



Centro Universitário de Brasília - UniCEUB  
Faculdade de Ciências Jurídicas e Sociais - FAJS  
Curso de Bacharelado em Direito / Relações Internacionais

**THIAGO TOMICH NETTO GUTERRES SOARES**

**LGPD: O regime jurídico da responsabilidade civil dos agentes de tratamento  
de dados pessoais**

**BRASÍLIA  
2021**

**THIAGO TOMICH NETTO GUTERRES SOARES**

**LGPD: O regime jurídico da responsabilidade civil dos agentes de tratamento  
de dados pessoais**

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito, pela Faculdade de Ciências Jurídicas e Sociais - FAJS, do Centro Universitário de Brasília (UnICEUB).

Orientador: Paulo Rená da Silva Santarém.

**BRASÍLIA**

**2021**

**THIAGO TOMICH NETTO GUTERRES SOARES**

**LGPD: O regime jurídico da responsabilidade civil dos agentes de tratamento  
de dados pessoais**

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito, pela Faculdade de Ciências Jurídicas e Sociais - FAJS, do Centro Universitário de Brasília (UniCEUB).

Orientador: Paulo Rená da Silva Santarém.

**BRASÍLIA, 12 DE ABRIL DE 2021**

**BANCA AVALIADORA**

---

**Paulo Rená da Silva Santarém**  
**Professor Orientador**

---

**Professor(a) Avaliador(a)**

## **LGPD: O regime jurídico da responsabilidade civil dos agentes de tratamento de dados pessoais**

THIAGO TOMICH NETTO GUTERRES SOARES<sup>1</sup>

### **RESUMO**

O presente trabalho analisa o regime de responsabilização civil dos agentes de tratamento de dados pessoais, previsto nos artigos 42 e 44 da Lei Geral de Proteção de Dados Pessoais (LGPD). A metodologia do estudo consiste inicialmente em apresentar a proteção de dados pessoais e seus desdobramentos sociais no cenário internacional e nacional. Posterior a isto, a pesquisa se debruça sobre uma investigação doutrinária e legal acerca do regime de responsabilidade civil inaugurado com a nova legislação, além de buscar nas jurisprudências do Supremo Tribunal Federal e Superior Tribunal de Justiça julgados que auxiliassem na compreensão da questão. Frente a isto, foi constatado que entre os doutrinadores brasileiros há uma divisão no tange o regime adequado, coexistindo defensores do regime subjetivo e objetivo, já em âmbito jurisprudencial, verificou-se que no STJ já há julgados como o do Recurso Especial 1.457.199/RS, o qual possui entendimento apto a auxiliar a questão da responsabilização civil dos agentes de tratamento. Chegando-se a conclusão que pelo contexto jurídico e social observado, a responsabilidade civil objetiva favoreceria o titular dos dados, mas não foi o regime positivado no texto da LGPD.

**Palavras-chave:** Responsabilidade Civil. Dados Pessoais. Lei Geral de Proteção de Dados Pessoais. Agentes de Tratamento. Regime de Responsabilidade Subjetiva , Regime Responsabilidade Objetiva.

---

<sup>1</sup> Estudante do curso de Direito no UniCEUB.

## LISTA DE SIGLAS E ABREVIATURAS

ADI	Ações Diretas de Inconstitucionalidade
ADPF	Arguição de Descumprimento de Preceito Fundamental
Art.	Artigo
CC	Código Civil
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CPE	Comissão Parlamentar Especial
CPF	Cadastro de Pessoas Físicas
DUDH	Declaração Universal dos Direitos Humanos
GDPR	Regulamento Geral sobre a Proteção de Dados
IBGE	Instituto Brasileiro de Geografia e Estatística
IDEC	Instituto Brasileiro de Defesa do Consumidor
ISO	Organização Internacional de Normalização
LGPD	Lei Geral de Proteção de Dados Pessoais
MC	Medida Cautelar
OCDE	Organização para Cooperação e Desenvolvimento Econômico
PL	Projeto de Lei
REsp	Recurso Especial
RG	Registro Geral
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
UE	União Europeia

## SUMÁRIO

<b>1 INTRODUÇÃO</b>	<b>6</b>
<b>2 PROTEÇÃO DE DADOS PESSOAIS</b>	<b>7</b>
<b>2.1 Conceito de Proteção de Dados Pessoais</b>	<b>9</b>
<b>2.2 Contextualização do Cenário Global em Proteção de Dados</b>	<b>10</b>
<i>2.2.1 Contextualização do cenário nacional em proteção de dados</i>	<i>12</i>
<b>2.3 Lei Geral de proteção de Dados - LGPD</b>	<b>13</b>
<i>2.3.1 Definição</i>	<i>13</i>
<i>2.3.2 Fundamentos</i>	<i>14</i>
<i>2.3.3 Princípios</i>	<i>15</i>
<b>2.4 Agentes de Tratamento de Dados</b>	<b>18</b>
<i>2.4.1 Controlador</i>	<i>19</i>
<i>2.4.2 Operador</i>	<i>19</i>
<i>2.4.3 Encarregado / Data Protect Office</i>	<i>20</i>
<b>3 REGIME DE RESPONSABILIDADE DOS AGENTES DE TRATAMENTO</b>	<b>21</b>
<b>3.1 Conceito de Responsabilidade Civil</b>	<b>21</b>
<b>3.2 Pressupostos</b>	<b>21</b>
<i>3.2.1 Conduta ilícita</i>	<i>21</i>
<i>3.2.2 Nexo de Causalidade</i>	<i>22</i>
<i>3.2.3 Dano</i>	<i>22</i>
<b>3.3 Classificações</b>	<b>23</b>
<i>3.3.1 Obrigação: Solidária - subsidiária</i>	<i>23</i>
<i>3.3.2 Vínculo jurídico: extracontratual - contratual</i>	<i>24</i>
<i>3.3.3 Voluntariedade: objetiva - subjetiva</i>	<i>24</i>
<b>3.4 Pressupostos da Responsabilidade Civil em Proteção de Dados</b>	<b>26</b>
<i>3.4.1 Da Conduta Ilícita</i>	<i>27</i>
<i>3.4.2 Do Nexo de Causalidade</i>	<i>28</i>
<i>3.4.3 Do Dano</i>	<i>29</i>

<b>3.5 Doutrina Sobre o Regime de Responsabilidade Civil dos Agentes de Tratamento</b>	<b>30</b>
<i>3.5.1 Regime de Responsabilidade Civil Subjetiva dos Agentes de Tratamento</i>	<b>32</b>
<i>3.5.2 Regime de Responsabilidade Civil Objetiva dos Agentes de Tratamento</i>	<b>36</b>
<i>3.5.3 Um Sistema Especial de Responsabilidade Civil Objetiva Proativa em Segurança Baseado na RGD</i>	<b>40</b>
<b>3.6 Julgados Relacionados a Proteção de Dados</b>	<b>42</b>
<i>3.6.1 Julgados do Supremo Tribunal Federal</i>	<b>42</b>
<i>3.6.2 Julgados do Superior Tribunal de Justiça</i>	<b>43</b>
<b>4 CONSIDERAÇÕES FINAIS</b>	<b>46</b>
<b>5 REFERÊNCIAS BIBLIOGRÁFICAS</b>	<b>49</b>

## 1 INTRODUÇÃO

O presente trabalho tem por objetivo principal realizar uma análise legal, doutrinária e jurisprudencial no que se refere à questão da culpa na responsabilização civil dos agentes de tratamento de dados, os quais foram inseridos recentemente no ordenamento jurídico pátrio com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD).

Frente ao exposto, destaca-se a seguinte problemática: o legislador pátrio foi expresso ao fixar o regime de responsabilização dos agentes de tratamento de dados pessoais, no capítulo VI da LGPD? Qual a avaliação por parte da doutrina e quais os posicionamentos encontrados no âmbito jurisprudencial.

Para enfrentar essas questões, o trabalho será dividido em 2 capítulos. O primeiro, apresentará a proteção de dados pessoais. Discorrerá sobre os desdobramentos sociais relacionados ao objeto, a conceituação do que se entende por proteção de dados e sua contextualização nos cenários internacional e nacional. Em seguida abordará especificamente a LGPD. Organiza-se em quatro tópicos (i) a definição da norma; (ii) os fundamentos escolhidos pelo legislador para alicerçar a norma; (iii) os princípios que fornecem o suporte teórico na interpretação e execução da atividade de tratamento de dados; (iv) a apresentação e classificação legal dos agentes de tratamento de dados pessoais, e o regime de responsabilização destes.

