é responsável, por algum pertence, ou por mera imposição legal.

Acerca dos pressupostos do dever de indenizar, vale ressaltar que a conduta humana, seja ela omissiva ou comissiva, é imprescindível para que haja a configuração da responsabilidade civil. Visto que, é com base em sua ação ou omissão voluntária que, a inobservância do dever jurídico rudimentar, verificar-se-á o dano gerado a terceiro. Sendo a conduta humana reputada como um dos componentes da responsabilidade civil (ROSENVALD, 2017, p. 119).

A conduta humana classifica-se em positiva quando advém de ação, ou seja, de atitudes pragmáticas por parte do indivíduo, constituído pela execução de atos fomentadores do dano ao âmbito jurídico de terceiro. Em contrapartida, a conduta

denominada negativa resulta de omissão humana, tachada pela recusa, pela inércia ou pela estagnação que culminará em lesão a terceiro.

O fulcro basilar deste elemento é a voluntariedade que compreende simplesmente o discernimento do que se faz, ou seja, de dispor sobre sua ação ou omissão. É, precipuamente, o ânimo em agir de determinada maneira, sendo, desse modo, o impulso causal comportamental. Não podendo, essa consciência, ser confundida com o desígnio de suscitar a lesão, dado que esse ato caracteriza o dolo, elemento que pode ser ou não ser imputado à conduta humana.

Desse modo, Gagliano e Pamplona Filho salientam que essa percepção deve ser entendida como “o conhecimento dos atos materiais que se está praticando, não se exigindo, necessariamente, a consciência subjetiva da ilicitude do ato.” Podem ou não as ações e omissões do ser humano, dependendo da natureza da responsabilidade civil, sofrerem a incidência de dois elementos acidentais, também conhecidos como elementos subjetivos: dolo ou culpa. Em relação ao primeiro elemento, tem-se a conduta dolosa quando o autor tem a intenção de suscitar o resultado danoso. Consequentemente, o autor tem discernimento da ilicitude do resultado que visa alcançar com a sua conduta (GAGLIANO; PAMPLONA FILHO, 2011, p. 80).

Ainda em relação à conduta humana, via de regra, a conduta que propicia a violação ao encargo jurídico primário antecedente, normalmente, configura-se como ato ilícito. Por esse motivo, reitera-se que o ato ilícito é o âmago da responsabilidade civil, seu fato gerador, tal como o parâmetro da reparação do dano. O artigo 186 do Código Civil de 2002 traz, nessa perspectiva, o ato ilícito como base fomentadora da responsabilidade civil: “aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito” (BRASIL, 2002).

Não obstante, é oportuno enfatizar, como aponta Stolze e Pamplona Filho “que nem sempre a conduta deverá ser revestida de antijuridicidade”. Nos casos previstos em lei, é possível ocorrer responsabilidade civil por tentativa de ato ilícito, em virtude de lei. Isto é, a ilicitude, não necessariamente, escoltará a conduta humana ensejadora de responsabilização (GAGLIANO; PAMPLONA FILHO, 2011, p. 80).

Outro requisito crucial para configuração da responsabilidade civil, é o dano, vez que não tem como debater sobre responsabilidade ou ressarcimento, sem que haja a ocorrência da lesão. Quando se refere a lesão, ao dano, pressupõe relação ao

patrimônio, porém Cavalieri Filho (2014, p. 103) adita que o conceito de dano carece de sua consequência:

> Correto conceituar o dano como sendo lesão a um bem ou interesse juridicamente tutelado, qualquer que seja a sua natureza, quer se trate de um bem patrimonial, quer se trate de um bem integrante da personalidade da vítima, como sua honra, a imagem, a liberdade etc. Em suma, dano é lesão de um bem jurídico, tanto patrimonial como moral, vindo daí a divisão em dano patrimonial e moral.

Portanto, como dito alhures, o dano pode ser classificado como material e moral. O primeiro fere diretamente os bens, gerando uma redução ao patrimônio da vítima, o segundo alcança a personalidade da vítima, como sua honra, imagem, liberdade, dentre outros.

O dano material está estreitamente atado à ideia de patrimônio, Diniz leciona que o compreende como “o conjunto de bens economicamente úteis e capazes de serem avaliados pecuniariamente”. Ressalta-se que os bens materiais são aqueles que dispõem de valor econômico, apesar disso não necessariamente sejam corpóreos, dado que os bens incorpóreos igualmente podem possuir valor econômico, como por exemplo o direito de crédito (DINIZ, 2013, p. 61).