No segundo capítulo, o trabalho tratará da responsabilidade civil no ordenamento jurídico pátrio. Indica seus três pressupostos e suas diversas classificações, destacando as características essenciais à compreensão da matéria quanto à proteção de dados pessoais. Então, serão analisados pressupostos de responsabilidade civil aplicado em proteção de dados, bem como o posicionamento da doutrina em relação à exigência de culpa nos casos de responsabilização dos agentes de tratamento por dano causado ao titular dos dados, além da jurisprudência do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ) relacionados.



O intuito é fazer uma análise sobre qual seria o regime de responsabilidade civil condizente com a LGPD, tendo em vista a conformação ideal e a realizada expressa no texto da legislação.

## 2 PROTEÇÃO DE DADOS PESSOAIS

Atualmente, vive-se na Sociedade da Informação<sup>2</sup>, na qual a proteção de dados pessoais, apresenta-se como um delicado desafio a ser enfrentado pelo direito contemporâneo. Se de um lado da moeda tem-se uma excessiva velocidade dos avanços tecnológicos relacionados a esse novo ativo econômico, do outro, encontra-se o demorado processo legislativo intrínseco à produção de normas jurídicas. No ordenamento jurídico brasileiro, a proteção de dados pessoais já possui base normativa desde a Constituição Federal de 1988 (CF/88), que preconiza a inviolabilidade da intimidade e vida privada, autodeterminação informacional e livre desenvolvimento da personalidade (BRASIL, 1988).

Frente à previsão constitucional, somado ainda aos escândalos da Cambridge Analytics, Facebook e Uber, gerou-se uma reivindicação da sociedade por uma regulação no setor, tendo o Congresso Nacional elaborado em 14 de agosto de 2018 a lei nº 13.709/18, conhecida como “Lei Geral de Proteção de Dados Pessoais”, que entrará em vigência a partir de 1 de agosto de 2021 (BRASIL, 2018a). Dito isto, pense no seguinte exemplo do professores Cots e Oliveira (2019, p. 1818), para melhor imersão no tema apresentado:

Para entendermos melhor, basta imaginar uma sala de aulas com 40 alunos. Imagine que colocássemos uma venda na professora e fornecêssemos diversas informações até que a mesma adivinhe de qual aluno está-se falando. A primeira informação poderia ser que o aluno oculto é um menino, o que poderia eliminar metade das possibilidades. A próxima informação é que o aluno tem pele negra. Mais uma leva de alunos são eliminados da possibilidade. Assim, informação após informação, vai se afunilando as possibilidades até

---

<sup>2</sup> “Essa nova forma de organização social foi sedimentada em razão da evolução tecnológica recente, que criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imaginável. Os relacionamentos sociais foram energizados por um fluxo informacional que não encontram mais obstáculos físicos distanciais. Há uma nova compreensão (mais abreviada) da relação entre tempo-espço, o que outrora acarretava maior cadência às interações sociais”. (BIONI, 2019, p. 3).

que a professora identifique precisamente seu aluno. Verifique-se que o aluno não estava identificado, mas era identificável mediante a conjugação das informações que se tinha daquela sala de aulas.

Na mencionada lei, observa-se que o critério adotado na definição de dado pessoal foi o de caráter expansionista<sup>3</sup>, e, por força disso, não define apenas como dados pessoais as informações que imediatamente identificam um indivíduo, como nome, Cadastro de Pessoas Físicas (CPF), Registro Geral (RG), imagem, entre outros. O fato é que o legislador também escolheu proteger dados que tornem uma pessoa identificável de forma não imediata e direta; logo, informações que mesmo não possuindo feição de dados pessoais, mas que possuem a capacidade de identificação da pessoa natural, requerem a devida proteção legal.

Neste capítulo inicial, o presente trabalho se propõe em apresentar o tema de forma sintética, indicando os principais pontos sobre o fenômeno social de proteção, proteção de dados no mundo e seus reflexos na legislação brasileira, juntamente com os pontos relevantes sobre as questões tocantes à responsabilização civil na jurisdição brasileira.

## 2.1 Conceito de Proteção de Dados Pessoais

Inicialmente, ao falar de proteção de dados, faz-se necessário previamente compreender a distinção conceitual dos três elementos intrínsecos ao objeto estudado, sendo eles: o dado, a informação e o conhecimento, pois apesar de serem entendidos como similares, em termos de conceituação técnica, será demonstrado que são sensivelmente opostos. Nesta senda, o dado é o elemento primitivo (DONEDA, 2006, p. 152) dos três mencionados, já que em seu estado original não acresce ao conhecimento ou gera informação, sendo o mesmo simplesmente um fato bruto que necessita de alguma forma de tratamento, processamento e organização, para que possa se extrair desta fonte algo inteligível

---

<sup>3</sup> Segundo Bioni (2019, p. 59), via de regra, “prevalece o conceito *expansionista* pelo qual dado pessoal equivale a uma informação que, direta ou indiretamente, identifica um sujeito. Essa definição abraça, portanto, mesmo as informações que têm o potencial de identificar alguém, ainda que de maneira remota”.

e, por conseguinte, obter informações sobre o assunto desejado (BIONI, 2019, p. 31).

Já o segundo elemento é mais complexo, pois os mesmos dados podem gerar inúmeros tipos de informações, a depender do interesse do agente que realiza o tratamento; logo o elemento “informação” constitui-se pela organização dos dados em busca de esclarecimentos sobre a questão em análise. Em termos práticos, pense no seguinte exemplo: uma determinada empresa, na posse dos dados acerca dos hábitos de consumo dos seus clientes, realiza o tratamento de tais dados, e com isso empreende de forma mais eficiente no mercado, pois possui a informação sobre quais produtos têm melhor aceitação por sua clientela, e, assim, aumentando a possibilidade de êxito da atividade empresarial, já que na posse de tais informações podem melhorar a concepção e segmentação do produto/serviço, além de tornar a publicidade do item oferecido mais eficiente (BIONI, 2019, p. 31).

Por fim, tem-se o elemento do conhecimento, que consiste na absorção das informações fornecidas pelo tratamento dos dados. O elemento final da cadeia serve de auxílio para que a tomada de decisão da empresa seja a mais eficiente possível em relação aos objetivos almejados. Bioni (2019, p. 8) exemplifica de forma brilhante como tal elemento se traduz na realidade:

A informação em si não é o que alavanca eficiência na atividade empresarial, mas o seu processamento-organização a ser transformado em um conhecimento aplicado. No caso da Zara, os bens de consumo são projetados de acordo com a reação do mercado consumidor, sendo este o conhecimento gerado dos dados extraídos das vendas junto ao seu público-alvo.

Apresentados os elementos, a questão que se apresenta como relevante é o fato que esta atividade do uso de dados revelam informações relacionadas a direitos fundamentais, como o de privacidade, autodeterminação informacional e livre desenvolvimento da personalidade. Frente a isto, decorre a necessidade de o estado resguardar estas informações, para que não haja violação dos mencionados direitos, já que estas são garantias fundamentais constitucionalmente previstas. Nessa senda, a proteção de dados pessoais consiste na tutela jurídica para o correto uso destas informações, juntamente com a possibilidade de o titular dos dados determinar se terá seus dados tratados além da forma que seus dados serão

utilizados, pois “Longe de representar ‘informações sem dono’ livremente coletáveis na internet, os dados pessoais exprimem uma importante projeção da personalidade humana, exigindo firme proteção da ordem jurídica”. (SCHREIBER, 2020, p. 331).

## **2.2 Contextualização do Cenário Global em Proteção de Dados**

Sendo a proteção de dados pessoais, em sua essência, um desdobramento dos direitos de privacidade e livre desenvolvimento da personalidade em consequência aos avanços de tecnologias da sociedade moderna, faz-se necessário entender o ponto de origem da questão. Tem-se no clássico artigo de Samuel Warren e Louis Brandeis (1890), o primeiro paradigma deste fundamental direito, sendo o direito de ser deixado só “*right to be let alone*”, que consistia em defender as crescentes ameaças à personalidade humana decorrentes da massificação da mídia e abusos da imagem e de informações pessoais, vindo o mesmo a ser incorporado à grande parte dos ordenamentos jurídicos nacionais, e reafirmado no art. 12 da Declaração Universal dos Direitos Humanos (DUDH) (CUEVA, 2019, p. 2777).

Já na década de 1970, com o rápido avanço da informática, gerando crescentes ameaças ao direito de intimidade e privacidade, observou-se o surgimento das normas de proteção de dados de primeira geração. Ao ater-se ao continente europeu, tem-se: a Lei de dados da Suécia, de 1973; Portugal em 1976, sendo o primeiro país a colocar o direito à proteção de dados com caráter constitucional, e por último a lei federal de proteção de dados da Alemanha, de 1977 (*Bundesdatenschutzgesetz*). Já em análise ao continente americano, em 1974 editaram a lei mais conhecida em proteção de dados americana, intitulada como “Privacy Act”, a qual deu aos norte-americanos maior segurança nas atividades de tratamento de dados pessoais, além da possibilidade de poder verificar abusos na coleta (RAURO, 2013, p. 176).

Na década de 80, o continente europeu já despontava na vanguarda da proteção de dados ao editar a Convenção do Conselho da Europa nº 108, de 1981, a qual possuía como fim criar regulamentos para a proteção de indivíduos do

processamento automático de dados. Ainda na referida década, mais especificamente em 1983, a Corte Constitucional Alemã em ação, que abordava a inconstitucionalidade da Lei de Recenseamento (*Volkszählungsgesetz*), a qual obrigava os cidadãos alemães a fornecerem dados ao governo. Neste julgamento, reconheceu-se a existência do direito de autodeterminação informativa, fundamentando-se no mencionado direito de livre desenvolvimento da personalidade e da dignidade da pessoa humana. Por força do inovador direito, o indivíduo passou a ter a capacidade de determinar sobre a exibição dos seus dados pessoais (CUEVA, 2019, p. 2777).

Ponto fundamental no cenário mundial da proteção de dados, foi marcada com a edição da Diretiva Europeia n° 46 de 1995, denominada como “Diretiva de Proteção de Dados”, sendo naquela época o principal e inovador instrumento jurídico na busca de tutelar e regular o tratamento de dados em decisões automatizadas, com o fim de evitar o desrespeito aos direitos atrelados à atividade, tendo como ponto principal a exigência que cada país-membro institísse uma agência ou comissário de proteção de dados, além de editar leis específicas relacionadas à questão (EUR-LEX, 2014).

No final do século XX, já se observa entre as nações europeias uma grande produção jurídica em proteção de dados pessoais. Especificamente em 2000, a União Europeia (UE), em sua Carta dos Direitos Fundamentais, definiu no art. 8°, o direito de o indivíduo ter seus dados pessoais protegidos. Mais adiante, já no início do século XIX, a UE editou a diretiva n° 58, de 2002, com foco na proteção da privacidade no âmbito das comunicações eletrônicas. Já em 2016, a sistemática de proteção de dados foi revisada e alterada, resultando no Regulamento Europeu n° 679, de 2016 denominado “Regulamento Geral de Proteção de Dados”, o qual passava a versar sobre a proteção das pessoas naturais com respeito ao processamento de dados pessoais e ao livre movimento desses dados, sendo o RGPS o modelo base da legislação brasileira (CÂMARA, 2018).

Por fim, tem-se como divisor de águas, no cenário mundial da proteção de dados, tendo resultado na mencionada alteração da legislação europeia, e na criação de legislações de dados ao redor do globo - inclusive a brasileira - as diretrizes elaboradas pela Organização para Cooperação e Desenvolvimento

Econômico (OCDE), que em 11 de julho de 2013, por meio de seu Conselho, emitiu uma série de recomendação às nações no momento de elaborarem suas respectivas leis, definindo os principais princípios norteadores para o processamento e compartilhamento de dados, evitando que haja violação de direitos individuais, em que dentre eles destacam-se: o Princípio da Limitação de Coleta, Transparência, Qualidade dos Dados, Finalidade e o da Responsabilidade (CUEVA, 2019, p. 2792).

### *2.2.1 Contextualização do cenário nacional em proteção de dados*

No cenário nacional, já se observava uma proteção constitucional a direitos atrelados aos dados, ao tutelar a intimidade, privacidade (art. 5º, X), além de instituir e assegurar o remédio constitucional do *habeas data*, o qual assegura o livre acesso do cidadão a informações que lhe digam respeito contidas em registros ou banco de dados públicos (art. 5º, LXIX e LXXII). Soma-se ao cenário nacional as regras do Código de Defesa do Consumidor (CDC) (art. 43), o qual possui regra própria a respeito de banco de dados e cadastros de consumidores juntamente com a lei nº 12.414/2011, que disciplina o cadastro positivo, e, por final, a lei nº 12.965/2014, denominada “Marco Civil da Internet”, sendo a lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado (CUEVA, 2019, p. 2808).

Nesse contexto a mencionada Lei nº 13.709/2018, nomeada de “Lei Geral de Proteção de Dados”, vem a complementar o Marco Civil da Internet, instituindo inovador instrumento jurídico no ordenamento jurídico brasileiro, que com cujo tem por finalidade a proteção dos direitos individuais e coletivos no momento do tratamento de dados pessoais, além de colocar o Brasil em conformidade com os parâmetros globais exigidos para que o processamento e compartilhamento de dados entre nações. Feita a introdução pertinente ao objeto de estudo, o presente trabalho passará a analisar os principais pontos da lei brasileira, abordando suas definições, fundamentos e princípios.

## 2.3 Lei Geral de proteção de Dados - LGPD

Ao tratar das questões relacionadas à LGPD, será destacado os principais pontos relacionados a sua definição, os fundamentos que a baseiam além dos princípios a serem respeitados, no momento do tratamento de dados pessoais.

### 2.3.1 Definição

A LGPD, de nº 13.709, de 14 de agosto de 2018, é uma Lei Federal que se dedica à vulnerabilidade do titular de dados pessoais, cuja finalidade é a proteção das pessoas naturais contra o tratamento ilegal destes dados realizado por qualquer pessoa, independentemente de ser pessoa física ou jurídica, de direito público ou privado, conforme previsto em seu art. 1<sup>o</sup><sup>4</sup> (BRASIL, 2018a). Logo, é possível notar que, pelo verbo proteger, contido no referido artigo, o legislador viu o titular dos dados em posição de desigualdade frente ao agente de tratamento, ficando nítida a sua vulnerabilidade (COTS, 2020, p. 1272).

### 2.3.2 Fundamentos

A LGPD, em seu art. 2<sup>o</sup>, define de forma clara e direta, em 7 (sete) incisos, quais são seus fundamentos, sendo eles:

I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - à inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018a, n. p.).

O respeito à privacidade, à liberdade de expressão, de informação, de comunicação e de opinião, além da inviolabilidade da intimidade, da honra e da imagem, como fundamentos da LGPD, vem a demonstrar a preocupação da mesma com direitos fundamentais e essenciais ao desenvolvimento da personalidade do indivíduo. Atualmente não se trata exclusivamente de isolamento ou solidão, mas de

---

<sup>4</sup> “Art. 1<sup>o</sup> Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”. (BRASIL, 2018, n. p.).

conferir o poder ao indivíduo de propiciar o controle pleno da sua privacidade, de suas manifestações, controlando, assim, quem será admitido na esfera de sua vida íntima, e de não ser repreendido por expressar suas posições ideológicas. Nesse sentido, a lei de dados brasileira previu ferramentas para que a pessoa natural tenha maior controle das informações relacionadas à sua vida privada (COTS; OLIVEIRA, 2019, p. 1338).

Pelo fundamento da Autodeterminação Informativa, a pessoa natural, titular do dado pessoal que venha a sofrer tratamento por controlador/operador, tem o pleno direito de saber o que é feito com seus dados e da fidedignidade dos mesmos. Desta forma, por este fundamento, soma-se a possibilidade de manifestação de vontade do titular, que não poderá ser impedida por terceiros, com a obrigação do controlador em prestar informações sobre seus dados (COTS; OLIVEIRA, 2019, p. 1339).

O desenvolvimento econômico e tecnológico, e a inovação juntamente com a livre iniciativa, a livre concorrência e a defesa do consumidor, são interesses do Estado. Tais fundamentos possuem caráter constitucional, vez que são previstos na CF/88, visto que para os países adotantes da economia de mercado, é de suma importância o desenvolvimento econômico, de pesquisas e inovação tecnológica, além de possuir um mercado consumidor forte e seguro. Desta forma, o regramento imposto pela LGPD não deve, a não ser em casos excepcionais, piorar ou impedir o perfeito desempenho do Estado na realização de seus interesses, e um deles, como visto, é o desenvolvimento econômico, tecnológico e a inovação (COTS; OLIVEIRA, 2019, p. 1461).

Quanto ao fundamento relacionado aos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, destaca-se a última parte, na qual observou-se no mundo a utilização dos dados pessoais nos processos eleitorais das maiores democracias do planeta, sendo que tais práticas feriam o direito de livre desenvolvimento da personalidade e o exercício da cidadania naquela época. Logo, ao colocar tais direitos como fundamento da lei, vem a demonstrar a sensibilidade da mesma com a inviolabilidade dos mencionados direitos.