Não se deve analisar o dano ao patrimônio apenas pela ótica hodierna, mas também sob a ótica iminente, dividindo-os em dois pontos. O dano emergente, refere-se ao efetivo detrimento recebido pelo fato danoso, isto é, o montante perdido, sendo avaliado com a simples dedução do valor atual do bem lesado, do valor que teria em seu estado originário. Em contrapartida, há os lucros cessantes, entendidos por Gagliano e Pamplona Filho como “aquilo que se deixou de ganhar por força do dano”. Desse modo, certifica-se que o dano material, é o prejuízo a direito de natureza patrimonial, é a redução do patrimônio com montante avaliável, resultante da ocorrência danosa, ao contrário do dano moral (GAGLIANO; PAMPLONA FILHO, 2011, p. 83).

O dano moral ou extrapatrimonial são outras modalidades experimentado pela vítima, que se estende aos bens personalíssimos da vítima, compondo-se segundo assenta Farias et. al. “na lesão de direito cujo conteúdo não é pecuniário, nem comercialmente redutível a dinheiro”. Complementando ainda admite-se afirmar que o dano moral “é aquele que lesiona a esfera personalíssima da pessoa (seus direitos

de personalidade), violando por exemplo, sua intimidade, vida privada, honra e imagem, bens jurídicos tutelados constitucionalmente" (FARIAS et. al., 2017, p. 97).

Assim, o dano moral é meramente a violação do direito à dignidade constatado o cenário total de dignidade aduzido pela Constituição Federal de 1988, na qual estabeleceu o cerne do ser humano, independente de nacionalidade, sexo, raça, cultura, cor, credo, idade e fortuna. Trata-se de direito intrínseco da pessoa humana, do nascimento à morte.

Destaque-se que, o dano moral não está, obrigatoriamente, condicionado a reações psíquicas da vítima. Sendo possível o dano à dignidade da pessoa humana sem sofrimento, vexame, dor, bem como é possível haver sofrimento, vexame e dor sem que haja a violação da dignidade, desse modo, o dano moral é aquele que gera abalo à dignidade da pessoa sem necessário abalo psicológico.

Apesar do dano moral ser reputado como de natureza não patrimonial, por vezes causa implicações na vida financeira da vítima. Isto posto, o dano moral é classificado pelos juristas em duas correntes: o dano moral direto e dano moral indireto. Quanto ao primeiro, Diniz (2013, p. 83) leciona que:

> Consiste na lesão a um interesse que visa a satisfação ou gozo de um bem jurídico extrapatrimonial contido nos direitos da personalidade (como a vida, a integridade corporal, a liberdade, a honra, o decoro, a intimidade, os sentimentos afetivos, a própria imagem) ou nos atributos da pessoa (como o nome, a capacidade, o estado de família).

A segunda corrente diz que o dano moral indireto se dá de forma subsidiária ao dano material. Havendo uma lesão inerente a um bem ou interesse de cunho patrimonial, refletindo perda no campo extrapatrimonial da vítima, conforme narra Gagliano e Pamplona Filho quando "houve furto de um bem de grande valor afetivo". O furto indica perda de patrimônio, mas se tratando de bem com alto valor afetivo, a sequela da perda de patrimônio ou do furto acarreta em dano de cunho psicológico e extrapatrimonial (GAGLIANO; PAMPLONA FILHO, 2011, p. 109).

A definição ou os preceitos sobre nexo causal ou nexo de causalidade, são o elo efetivo entre o comportamento do agente e o resultado deste comportamento, concerne na realidade um vínculo, uma relação entre o comportamento e seu resultado. A causa é toda ação ou omissão no qual o resultado não teria acontecido, todavia, se adotássemos apenas a causa como fruto do crime expor-se-á a uma regressão sem fim.

Venosa entende que o nexo causal “é o liame que une a conduta do agente ao dano, é por meio do exame da relação causal que concluímos quem foi o causador do dano, trata-se de elemento indispensável.” Na responsabilidade objetiva a culpa é dispensada, porém o nexo causal não será dispensado, não haverá ressarcimento à vítima do dano se ela não apontar o nexo causal que leva o ato lesivo ao responsável (VENOSA, 2007, p. 112).

Cavalieri Filho entende que o nexo causal tem um conceito não jurídico, decorrente das leis naturais, é a ligação, relação ou vínculo de causa e efeito entre a ação e o resultado. Há três teorias principais apontadas pela doutrina, elaboradas para elucidar o nexo causal ou nexo de causalidade: “a) teoria da equivalência das condições; b) teoria da causalidade adequada; c) teoria da causalidade direta ou imediata (interrupção do nexo causal)” (CAVALIERI FILHO, 2014, p. 71).