### 2.3.3 Princípios

O legislador no art. 6<sup>o</sup>, da Lei de Dados brasileira, fala que as atividades envolvendo tratamento de dados pessoais deverão observar a boa-fé e 10 (dez) princípios que se correlacionam, distribuídos nos seus incisos, os quais serão abordados mais adiante. Quanto aos princípios jurídicos, primeiro deve-se compreender que, ao se falar desta fonte do direito, está a se falar do suporte teórico e dos valores sobre os quais o legislador pátrio se baseou no momento de criação da norma. Na definição doutrinária de Silva (2001, p. 639), princípios são:

Princípios, no plural, significam as normas elementares ou os requisitos primordiais instituídos como base, como alicerce de alguma coisa [...] revelam o conjunto de regras ou preceitos, que se fixam para servir de norma a toda espécie e ação jurídica, traçando, assim, a conduta a ser tida em qualquer operação jurídica [...] exprimem sentido mais relevante que o da própria norma ou regra jurídica [...] mostram-se a própria razão fundamental de ser das coisas jurídicas, convertendo-as em perfeitos axiomas [...] significam os pontos básicos, que servem de ponto de partida ou de elementos vitais do próprio Direito.

Desta forma, é de suma importância o estabelecimento pela LGPD de princípios legais ao regular o tratamento de dados. Entretanto, por se tratar de um setor intrinsecamente ligado ao mundo digital e tecnológico, há o risco da criação de um ordenamento juridicamente rígido passível de acarretar o ancilamento prematuro da nova normativa. Assim, pode-se observar que, frente à questão apresentada, o legislador, ao estabelecer princípios na atividade de tratamento de dados, tentou criar uma norma com a capacidade de adaptar-se a uma seara de relações muito dinâmicas, conferindo maior tempo de “validade” à lei (COTS, 2020, p. 1957).

Traçadas as considerações introdutórias, faz-se pertinente examinar os mencionados princípios jurídicos considerados pela LGPD, em relação à atividade de tratamento, sendo eles os da: i) Finalidade; ii) Adequação; iii) Necessidade; iv) Livre Acesso; v) Qualidade dos Dados; vi) Transparência; vii) Segurança; viii) Prevenção; ix) Não Discriminação; e, x) Responsabilização e Prestação de Contas.

---

<sup>5</sup> “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: i) finalidade; ii) adequação; iii) necessidade; iv) livre acesso; v) qualidade dos dados; vi) transparência; vii) segurança; viii) prevenção; ix) não discriminação; e, x) responsabilização e prestação de contas”.

i) Finalidade: Por força de tal princípio, o tratamento de dados necessita ter uma finalidade, e, devido a isto, para a realização do tratamento, deve-se obter um resultado explícito, específico e legítimo. O princípio não vale apenas para limitar o objetivo final do tratamento, mas para tornar previsível o que dele se espera, inviabilizando tratamento posterior desvinculado com a finalidade original. Exemplos de violação ao Princípio da Finalidade: i) informar que a coleta de dados servirá para faturamento de produto ou serviço, mas utilizar os dados para campanhas de *marketing*; ii) informar que o compartilhamento de dados se dará com empresa X, mas compartilhar os mesmos com a empresa Y; iii) informar que os dados não serão copiados, mas realizar cópia destes (COTS, 2020, p. 1977);

ii) Adequação: O Princípio da Adequação está diretamente relacionado com o princípio anterior, entretanto, diferente daquele, que visa o fim do tratamento, pois este tem como objeto o meio, ou seja, o procedimento realizado pelo agente de tratamento para chegar na finalidade pretendida. Exemplos de violação ao Princípio da Adequação: i) informar comunicação com determinados operadores, mas realizar comercialização livre dos dados pessoais no mercado; ii) informar que os dados serão eliminados, mas deter consigo cópia dos mesmos; iii) informar que os dados serão anonimizados, mas realizar o procedimento de pseudo anonimização (COTS, 2020, p. 1988);

iii) Necessidade: Já o Princípio da Necessidade, o agente de tratamento, ao realizar a atividade, deve limitar-se aos mínimos dados necessários para atingir a finalidade pretendida, descartando o que for em excesso e desnecessário. Exemplos de violação ao Princípio da Necessidade: i) solicitar cor da pele para faturamento de produtos ou serviços; ii) solicitar orientação sexual para admissão de empregado; iii) solicitar todos os endereços em que a pessoa pode ser encontrada, a fim de realizar a entrega de produto em apenas um deles (COTS, 2020, p. 1988);

iv) Não Discriminação: Pelo Princípio da Não Discriminação, há vedação legal de tratar dados para fins discriminatórios ilícitos ou abusivos. Exemplos de violação ao Princípio da Não Discriminação: i) realizar senso para dispensa de empregados de determinada religião; ii) realizar a oferta de produtos ou serviços apenas para pessoas de determinada nacionalidade; iii) não admitir como usuário pessoas do sexo feminino (COTS, 2020, p. 2002);

v) **Transparência:** O Princípio da Transparência vem a garantir que o titular dos dados pessoais tenha sempre informações claras, precisas e acessíveis em relação ao tratamento de seus dados pessoais. Exemplos de violação ao Princípio da Transparência: i) não informar a qualificação completa do controlador; ii) deixar de descrever a abrangência do tratamento realizado; iii) não fornecer fácil acesso às informações de tratamento” (COTS, 2020, p. 2015);

vi) **Segurança e Prevenção:** Neste caso, tem-se princípios complementares, que por força destes, os agentes de tratamento - controlador e operador- devem se valer de técnicas que sejam efetivamente aptas a proteger os dados pessoais de acessos não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração ou difusão, que causem dano ao titular, tendo o princípio como ideia central à preservação, em ambiente seguro, dos dados pessoais, objeto do tratamento. Desta forma, deverão ser utilizadas, sempre, técnicas atuais de segurança e procedimentos constantemente aprimorados, com vistas a garantir a manutenção da segurança e prevenção. Vale destacar que, por força deste princípio, é imposto aos agentes de tratamento um dever continuado de fornecer aos dados uma segurança efetiva, pois havendo falha com estes, o operador ou controlador poderão ser responsabilizados civil e administrativamente (PESTANA, [20--], p. 7-8);

vii) **Responsabilização e Prestação de Contas:** Relaciona-se com a demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da efetividade dessas medidas. O agente não só deverá comprovar ter adotado os procedimentos e praticado os atos permitidos pela LGPD, como também que todos eles tenham tido a eficácia esperada, pois caso contrário, ainda que tenha agido com boa-fé, ocorrido o descumprimento das normas de proteção de dados, haverá ofensa ao Princípio da Responsabilização e da Prestação de Contas (PESTANA, [20--], p. 8-9);

viii) **Qualidade dos Dados:** Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade, e para o cumprimento da finalidade de seu tratamento, vez que, havendo dados de qualidade duvidosa, toda a atividade de tratamento de dados pessoais poderá estar em risco, e, assim, não atingindo as finalidades desejadas (BRASIL, 2018a, n. p.);

ix) Livre Acesso: Um dos princípios centrais da LGPD, no que concerne ao tratamento, é que os titulares dos dados tenham a garantia de acesso facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Tal atividade geralmente é desenvolvida pelo encarregado definido pelo controlador dos dados (BRASIL, 2018a, n. p.).

## **2.4 Agentes de Tratamento de Dados**

Pode-se dizer que os agentes de tratamento figuram como os novos atores nesse cenário de proteção de dados, pois a eles exige-se uma série de deveres a serem cumpridos ao exercer a atividade com dados. Previstos inicialmente no artigo 5<sup>o</sup>, incisos VI, VII da LGPD, possuem regulamentação própria no Capítulo VI, com acréscimo do personagem encarregado pelo art. 41<sup>7</sup> (BRASIL, 2018a, n. p.).

### *2.4.1 Controlador*

Por definição, na LGPD, o controlador pode ser classificado como “pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018a, n. p.). Se equiparando à figura do responsável no Regulamento Geral sobre a Proteção de Dados (GDPR), isto é, à empresa que demanda o tratamento, pode ela mesma executá-lo ou designar um operador. A lei brasileira, no entanto, diverge em um ponto da lei europeia: o controlador pode ser pessoa natural - já na GDPR essa classificação é limitada à pessoa jurídica. Desta forma, é incumbência do controlador seguir o disposto na LGPD, devendo realizar o tratamento de acordo com os princípios ou orientar corretamente o operador, para que este realize um tratamento lícito.

Por fim, no quesito da responsabilidade, ele responde por danos patrimoniais, morais, individuais ou coletivos, além de violações à legislação decorrentes do dever de reparação. Responde, ainda, de forma solidária, pelos

---

<sup>6</sup> Art. 5<sup>o</sup> Para os fins desta Lei, considera-se:

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

<sup>7</sup> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

danos causados pelo operador, nos casos de estar diretamente envolvido no tratamento que resultar em danos (KAUER, [20--], n. p.).

#### 2.4.2 Operador

Quanto ao operador, cabe a este apenas cumprir as ordens do controlador quanto à finalidade do tratamento, além de atuar com respeito aos dispositivos legais da LGPD. O operador por definição legal é “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”, ou seja, é o equivalente ao subcontratante da GDPR, sendo o processador dos dados pessoais. O operador deve seguir as diretrizes indicadas pelo controlador, e tratar os dados de acordo com a normativa implementada pela LGPD. Responde o operador de forma solidária ao controlador pelos danos causados, caso atue em desarmonia com as obrigações da legislação de proteção de dados ou quando não seguir as instruções do controlador, casos em que se equiparava ao controlador (KAUER, [20--], n. p.).

#### 2.4.3 Encarregado / Data Protect Office

Definido legalmente como: “Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados”. Equivale à figura do *Data Protection Office*, da GDPR, e tem como responsabilidade legal ser o canal de comunicação do controlador com os titulares e autoridade nacional, fornecendo esclarecimentos, providências e orientações internas. No texto original da LGPD, havia a exigência de que o encarregado fosse pessoa física; mas a redação foi alterada com a MP 869/2018 (BRASIL, 2018b, n. p.). Quanto à responsabilidade dele, é importante frisar que não há previsão sobre esta figura responder legalmente. A responsabilidade, em caso de incidente, é do controlador ou operador (a depender do caso concreto); mas nunca do departamento encarregado (KAUER, [20--], n. p.).

### **3 REGIME DE RESPONSABILIDADE DOS AGENTES DE TRATAMENTO**

#### **3.1 Conceito de Responsabilidade Civil**

Conforme leciona Carlos Roberto Gonçalves (2011, p. 24): “A responsabilidade civil tem, pois, como um de seus pressupostos, a violação do dever jurídico e o dano. Há um dever jurídico originário, cuja violação gera um dever jurídico sucessivo ou secundário, que é o de indenizar o prejuízo”. Neste tópico, serão feitas breves considerações sobre os conceitos relacionados à responsabilidade civil no direito brasileiro, para refrescá-los dos pontos de importância ao objeto estudado.

#### **3.2 Pressupostos**

Quanto aos pressupostos, cabe destacar que estes se traduzem em condições previamente necessárias para que se possa iniciar determinado ato jurídico, nos casos em que se verifica a responsabilização civil de determinada pessoa, faz-se necessário observar três requisitos, sendo eles a conduta ilícita imputada ao agente, o nexo de causalidade desta e por último analisar a extensão do dano sofrido.

##### **3.2.1 Conduta ilícita**

Segundo previsão do Código Civil (CC) brasileiro, no Título III - “Dos Atos Ilícitos”:

Aquele que por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral ou no caso do titular de um direito que, ao exercê-lo, excede manifestamente os limites de seu fim econômico, social, em ofensa à boa-fé e aos bons costumes, comete ato ilícito (BRASIL, 2002, n. p.).

Pelo que se depreende do texto legal, no direito brasileiro foi estabelecida a responsabilidade aquiliana ou extracontratual (3.3.2), logo, aquele, ainda que involuntariamente, tenha uma conduta e decorrente desta, venha causar danos na esfera de direitos de outrem, comete ato ilícito e assim fica obrigado a reparar tais

prejuízos. Isto é, o agente de tratamento que causar danos no exercício da atividade de tratamento de dados, terá que indenizá-los a quem sofreu (GONÇALVES, 2020, p. 63).

### 3.2.2 *Nexo de Causalidade*

O nexo de causalidade é um pressuposto de fácil entendimento, segundo Venosa (2010, p. 403) “o nexo causal é o liame que une a conduta do agente ao dano [...]”. Nesse condão, o nexo de causalidade é requisito essencial para imputar ao agente qualquer tipo de responsabilidade civil e/ou penal. Portanto, este é o elemento ligado à responsabilidade civil, que trata da relação de causalidade entre a ação ou omissão na conduta ilícita do agente e suas contribuições para o dano verificado.

Pode-se concluir que este não é o elemento central ligado a responsabilidade civil, mas um meio para que se possa chegar nela, vez que para que seja auferida a culpabilidade da conduta do agente e as extensões do dano, é necessário, a demonstração do nexo de causa e efeito entre os outros dois pressupostos da responsabilidade

### 3.2.3 *Dano*

O dano consiste no prejuízo sofrido pela vítima do ato ilícito, o qual ensejou a responsabilidade civil. É o principal ponto da responsabilidade civil, visto que, a partir dele, é que será necessária a fixação da indenização relativa ao dano suportado pela vítima. Cabe destacar que o dano deverá ser observado tanto no caso de responsabilidade civil subjetiva, quanto da responsabilidade civil objetiva, sendo que, nos dois casos, não ocorrendo o dano, não será cabível qualquer indenização. Nos dizeres de Venosa (2013, p. 38):

Dano consiste no prejuízo sofrido pelo agente. Pode ser individual ou coletivo, moral ou material, ou melhor, econômico e não econômico. A noção de dano sempre foi objeto de muita controvérsia. Na noção de dano está sempre presente a noção de prejuízo. Nem sempre a transgressão de uma norma ocasiona dano. Somente haverá possibilidade de indenização, como regra, se o ato ilícito ocasionar dano. Cuida-se, portanto, do dano injusto, aplicação do princípio pelo qual a ninguém é dado prejudicar outrem (*neminem laedere*) (BAPTISTA, 2003, p. 47).

Portanto, o dano, configura-se como elemento central da responsabilidade civil, sendo necessária a demonstração de um prejuízo material ou moral causado pelo agente na esfera de direito de outrem, possibilitando desta forma uma indenização pelo transtorno sofrido. Tendo sido apresentados os pressupostos necessários à responsabilidade civil, faz-se mister abordar as classificações pertinentes à questão estudada.

### **3.3 Classificações**

Quanto a este item, será abordado rapidamente as principais classificações da responsabilidade civil no direito brasileiro, levando em consideração os aspectos relacionados à natureza da obrigação, o vínculo jurídico na relação e por último a voluntariedade da conduta.

#### *3.3.1 Obrigação: Solidária - subsidiária*

A solidariedade e subsidiariedade na responsabilidade civil relacionam-se com a responsabilidade inicial da obrigação de ressarcimento do dano causado. Nos casos em que são vários responsáveis pelo dano, sendo hipótese de responsabilização solidária, todos respondem com seu patrimônio até o limite do dano, cabendo, a quem pagou, o direito de regresso contra os demais. Já nas situações de subsidiariedade, há uma ordem no momento de demandar os responsáveis, caso o principal não quite a obrigação, o subsidiário possui legitimidade passiva para figurar na demanda.

#### *3.3.2 Vínculo jurídico: extracontratual - contratual*

Já esta classificação, é atrelada à natureza do dever jurídico violado pelo responsável. A responsabilidade contratual ocorre pela inexecução contratual, ou seja, a falta de inadimplemento ou mora no cumprimento de uma obrigação estabelecida em contrato. Logo, não há necessidade do contratante que sofreu o dano provar a culpa, vez que a própria inadimplência se presta a isto.

Do outro lado, tem-se a regra geral do direito brasileiro, a responsabilidade extracontratual, conhecida como aquiliana, ocasionada pelo inadimplemento normativo do responsável pelo dano, tendo por fonte deveres jurídicos originados da



lei e do ordenamento jurídico em geral. É a responsabilidade que nos interessa, vez que os agentes de tratamento devem observar todos os princípios acima mencionados além das várias normativas impostas pela LGPD ao realizar a atividade de tratamento de dados pessoais.

### 3.3.3 *Voluntariedade: objetiva - subjetiva*

Aqui se insere a problemática do presente trabalho, pois a premissa deste estudo é analisar a voluntariedade da culpa ao definir responsabilidade dos agentes de tratamento por danos decorrentes da atividade exercida. Dito isto, verifica-se no direito civil brasileiro duas formas de responsabilização parametrizada pela culpa na conduta daquele que causa o dano a outrem.

Desta forma, por força dos dispositivos contidos nos artigos 186<sup>8</sup>, 187<sup>9</sup> e 927<sup>10</sup> do CC tem-se como cláusula geral no ordenamento jurídico brasileiro, a necessidade de demonstração da culpa na prática do ato ilícito gerador do dano, tal característica está ligada intrinsecamente à subjetividade da conduta, ou seja, há a necessidade de ampla discussão sobre a vontade do agente em relação ao dano causado. Seguindo os ensinamentos de Cavalieri Filho (2003, p. 36), tem-se que:

Responsabilidade subjetiva teremos sempre, até o juízo final, mesmo não havendo lei prevendo-a, porque essa responsabilidade faz parte da ética, da moral, do sentimento natural de justiça. Decorre daquele princípio superior de direito, de que ninguém deve causar dano a outrem. Então, vale ressaltar, sempre que não tivermos disposição legal expressa consagrando a responsabilidade objetiva, persiste a responsabilidade subjetiva, como sistema subsidiário, como princípio universal de direito; posso não responder objetivamente por falta de previsão legal, mas, subjetivamente, se causar dano a outrem, vou ter sempre que responder [...].