A primeira teoria, também denominada de *sine qua non* (sem o qual não pode ser), foi desenvolvida por Von Buri, um jurista alemão, na segunda metade do século XIX. Gagliano e Pamplona Filho destacam que “essa teoria não diferencia os antecedentes do resultado danoso, de forma que tudo aquilo que concorra para o evento será considerado causa.” Deste modo a equivalência de condições diz que todas as razões causais se equivalem caso haja nexo com o resultado. Qualquer eventualidade sucedida na formação do caso será vista como causa. Considerar-se-á causa todo antecedente que participar da rede de fatos que culminaram no dano (GAGLIANO; PAMPLONA FILHO, 2011, p. 133).

Gonçalves julga o princípio da equivalência das condições como fomentadora do dano o estado por si só propícia a produzi-la, calhando à certo dano, concluindo que o fato originador era apto a lhe dar causa, se este vínculo de causa e efeito se encontra sempre em feitos deste feitio, logo, sendo possível afirmar que a causa era própria a produzir o efeito (GONÇALVES, 2014, p. 24).

Na hipótese de existir por uma rigidez uma lesão com causa acidental é plausível afirmar que a causa não era oportuna. Em outras palavras, a causa oportuna consoante Gonçalves “deverá abstratamente, e segundo para apreciação probabilística, ser apta à efetivação do resultado” (GONÇALVES, 2014, p. 25).

A terceira teoria é a da interrupção do nexo causal, também chamada de causalidade direta e imediata ou de a teoria da causalidade necessária, no qual a causa é apenas uma preliminar fática ligada mediante um elo de necessidade ao resultado danoso, é um fruto direto e imediato, carece de uma conduta entre e o dano,

um liame de causa e resultado direta e imediata, deverá ser uma causa necessária, inexistindo outra que elucide o mesmo dano (GAGLIANO e PAMPLONA FILHO, 2011, p. 138).

Portanto, no direito, indubitavelmente, não se fala em responsabilidade civil sem haver nexo de causalidade entre a conduta e o dano gerado, contraindo resultado direto e imediato, implicando conduta entre dano e ressarcimento ou sanção.

3.4 RESPONSABILIDASDE DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Apesar de o dispositivo 5º, inc. II da LGPD trazer a definição de dados sensíveis, exemplificado por um rol não taxativo, vale ressaltar que o tratamento de dados que não estejam elencados na legislação como tal pode direcionar a efeitos práticos discriminatórios, cujas consequências a LGPD almeja afastar justamente ao reconhecer e proteger essa categoria de dados sensíveis. Ou seja, a categoria de dados sensíveis não pode ser considerada como estruturalmente diferente da categoria dos dados não sensíveis, ao passo em que ambas estão sujeitas à potencialidade de atos discriminatórios e ocasionadores de danos a seus titulares (BRASIL, 2018).

Nesse sentido, não deve existir diferença de regimes de responsabilidade civil fundamentada em uma classificação dos dados como sensíveis ou não. Isto é, o regime de responsabilidade civil aderido pela LGPD é único, independentemente da natureza do dado protegido, se sensível ou não, porque o efeito de sua violação (dano patrimonial ou moral, individual ou coletivo) independe dessa classificação, devendo ser reparado em sua totalidade.

Mediante as considerações expostas, percebe-se que o exame do conteúdo da LGPD não pode ignorar toda a evolução ocorrida na sistemática da responsabilidade civil, sendo esta um legado propiciado pelo Direito Privado, sobretudo das normas elencadas no Código Civil de 2002 e na legislação consumerista que, por sua elevada natureza principiológica e valorativa no sistema jurídico brasileiro, propiciaram a constante edificação e reconstrução da interpretação dos institutos de Direito Privado, funcionalizando-os para suprir os anseios empíricos de uma sociedade em frequente mutação, globalizada e de intensa complexidade,

garantindo-se a primazia ao caráter ético que deve refletir a conduta humana e todas as relações sociais (COSTA NETO, 2018, p. 62).

De acordo com a análise dos dispositivos 42 a 45 da LGPD, se elevam duas vertentes interpretativas sobre a natureza da responsabilidade civil dos agentes de tratamento de dados pessoais, para parcela da doutrina, a responsabilidade civil envolvendo tais agentes seria considerada subjetiva, ao passo que a posição contrária compreende que a LGPD teria se aderido ao sistema do risco sendo, dessa forma, objetiva (BRASIL, 2018).

Tais vertentes se originam do fato da aparente imprecisão da Lei no tocante à responsabilização civil. Divergência esboçada na doutrina elucidada entre autores que sustentam ter a LGPD determinado um sistema fundado na responsabilidade objetiva ou subjetiva, sendo ambas as posições respeitáveis, segundo Tasso (2020, p. 104).