Essa responsabilidade só vai se configurar quando houver conduta culposa, nexos causal e dano, com aquela complexidade toda de provar a culpa, como violação ao dever de cuidado. Cláusula geral,

---

<sup>8</sup> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. (BRASIL, 2002, n. p.).

<sup>9</sup> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes. (BRASIL, 2002, n. p.).

<sup>10</sup> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. (BRASIL, 2002, n. p.).

aberta, que sempre exigirá um juízo de valor, porque em cada caso teremos que ver se houve previsibilidade, se houve um comportamento adequado etc.

Do outro lado, há a responsabilização objetiva, onde independe da existência do elemento culpa, vez que esta é presumida em favor de quem suportou o dano, cabendo discutir apenas a ilicitude do ato e o dano. Tal tipo de responsabilização foi inicialmente prevista no âmbito das relações de consumo, em que o consumidor se mostrava como parte vulnerável. Posteriormente, com a vigência do CC (BRASIL, 2002), aquele que pratica atividade com potencial de gerar risco à coletividade, passou a responder de forma objetiva, conforme previsão do contida no art. 927, parágrafo único<sup>11</sup>.

Frente a isto, faz-se necessário destacar os pontos relevantes, referente à responsabilidade pelo exercício de uma atividade de risco. Na doutrina de Cavalieri Filho (2003, p. 40), encontra-se esclarecedores ensinamentos sobre a questão, ao analisar o termo atividade:

Mas no parágrafo único do art. 927, o Código usou a outra expressão “atividade”. E será que o fez por mera coincidência? Não. Isso deve ter relevância. Se ali diz “atividade”, é porque estava querendo se referir a uma outra modalidade de comportamento, a uma outra espécie de conduta, que não a mera “ação ou omissão voluntária, negligência ou imprudência”. Qual seria? [...]

Não há dúvida, portanto, de que o próprio Código Civil, e não apenas o Código do Consumidor, utilizou em mais de um lugar a palavra “atividade”, não para indicar a ação ou omissão esporádica, isolada de alguém, mas a conduta profissional, habitual, economicamente organizada.

Desta forma, percebe-se que ao falar de atividade, há o elemento econômico intrínseco. Quanto ao risco, cabe destacar que o direito civil brasileiro é adepto da Teoria do Risco Criado<sup>12</sup>, frente a isto, deve-se compreender que certas atividades têm o condão de gerar perigo é probabilidade de dano a direitos de

---

<sup>11</sup> “Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem”. (BRASIL, 2002, n. p.).

<sup>12</sup> “Aquele que, em razão de sua atividade ou profissão, cria um perigo, está sujeito à reparação do dano que causar, salvo prova de haver adotado todas as medidas idôneas a evitá-lo, [...] A teoria do risco criado importa em ampliação do conceito do risco proveito. Aumenta os encargos do agente, é, porém, mais equitativa para a vítima, que não tem de provar que o dano resultou de uma vantagem ou de um benefício obtido pelo causador do dano”. (PEREIRA, 1992, p. 24).

outrem. Por força disso, na ocorrência do dano, o infrator assume o risco, não havendo espaço para discussão se houve culpa, respondendo objetivamente.

A questão que se problematiza a partir do presente momento, é compreender dentre os dois modelos, qual atinge de fato os objetivos pretendidos com a lei de dados brasileira, ao fixar a responsabilização dos agentes de tratamento de dados pessoais. Ou seja, nos casos em que esta atividade gere danos ao titular, deve o agente responder mediante culpa pelo modelo tradicional ou seguir o modelo do risco/vulnerabilidade e, assim, presumindo a culpa em favor de quem suportou o dano.

### **3.4 Pressupostos da Responsabilidade Civil em Proteção de Dados**

Neste item, o presente trabalho se propõe em realizar uma curta análise dos pressupostos da responsabilidade civil com prisma voltado para LGPD, examinando: i) conduta que ensejaria reparação; ii) nexo de causalidade da conduta do agente com o ilícito; iii) e o que se entende como dano. Não sendo objeto deste tópico a análise da culpabilidade objetiva ou subjetiva dos agentes de tratamento, pois tais questionamentos irão ser analisados separadamente nos itens 3.2.1 e 3.2.2, respectivamente.

#### **3.4.1 Da Conduta Ilícita**

Pela simples leitura da LGPD, evidencia-se a existência de duas antijuridicidades que dão ensejo à responsabilização dos agentes de tratamentos, são elas:

i) O agente de tratamento, que no exercício da atividade, violar a legislação de proteção de dados<sup>13</sup>, causando dano patrimonial ou extrapatrimonial a terceiros (Art. 42, LGPD). Assim, incorre em conduta ilícita, com consequente violação da legislação o operador que no tratamento de dados não observa as bases legais

---

<sup>13</sup> De acordo com Capanema (2020, p.165), “A responsabilidade surge do exercício da atividade de proteção de dados que viole a ‘legislação de proteção de dados’. Por essa expressão, o legislador reconhece que a proteção de dados é um microsistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. Deve-se aqui fazer uma analogia com o conceito de ‘legislação tributária’ do art. 96 do CTN, para incluir não apenas as leis que versem sobre a proteção de dados, mas as normas administrativas regulamentares que serão expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades”.

impostas pela LGPD, referentes aos princípios norteadores e aos requisitos para o tratamento de dados pessoais previstos no capítulo I (Disposições Preliminares) e capítulo II (Do Tratamento de Dados Pessoais). Logo, caso o agente de tratamento venha exercer a atividade, coletando dados sem finalidade específica ou consentimento prévio do titular dos dados, incorrerá na conduta ilícita tipificada.

ii) Pelo não fornecimento de um nível adequado de segurança de dados esperado pelo titular (Art. 44 c/c 46, LGPD). Relacionado a esta antijuridicidade, cabe destaque para o que se entenderá como nível adequado, visto a complexidade da atividade de segurança da informação, devendo ser consideradas apenas aquelas medidas previstas em padrões devidamente reconhecidos, como as denominadas normas da Organização Internacional de Normalização (ISO)<sup>14</sup> (CAPANEMA, 2020). Já em relação ao nível adequado de segurança esperado pelo titular, tem-se no exemplo de Cots e Oliveira (2019, p. 205), uma visão de como isso se traduz na realidade:

O titular que abre conta bancária tem uma expectativa alta de segurança de seus dados pessoais. Se o faz na agência bancária ou por meio de aplicativo pode fazer essa expectativa variar, mas continua, em ambos os casos, sendo alta. Por outro lado, o titular que fornece dados pessoais, como seu nome e telefone, para participação em um sorteio realizado pelo açougue de sua rua, tem uma expectativa de segurança completamente diferente daquela verificada no primeiro exemplo. Deveria o açougue contratar todas as ferramentas tecnológicas que um banco geralmente contrata, a fim de realizar a coleta de dados pessoais para seu sorteio? Obviamente que não e não se pode esperar que isso aconteça, ou seja, a relação do açougue com o titular não cria altos graus de expectativa de segurança dos dados pessoais.

O que se destaca de importante nesse ponto é perceber que o legislador criou duas condutas antijurídicas passíveis de responsabilização: a primeira específica, fundamentada na violação “direta” da legislação de proteção de dados pessoais, e uma segunda relativa aos deveres gerais de segurança dos agentes de tratamento no exercício da atividade.

---

<sup>14</sup> ISO é o acrônimo de *International Organization for Standardization*, uma entidade internacional que estabelece normas e padrões. O padrão ISO 27001, por exemplo, é destinado à segurança da Informação. Seu sítio está disponível em: <https://www.iso.org/home.html>. Acesso em: 14 out. 2020.

### 3.4.2 Do Nexo de Causalidade

Partindo da premissa firmada no item 3.2.2, na qual nexo causal é o elemento referencial entre a conduta e o resultado. É através dele que se pode concluir quem foi o causador do dano; logo, para fins de responsabilização civil, será necessário, no caso concreto, examinar a correlação entre o dano suportado pelo titular em conjunção com a conduta adotada pelo agente de tratamento. Segundo considerações de Cots e Oliveira (2019, p. 175): “o nexo causal do dano está intrinsecamente ligado à violação LGPD, sendo que, se não houve violação, não se torna aplicável o art. 42, não se configura o ilícito”.

Referente ao nexo de causalidade, imagine a situação, na qual uma incorporadora XZA ao estabelecer um contrato de compra de imóvel com o cliente X, obtém em decorrência dessa relação contratual informações do seu cliente. Na posse dessas informações - sem consentimento dos titulares - compartilha com seus parceiros de atividade para que esses possam captar clientes e oferecer seus serviços, vindo tais parceiros a oferecer efetivamente tais serviços.

O cliente X, titular dos dados, sente que sua privacidade foi violada pela conduta adotada, ao entrar em juízo demonstrando que não consentiu com o compartilhamento das informações, poderá pleitear contra o agente de tratamento responsável a indenização pelos danos sofridos. O caso exemplificado corresponde aos fatos narrados na primeira decisão relacionada à LGPD processo nº 1080233-94.2019.8.26.0100, que tramita na 13ª vara cível do Tribunal de Justiça do Estado de São Paulo.

### 3.4.3 Do Dano

Nesse modelo atual em que os dados pessoais assumem papel fundamental no desenvolvimento social e econômico das sociedades, crescem da mesma forma os riscos inerentes à atividade de tratamento de dados. O fato é que não se pode ainda precisar com exatidão a extensão dos danos, pois há infinitas possibilidades de uso para esses dados, mas das violações já presenciadas<sup>15</sup>, demonstrou-se que as potencialidades danosas são altas, tanto em termos individuais quanto coletivos.

---

<sup>15</sup> Caso do Facebook com a Cambridge Analytics; Caso do aplicativo Uber.

Entretanto, para nascer a responsabilidade civil com direito ao ressarcimento, deve-se constatar um efetivo dano suportado pelo titular, já que a simples violação dos deveres legais, sem verificação do dano, ensejaria apenas responsabilização administrativa do operador. Sucede que nos casos de danos patrimoniais, à percepção, é mais palpável, no sentido de que um prejuízo ou um lucro cessante, em virtude de violação legal, terá mensuração de extensão do dano de maneira exata e matemática, fato esse que não se vislumbra no dano de cunho moral, na qual uma análise da extensão do dano sofrido é mais complexa (CAPANEMA, 2020, p. 165).

Frente a isto, cabe destacar que a supracitada decisão relacionada à nova legislação de dados brasileira, segundo notícia do *site* Capital Digital (QUEIROZ, 2020), se deu no processo nº 1080233-94.2019.8.26.0100, que tramita na 13ª vara cível do Tribunal de Justiça do Estado de São Paulo, em que nele a juíza Tonia Yuka Koroku, ao proferir sentença, julgou procedente a ação de indenização por danos morais, entendendo a magistrada que haveria a existência de dano extrapatrimonial pelo fato da ré ter compartilhado dados sensíveis sem prévio consentimento do autor, lhe ocasionando infortúnios na esfera privada, e nesse sentido proferiu decisão nos seguintes termos:

O dano à esfera extrapatrimonial também fora demonstrado. Justamente por conta do ato ilícito relativo ao acesso de dados titularizados pelo autor a terceiros, houve violação a direitos de personalidade (intimidade, privacidade, nome). O dano, nesta hipótese, decorre do próprio ilícito (*in re ipsa*), e resta corroborado pelos documentos que comprovam que o requerente fora assediado por diversas empresas por conta da conduta ilícita da requerida (TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO, 2020, p. 1258).

Logo, deve-se verificar no caso concreto se o titular sofreu efetiva lesão aos seus direitos patrimoniais ou extrapatrimoniais pela conduta adotada pelo agente de tratamento, e se esta conduta se adequa como violadora da norma legal. Restando demonstrado como se dão os pressupostos de responsabilidade civil em proteção de dados, o presente artigo agora se debruça sobre a maneira como a doutrina brasileira vem se posicionando frente à questão de qual seria o regime adequado de responsabilização.

### 3.5 Doutrina Sobre o Regime de Responsabilidade Civil dos Agentes de Tratamento

Inicialmente, cumpre salientar que a análise do regime de responsabilidade estará atrelada ao regime geral adotado na LGPD (BRASIL, 2018a, n. p.), ficando de fora o regramento específico do instituído no art. 45<sup>16</sup>, pelo fato de sua redação deixar de forma clara, que nas hipóteses de violação do direito do titular no âmbito das relações de consumo, permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente, no caso, a sistemática de responsabilização consagrada no CDC (BRASIL, 1990, n. p.).

Partindo dessa premissa, o legislador pátrio na elaboração da LGPD empregou uma técnica legislativa imprecisa, ao definir qual seria o regime de responsabilização geral definido na Seção III, que trata da responsabilidade e ressarcimento de danos. Ocorre que isto deveria ter sido discriminado de forma clara, pois evitaria uma série de controvérsias que, inevitavelmente, vão surgir em consequência dessa falta de clareza (GUEDES, 2019, p. 169). Ao invés disso, limitou-se o legislador a estabelecer, no art. 42<sup>17</sup>, a hipótese de responsabilização dos agentes de tratamento nos casos de violações à legislação. Já no art. 44<sup>18</sup>, indicou que há responsabilização nos casos de ofensa às normas técnicas relacionadas ao dever de segurança na proteção de dados (CAPANEMA, 2020, p. 165).

---

<sup>16</sup> “Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”.

<sup>17</sup> “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.

§ 1º 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”.

<sup>18</sup> “Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano”.

Ratifica-se esse posicionamento de incerteza em relação ao regime escolhido pelo legislador com a interpretação dada por Anderson Schreiber (2020, p. 331 p.334), indicando que, se:

“ A LGPD não foi extremamente feliz no desenho das normas atinentes à responsabilidade civil. Há falhas e omissões que podem e precisam ser sanadas pelo intérprete, em busca de um regime de responsabilidade civil que se afigure, a um só tempo, coerente e eficaz. As diferentes soluções interpretativas devem ser construídas a partir de elementos constantes não apenas da LGPD em si, mas também de outras normas que compõem o tecido normativo brasileiro, em especial as normas constitucionais. (...)”

(...) Por um lado, o art. 42 não alude, em sua literalidade, à culpa, o que poderia indicar a adoção de um regime de responsabilidade objetiva. Por outro lado, o art. 42 não emprega a expressão “independentemente de culpa”, como fizeram o Código Civil (arts. 927, parágrafo único, e 931) e o Código de Defesa do Consumidor (arts. 12, caput, e 14, caput), podendo-se extrair da omissão uma preferência pela responsabilidade subjetiva. “

Referente ao regime adequado de responsabilização civil dos agentes de tratamentos de dados, observa-se na doutrina uma dicotomia tradicional da seara jurídica. Há expoentes como Rafael Zanatta em 2017 e Laura Schertel Mendes, já em 2018, que defendem o regime de responsabilização objetiva, visto considerarem que na ação de tratamento de dados revela-se um risco intrínseco, pois há um potencial danoso significativo nos casos de infração, dado que tais direitos estão relacionados à personalidade e à liberdade.

Do outro lado da doutrina, tem-se a linha de pensamento, que pela interpretação da LGPD, o regime de responsabilidade pertinente seria o de responsabilização subjetiva, tendo como expoente a doutrinadora Gisela Sampaio da Cruz Guedes, em 2019. Dentre os argumentos apresentados pelos autores, destaca-se o que alude sobre a legislação estabelecer padrões de procedimentos a serem respeitados pelos agentes de tratamento de dados, com a finalidade de fornecer maior segurança, discricção e boas práticas em administração de dados, sendo este um dos fatores elencados como justificativa para a constatação da responsabilidade subjetiva.

Após breve apresentação teórica da forma que a responsabilidade dos agentes de tratamento é vista por cada uma das correntes doutrinárias



mencionadas, o presente trabalho passa a realizar um estudo detalhado sob a argumentação apresentada pelos doutrinadores para fundamentar o regime defendido.

### *3.5.1 Regime de Responsabilidade Civil Subjetiva dos Agentes de Tratamento*

Apresentado o cenário da responsabilidade civil no âmbito da proteção de dados, o presente trabalho passa a se debruçar sobre sua questão central: o elemento culpa na responsabilização dos agentes de tratamento de dados pessoais, iniciando a presente análise pela corrente defensora da culpabilidade subjetiva dos agentes de tratamento. Logo, a professora Gisela Sampaio da Cruz Guedes (2019), defensora da natureza subjetiva da responsabilidade civil na LGPD, sugere como argumento inicial, que no texto inicial do Projeto de Lei (PL) nº 5.376 havia expressas previsões de responsabilização solidária e objetiva, uma delas no capítulo referente à transferência internacional de dados e a outra no antigo texto do art. 42 (BRASIL, 2018a):

Além disso, na Seção específica sobre “Responsabilidade e Ressarcimento de danos”, além de a inicial redação do art. 42 fazer uma abordagem ampla dos sujeitos obrigados a reparar o dano, não havia referência ao tratamento de dados em violação à lei. A redação determinava, de forma objetiva, apenas que: “Todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo” (GUEDES, 2019, p. 174).