As duas vertentes de tem um pressuposto comum, que é a fundamentação de que a Lei de Dados possui grande imprecisão terminológica, uma vez que o enunciado do artigo 42 não teria sido considerado nítido o bastante no tocante ao regime de responsabilidade civil (subjetiva ou objetiva) aderido pela LGPD (BRASIL, 2018).

No que diz respeito à sustentação que o tratamento de dados pessoais seria completamente inofensivo e não denotaria quaisquer riscos aos sujeitos envolvidos, principal fundamento em favor da responsabilidade subjetiva, o texto do dispositivo 42 da LGPD não viabiliza tal conclusão. Por mais zelo e atenção que se tenha o agente, nenhum trabalho humano é isento de riscos, devendo a ciências jurídicas determinar regras que viabilizam sua alocação adequada. Assim, Stajn (2011, p. 118) aduz que “se os riscos são probabilidades de perdas ou ganhos, quanto a estas, é necessário modelar mecanismos que propiciem sua transferência ou mitigação.”

Mediante esse contexto inafastável, o Direito atualmente tem regulado a responsabilização civil no sentido de suprimir o chamado “custo social da não-reparação” de danos ocasionados de maneira injusta, que se compreende em um fenômeno capaz de deteriorar a segurança jurídica, além de ser foco de injustiça que as mais variadas teorias jurídicas aferidas ao Direito Privado, como a análise econômica do direito e a constitucionalização do Direito Civil, não suportam e toleram (SCHREIBER, 2009, p. 221).

Dessa forma, a redação que afere “em razão do exercício de atividade de tratamento de dados pessoais” englobada no dispositivo 42 da LGPD não pode ser restrita de sentido, como assentam os doutrinadores que defendem a teoria subjetiva no cerne da Lei de Dados. Assim, o mencionado artigo reconhece, em seu texto e ainda que de modo implícito, que a atividade de tratamento de dados pessoais engloba riscos possíveis (BRASIL, 2018).

Sendo a legislação civil de 2002 o âmago irradiador dos princípios e normas de Direito Privado, a interpretação do dispositivo 42 da Lei de Dados deve ser efetuada de modo coeso e sistemático ao elencado no artigo 927, § único, do CC/2002, que aderiu a teoria da responsabilidade objetiva baseada no risco da atividade realizada pelo agente da função potencialmente lesiva, suprimindo a hipótese de socialização do dano na qual a vítima era obrigada a suportar o mesmo em virtude da complexidade de se atestar a culpa (BRASIL, 2002).

Nesse sentido, não seria factível que a LGPD tivesse elaborado um sistema de proteção de dados se, na materialização de tal sistema, este fosse debilitado ou praticamente inútil, ocasionando uma conjuntura de extensão do estado de lesão a um direito de personalidade. Sinaliza-se que o artigo 43 do mesmo diploma ressalta que a responsabilidade civil disposta na norma teria natureza subjetiva por englobar a necessidade de demonstração de culpa do agente de tratamento de dados pessoais, o que não se demonstra verídico, pois as situações expostas nos incisos I a III do referido artigo não comportam qualquer conexão com a exigência de culpa, mas se relacionam a situações de ruptura do nexo de causalidade (BARRETO et. al., 2018, p. 522).

O artigo 44 da LGPD, por seu turno, denota modelos comportamentais ao agente de tratamento de dados pessoais, isto é, determina deveres relativos aos resultados e não à mera diligência, cujo seu descumprimento demanda, por si só, a responsabilidade civil do indivíduo que causou o dano, independentemente de alcançada a constatação da culpa. Um empecilho frequentemente observado pelos defensores da responsabilidade civil subjetiva no plano da LGPD se emana no fato de que a aderência da teoria do risco da atividade poderia inibir a competição e a desenvoltura de novos meios tecnológicos. (BRASIL, 2018)

Desse modo, a doutrina de Moraes (2019, p. 14) explana que:

> Cuida-se, todavia, de falsa afirmação, pois a história já demonstrou que a aderência dos modelos de culpa presumida ou de responsabilidade objetiva, que flexibilizaram a dificuldade da prova da culpa, não restringiriam o desenvolvimento de novas tecnologias. Contrariamente, garantiu-se o completo desenvolvimento tecnológico e industrial e os dispêndios dos moldes de responsabilização objetivos, sobretudo nas relações consumeristas, foram integrados pelo mercado sem prejuízo do ressarcimento das vítimas de danos injustos, instaurando-se o modelo solidário de responsabilidade fundado na atenção e no cuidado para com o lesado. Assim, o fundamento de possível aumento dos custos de proteção dos dados pessoais para as organizações não se demonstra decisivo, tendo em vista que não se pode considerar que interesses conexos à proteção de dados pessoais dos titulares sejam de importância menor que os interesses empresariais.

Assim, Moraes define o modelo de responsabilidade civil adotado pela LGPD, em sentido amplo, como “proativo”, fundado em um sistema de prestação de contas, no qual a essência axiológica do instituto transpassaria da reparação do dano para sua prevenção efetiva (MORAES, 2019, p. 16).

Refere-se à definição de “prestação de contas", essa nova conjuntura de responsabilidade denominada “proativa”, com fulcro no inc. X, do art. 6º, da LGPD, que estabelece às organizações não ser o bastante cumprir os dispositivos da Lei, será ainda dispensável demonstrar a aderência de medidas efetivas e hábeis de atestar a observância e o cumprimento das normas de proteção de dados pessoais e, sobretudo, a eficácia de tais medidas. Assim, não descumprir a norma não é mais o suficiente, sendo também necessária a prevenção proativa para afastar a realização de danos (MORAES, 2019, p. 15).

A análise realizada pela autora advém da natureza multidisciplinar que a responsabilidade civil tem investido nas últimas décadas, no qual sua seara de atuação deixa de ser somente reparatória (isto é, estritamente jurídica) e passa a refletir incidências prévias (preventivas), edificando-se instrumentos para afastar a ocorrência do dano, denominada de responsabilidade preventiva (LOPEZ, 2010, p. 1231).

Contrabalanceando tais acepções, parece ser uma incoerência a legislação dispor sobre instrumentos de responsabilidade preventiva, tendentes a afastar a ocorrência do dano e, concomitantemente, subordinar da reparação de danos

oriundos de lesão a dados pessoais, sendo este um direito fundamental, ao regime da responsabilidade subjetiva, com todos os óbices a este intrínsecos.

Seria divergente, também, que a LGPD viabilizasse que a responsabilidade civil advinda de um mesmo fato objetivamente considerado (violação de regras de proteção de dados pessoais) pudesse possuir tratamento distinto de acordo com a natureza do agente envolvido, ou seja, subjetiva para os agentes de Direito Privado; e objetiva para entes de Direito Público, uma vez que, não tendo disposto regulação explícita à responsabilidade civil destes últimos, a respectiva responsabilização inevitavelmente verificará a teoria do risco administrativo (art. 37, § 6º, CF/88), assim, esta será objetiva para os atos comissivos e subjetiva para os omissivos (BRASIL, 1988).

Diversamente, ao não tratar com adequada especificidade o instituto da responsabilidade civil dos entes públicos quando da observância de danos oriundos do tratamento de dados pessoais, a LGPD deixou ao intérprete o encargo de proceder à integração do sistema protetivo. Desta feita, não restam questionamentos que, nessa situação, a responsabilização civil do ente público ocorre com embasamento na teoria do risco administrativo.

Nessa perspectiva, de acordo com o entendimento do Supremo Tribunal Federal, a responsabilidade do Estado no plano das tarefas que envolvem o tratamento de dados pessoais é observada em consonância aos critérios da responsabilidade objetiva para os atos omissivos, sendo estes refletidos no tratamento e compartilhamento inadequado de dados e, sob outro panorama, de acordo com os pressupostos da responsabilidade subjetiva quando se tratar de atos comissivos, como, por exemplo, a inobservância das regras de prevenção e de segurança da informação a propiciar o vazamento inadequado de dados pessoais do titular (TASSO, 2020, p. 104).

Assim, verifica-se que a referida duplicidade da sistemática da responsabilidade civil aderida pela LGPD, que o presente trabalho almejou demonstrar não existir, não pode servir de base para a aderência da teoria da culpa, que obstaculiza o acesso da vítima à justiça, além de também distanciar a reparação do dano, tendo em vista que, sendo os dados pessoais um direito fundamental, o dispositivo 29 da Convenção Interamericana de Direitos Humanos demanda que a interpretação das normas jurídicas que envolvem direitos humanos leve em consideração a regra mais benéfica à pessoa humana, elemento que é

frequentemente inobservado pelos defensores da teoria subjetiva no cerne da responsabilidade civil adotada pela LGPD (TASSO, 2020, p. 106).

No que tange às hipóteses de exclusão da responsabilização civil na LGPD, estas estão dispostas no art. 43. O primeiro inciso trata da hipótese em que o agente não efetuou o tratamento de dados que lhe foi aferido. Isto é, existiu um tratamento de dados, mas o indivíduo não possui qualquer ligação com este. Assemelha-se muito à questão da ilegitimidade passiva, que a Lei de Dados trata como matéria de mérito (BRASIL, 2018).

Por sua vez, o segundo inciso suprime a responsabilidade na hipótese em que o agente efetuou o tratamento, mas não existiu violação à legislação de proteção de dados. Na supracitada situação, o dano se realizou por ato lícito. A título de exemplo, seria a situação de uma decisão automatizada, fundada em pressupostos transparentes, informados (dispostos em termos de utilização) e sem viés, que indefira empréstimo a determinado consumidor (BRASIL, 2018).

O referido inciso dispõe de maneira expressa somente a hipótese em que não existiu violação à proteção de dados. Deve-se alcançar a interpretação do referido artigo em concomitância aos arts. 42, 44, 46 e parágrafo único, de acordo com os motivos já apresentados, de forma a permitir, também a alegação de falta de violação e norma técnica. Por último, o inciso III dispõe sobre a alegação de culpa exclusiva do titular ou de outrem, que serão as situações em que o dano for ocasionado por completa ingerência do titular, por terceiro ou ainda por um exercício conjunto do titular com o terceiro (BRASIL, 2018).

Demanda-se, assim, uma responsabilidade ainda maior por parte dos indivíduos responsáveis pelo tratamento de dados e um aditamento nas fiscalizações por parte da ANPD, não ignorando que a segurança não depende estritamente do ente governamental ou equipe de tecnologia de certa empresa. Portanto, a segurança das informações deve operar como um núcleo, um sistema vivo, no qual cada fase, desde a coleta até o tratamento dos dados, detenha uma fluência rigorosa e que esteja em contínua fiscalização e melhoramento.

CONCLUSÃO

Com a realização do presente estudo, foi possível verificar que incidentes de segurança, sobretudo no que tange o vazamento de dados pessoais sensíveis, é nociva para os titulares atingidos, que poderão ser atingidos por fraudes ou incursões de terceiros à sua privacidade, às organizações, que podem estar perdendo um importante ativo de seu negócio e a sociedade como um todo, que possui interesse no equilíbrio e na pacificação social, fatores que integram um plano fértil para a conjugação apropriada de direitos, tais como a tutela da privacidade, da livre iniciativa e do empreendedorismo.

O estudo verificou ainda que Lei nº 13.709/2018, LGPD, é um mecanismo legal essencial não somente para elencar direitos aos titulares, como também é indispensável à estruturação da ANPD, que desenvolve papel de suma relevância, incluindo o exercício nos incidentes que envolvem o vazamento de dados pessoais sensíveis. No entanto, a sociedade atualmente se encontra em um momento de transição, de uma conjuntura que era sem regulamentação para um cenário regulado e, mesmo que os óbices não estejam sendo ultrapassados com a velocidade almejada, a médio prazo, a tendência é que a LGPD seja ainda mais efetiva, à medida que as sanções administrativas passaram a ser aplicadas em 2021.

Os debates acerca das balizas de utilização de algoritmos estão distantes de encontrar uma solução simples e única que transpasse todos os dilemas enfrentados com a sua inserção cada vez mais intensa nos mais diversos âmbitos. Tendo em vista a potencialidade de que a utilização de algoritmos robusteça atos discriminatórios, a questão é se o sistema jurídico nacional e, em específico, a LGPD está apta para regular e combater comportamentos discriminatórios que propiciam ilegalidades, restrições de direitos e abusos.

Nessa toada, observou-se que a regulação do tratamento de dados na supracitada Lei, com a sua proibição expressa à discriminação abusiva e ilícita e os princípios gerais norteadores, apresenta-se como uma pequena evolução, que, todavia, certamente necessitará de desenvolturas dogmáticas para que possa ser adequadamente aferida e entendida. Nota-se, também, que a regulação das decisões automatizadas começada pela LGPD, ao intencionar aumentar a transparência e assegurar informações ao titular sobre os critérios usados pelo algoritmo, como

estabelecido em seu art. 20, complementa de maneira importante o princípio da não discriminação.

A LGPD, como demonstrado, além de detalhar as figuras do controlador e do operador, com suas respectivas tarefas. Restando nítido que, ao realizar a atividade de tratamento de dados, o agente de tratamento competente deve respeitar todos os princípios dispostos na Lei específica. Verificou-se, também, que o controlador consiste na principal figura responsável no conjunto da atividade de tratamento de dados, tendo em vista que é dele a tomada de decisão sobre o objetivo dos dados pessoais, vindo o operador a executar somente as ordens recebidas pelo controlador, respondendo somente se violadas ou se atuar em divergência com a legislação.

Portanto, o trabalho verificou que a responsabilidade civil no cerne das atividades que englobam o tratamento de dados pessoais sensíveis é verificada em conformidade aos critérios do regime objetivo para atos omissivos, sendo os mesmos refletidos no tratamento e compartilhamento inadequado de dados pessoais e, sob outro enfoque, em consonância às premissas da responsabilidade civil subjetiva, está se aplicará no cerne da LGPD quando se tratar de atos comissivos, à exemplo da não observância às normas de prevenção e segurança da informação, que podem ocasionar o vazamento inoportuno de dados pessoais do titular.

REFERÊNCIAS

BARRETO JUNIOR, Irineu Francisco; WANDERLEY, Ana Elizabeth Lapa; LEITE, Beatriz Salles Ferreira. **Sistemas de responsabilidade civil dos provedores de aplicações da internet por ato de terceiros**: Brasil, União Europeia e Estados Unidos da América. Revista Eletrônica do Curso de Direito da UFSM, v. 13, n. 2, Santa Maria, ago. 2018.

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

BORGES, Ricardo Capucio. **O fomento à cultura digital e a promoção da internet segundo o marco civil**. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). Marco civil da internet. São Paulo: Atlas, 2014.

BRASIL, Supremo Tribunal Federal. **ADI 6387**. Rel. Min. Rosa Weber, Decisão Monocrática, j. 24.04.2020, DJe 28.04.2020.

BRASIL. 5 ª Promotoria de Justiça de Tutela Coletiva de Defesa do Consumidor e do Contribuinte da Capital. **Ação civil pública com pedido de liminar em face da Decolar.com.** Autor: Ministério Público do Estado do Rio de Janeiro. Réu: Décolar.com. Rio de Janeiro, 25 de janeiro de 2018.

BRASIL. **Código de Defesa do Consumidor**. Lei n. 8.078/90, de 11 de setembro de 1990.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 12 abr. 2022.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm> Acesso em: 13 mai. 2022.

BRASIL. **Lei do Habeas Data**. Lei n. 9.507, de 12 de novembro de 1997. Disponível em: <https://www2.camara.leg.br/> Acesso em: 01 mai. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm> Acesso em: 08 jul. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 03 mai. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 05 mai. 2022.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm> Acesso em: 28 jun. 2022.

BRASIL. **Medida Provisória nº 1.124, de 13 de junho de 2022**. Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Mpv/mpv1124.htm> Acesso em: 15 jul. 2022.

CANCELIER, Mikhail Vieira de Lorenzi. **Infinito particular**: Privacidade no século XXI e a manutenção do direito de estar só. Florianópolis, 2016.

CARDOSO, Oscar Valente. **Lei Geral de Proteção de Dados e Diálogo das Fontes 3**: Código Civil. 2020. Disponível em: <https://jus.com.br/artigos/84569/lei-geral-de-protecao-de-dados-e-dialogo-das-fontes-3-codigo-civil> Acesso em: 27 jun. 2022.

CASTRO, Catarina Sarmento e. **Direito da informática**, privacidade e dados pessoais. Coimbra: Almedina, 2005.

CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil**. 11ª. Edição Revista e Ampliada, São Paulo: Editora Atlas SA, 2014.

COSTA NETO, Moacyr da. **A autonomia privada e a prevalência do negociado**. Revista Univap, v. 24, n. 45, Edição especial, São José dos Campos, 2018.

COTS, Márcio. **Promover a inovação e fomentar a ampla difusão de novas tecnologias e modelos de uso e acesso como objetivos da regulamentação do uso da internet no Brasil**. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). Marco civil da internet. São Paulo: Atlas, 2014.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2ª ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: 7. Responsabilidade Civil. 27. ed. São Paulo: Saraiva, 2013.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; NETTO, Felipe Peixoto Braga. Curso de Direito Civil: **Responsabilidade Civil**. 4. ed. rev. atual. e ampl. Salvador: Juspodivm, 2017.

FRAZÃO, Ana. **Plataformas digitais e os desafios para a regulação jurídica**. v.1. Belo Horizonte: Editora D'Plácido, 2018.

GAGLIANO, Pablo Stolze. PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil**. Responsabilidade Civil. São Paulo: Saraiva, 2011.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro** 4: Responsabilidade Civil. 9. ed. São Paulo: Saraiva, 2014.

HOSKEN, Maria. **Agentes de tratamento de dados na LGPD**. Disponível em: < http://www.anspnet.org.br/wp-content/uploads/2018/11/maria_hosken.pdf>. Acesso em: 27 jun. 2022.

LACOMBE, Francisco José Masset et al. **Administração**: princípios e tendências. São Paulo: Saraiva, 2003.

LOPEZ, Tereza Ancona. **Responsabilidade civil na sociedade do risco**. Revista da Faculdade de Direito da Universidade de São Paulo, v. 105, São Paulo, 2010.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018.

MARTINS, Guilherme Magalhães. **Direito Privado e Internet**. São Paulo: Atlas, 2014.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MIGUEL, Fernando Gomes. **Os desafios do Brasil na nova era da proteção de dados pessoais e da privacidade**. 2019. Disponível em: <https://www.migalhas.com.br/depeso/298736/os-desafios-do-brasil-na-nova-era-daprotecao-de-dados-pessoais-e-da-privacidade>. Acesso em: 09 jul. 2022.

MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor.** Revista dos Tribunais, São Paulo, v. 1009, 2019.

MORAES, Maria Celina Bodin de. **LGPD**: um novo regime de responsabilização civil dito —proativo. Revista Civilistica, ano 8, n. 3, Rio de Janeiro, 2019.

MOTA PINTO, Paulo da. **Direito ao livre desenvolvimento da personalidade**. In: RIBEIRO, Antônio de Pádua et al. Portugal-Brasil Ano 2000. Coimbra: Coimbra editora, 2000.

NORONHA, Fernando. **O direito dos contratos e seus princípios fundamentais (autonomia privada, boa-fé e justiça contratual)**. São Paulo: Saraiva, 1994.

OLIVEIRA, Ricardo Alexandre de. **Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico**. São Paulo: Revista dos Tribunais, dezembro 2018.

PEREIRA, Luiz Fernando. **A Lei Geral de Proteção de Dados Pessoais:** uma teoria finalística. Revista Jus Navigandi, set. 2018. Disponível em:

<https://jus.com.br/artigos/68967/a-lei-geral-de-protecao-de-dados-pessoais-uma-teoria-finalistica>. Acesso em: 25 jun. 2022.

POLIDO, Fabrício Bertini Pasquot; et al. **GDPR e suas repercussões no direito brasileiro**: Primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade, 2018.

PSCHEIDT, Kristian Rodrigo. **ANPD, de órgão para agência: mudança é muito maior do que parece. 2022**. Disponível em: <https://www.conjur.com.br/2022-jul-13/kristian-pscheidt-mudanca-anpd-maior-parece#:~:text=No%20entanto%2C%20no%20%C3%BAltimo%20dia,e%20foro%20no%20Distrito%20Federal. > Acesso em: 18 jul. 2022.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. **A Proteção de Dados Pessoais na Internet no Brasil:** Análise de decisões proferidas pelo Supremo tribunal Federal. In: Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS. 2016.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSENVALD, Nelson. **As funções da responsabilidade civil a reparação e a pena civil**. Saraiva Educação SA, 2017.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros à diluição dos danos. 2.ed. São Paulo: Atlas, 2009.

SILVA, Joseane Suzart Lopes da. **A proteção de dados pessoais dos consumidores e a Lei 13.709/2018**: em busca da efetividade dos direitos a privacidade, intimidade e autodeterminação. Revista de Direito do Consumidor, vol. 121, ano 28. São Paulo: Ed. RT, 2019.

SOMADOSSI, Henrique. **O que muda com a Lei Geral de Proteção de Dados (LGPD)**. 2018. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI286235,31047-O+que+muda+com+a+Lei+Geral+de+Protecao+de+Dados+LGPD>. Acesso em: 26 jun. 2022.

SOPRANA, Paula; CORONATO, Marcos. **Quanto valem seus dados pessoais?** Época. Disponível em: <http://epoca.globo.com/tecnologia/experiencias-digitais/noticia/2017/07/quanto-valem-seus-dados-pessoais.html>. Acesso em: 13 mai. 2022.

SOUZA, Maria Luciana Pereira de. **Proteção de dados pessoais na internet**: a mais recente instrumentalização do princípio da dignidade humana na sociedade da informação. Rio de Janeiro: Vozes, 2018.

STAJN, Rachel. **Sistema financeiro.** Rio de Janeiro: Elsevier, 2011.

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: Direito Digital e proteção de dados pessoais, São Paulo, ano 21, n. 53, São Paulo, 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, maio 2016. Disponível em: <https://bit.ly/2RC45KC>. Acesso em: 13 mai. 2022.

VENOSA, Sílvio de Salvo. **Direito civil**: responsabilidade civil. 7. ed. Vol. 4. São Paulo: Atlas, 2007.