Discorre a autora, que nas versões subsequentes do projeto legislativo, esse regime de responsabilidade deixou de ser mencionado como regramento geral. A referência expressa à responsabilidade objetiva foi completamente eliminada do texto legal, bem como se introduziu, no art. 42, a obrigação do dano pelo tratamento de dados, para fins de reparação civil, ter sido fruto do descumprimento da legislação de proteção de dados pessoais pelos agentes competentes (GUEDES, 2019, p. 174). Com isso, pode-se entender que, pela eliminação expressa referente à responsabilidade objetiva, o legislador pátrio optou por uma sistemática de verificação de culpa para configuração do dever indenizatório, seguindo o modelo tradicional de responsabilidade civil existente no CC.

Ainda nessa linha de raciocínio, tem-se os autores Cots e Oliveira (2019, p. 199), para os quais a responsabilidade civil segue o parâmetro geral do CC, fundamentado nos arts. 186, 187 e 927 (BRASIL, 2002, n. p.), sendo o art. 42 a principal disposição da LGPD que trata da responsabilidade civil dos agentes de tratamento. O artigo tem como premissa que o controlador ou operador responde pelos danos causados, sejam eles materiais, morais, individuais ou coletivos, quando houver violação à legislação. Desta forma, no caso concreto é que serão analisados os pressupostos da responsabilização civil juntamente com a culpa do agente de tratamento para incidência do dever reparatório, sendo o modelo do regime subjetivo de responsabilidade o que mais se ajusta a essa necessidade, de um processo de conhecimento para análise das circunstâncias relacionadas à culpa. (COTS; OLIVEIRA, 2019, p. 199).

Desponta ainda, como argumento na doutrina, que ao realizar uma interpretação teleológica, visando o fim a que se dirige a LGPD, observa-se que o “o legislador estabeleceu verdadeiros *standards* de condutas que devem ser seguidos pelos agentes de tratamento de dados” (GUEDES, 2019, p. 177), ao instituir no texto da LGPD o Capítulo VII, intitulado “Da Segurança e das Boas Práticas”, que é dividido em duas seções: (i) Seção I - “Da segurança e do sigilo de dados”, e (ii) Seção II - “Das Boas Práticas e da Governança”, criando uma série de deveres que devem ser observados pelos agentes de tratamento de dados.

Convergente com o argumento da autora supracitada, tem-se em Cots e Oliveira (2019, p. 224) uma análise comentada do art. 50 da LGPD, incluso no Capítulo VII, em que os autores indicaram que a LGPD implementou o “programa de governança em privacidade” similar à já conhecida política de segurança da informação, mas com foco no cumprimento da nova legislação, bem como demonstrando o comprometimento do agente de tratamento em cumprir e fazer cumprir a lei em relação aos seus contratados. Em consonância com essa linha de raciocínio, Guedes e Meireles (2019, p. 288) falam que seria incoerente o legislador ter imposto tantos deveres e fixado um padrão de conduta se fosse para responsabilizar os agentes, independentemente de sua culpa, pois pela lógica da responsabilidade objetiva, não caberia discutir descumprimento dos deveres

implementados pela lei, visto que no fundo está sendo analisado se o agente atuou ou não com culpa.

Na visão de Guedes e Meireles (2019, p. 290), a própria LGPD indica qual é o padrão de conduta socialmente esperado pelos agentes de tratamento, devendo os mesmos adotarem uma série de medidas de prevenção, segurança e boas práticas, visto que a sua atuação não será examinada meramente no plano abstrato, mas sim no caso concreto, considerando-se quais foram as medidas efetivas para evitar o dano, conter ou remediar. Isto posto, os autores consideram que pela criação desses *standards* de conduta, a LGPD se aproximou mais do regime subjetivo, pois conclui no sentido que pela noção de culpa implementada na lei de dados, se faz necessária a análise dos parâmetros de conduta socialmente aceitos para posterior verificação da culpabilidade do agente.

Desta forma, inferem os autores que além do fato da estrutura da LGPD ser pautada na criação de deveres e *standards* de conduta, há uma outra pista essencial que aponta para esse regime de responsabilidade subjetiva no tratamento de dados, que é a previsão contida no inciso II do art. 43 da lei, que ao contrário dos incisos I e III, que se referem à relação de causalidade, o inciso II remete à concepção de culpa como fundamento da responsabilidade civil (GUEDES, 2019, p. 178; BRASIL, 2018a).

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (BRASIL, 2018a, n. p.).

Por esta excludente de ilicitude contida no inciso II, o legislador isenta da obrigação indenizatória os agentes de tratamento, caso haja demonstrado em juízo que, se verificando os pressupostos de dano e nexos, não houve violação à lei ou que os *standards* de condutas foram devidamente respeitados, assim, comprovando que se o incidente ocorreu, não foi em razão da conduta adotada pelo agente. Portanto, tal inciso reflete que a escolha do legislador por um regime onde o elemento culpa

aparece como figura central, logo, o de responsabilidade subjetiva na qual haverá verificação da culpabilidade na conduta adotada pelo do infrator (GUEDES, 2019, p. 181).

Outro ponto relevante está relacionado ao dever de segurança do art. 44, pois no caso concreto, irá ser analisado se no tratamento de dados, os agentes obedeceram aos deveres de segurança, tendo fornecido os meios adequados de segurança à época do ocorrido. Logo, há necessidade de prova técnica sobre o vazamento, suas causas e desdobramentos, fator relevante a favor do regime de responsabilidade subjetiva, pois em consequência disto, se impõe na marcha processual a imprescindibilidade de um processo de conhecimento para discutir a conduta ilícita, à qual necessita de compreensão técnica específica advinda provavelmente de prova pericial. Logo, uma responsabilização sem prévia discussão sobre os pontos apresentados seria uma incompreensão da lei, já que na visão do autor, pela boa exegese da lei, prevalece o regime de responsabilidade subjetiva na qual haverá exaustiva discussão sobre os pressupostos da responsabilidade civil, devendo afastar o automatismo do regime objetivo puro (CORRÊA, 2019, p. n. p.).

Por fim, argumenta Guedes (2019, p. 296), que o tratamento de dados pessoais que versem apenas sobre informação relacionada à pessoa natural identificada ou identificável<sup>19</sup>, não seria uma atividade de risco, logo não haveria incidência da regra geral de responsabilidade objetiva prevista no art. 927, Parágrafo único do CC (BRASIL, 2002, n. p.). Subsistindo na visão da mesma, há incidência de responsabilidade objetiva apenas no caso em que ocorra tratamento de dados pessoais sensíveis<sup>20</sup>. Entretanto, conclui que esta seria a única janela para aplicação da responsabilidade objetiva, não mudando o fato de que o regime legal adotado pela LGPD foi o subjetivo (GUEDES; MEIRELES, 2019, p. 296).

Assim, conclui-se que os defensores do regime de responsabilidade civil subjetiva, entendem que a responsabilização deve seguir o modelo geral, visto a inexistência de previsão legal do modelo especial de responsabilização, logo há

---

<sup>19</sup> “Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável”. (BRASIL, 2018a, n. p.).

<sup>20</sup> “Art. 5º Para os fins desta Lei, considera-se: II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”. (BRASIL, 2018a, n. p.).

necessidade de verificação de culpa na conduta do agente, pois entendem que o tratamento de dados pessoais não configura atividade de risco, sustentam ainda, que não faria sentido o legislador criar tantos *standards de condutas*, se fosse para responsabilizar os agentes, independentemente de sua culpa, por final argumenta-se a necessidade de um processo de conhecimento nas situações em que necessite de uma cognição técnica específica.

### *3.5.2 Regime de Responsabilidade Civil Objetiva dos Agentes de Tratamento*

Expostos os argumentos da doutrina subjetivista, neste momento, investigar-se-á as principais premissas dos defensores da corrente objetivista. Logo, ao adotar na LGPD a existência de um regime objetivo, deve-se evitar cair no dilema de que este regime causaria empecilhos ao desenvolvimento de novas tecnologias na proteção de dados, visto sua maior probabilidade de demandas litigiosas. Ocorre que isso se trata de falso dilema, já superado na história, visto que a adoção de modelos de culpa presumida, onde se flexibiliza a comprovação da culpa, não há limitação ao desenvolvimento de novas tecnologias; ao contrário, assegura-se o pleno desenvolvimento tecnológico e industrial, sendo os custos desse modelo de responsabilização incorporados pelo mercado, sem prejuízo do ressarcimento das vítimas que suportaram o dano (MORAES; QUEIROZ, 2019, p. 128).

Partindo da premissa de que o regime de responsabilidade objetiva não é obstáculo para o desenvolvimento da indústria de dados, encontra-se na doutrina brasileira sólidos argumentos em defesa do regime analisado, dentre eles aparece Zanatta (2017, p. 188), segundo o qual a proteção de dados passa pelo fenômeno chamado de “regulação de risco”, ocasionando uma alteração no paradigma para a prevenção de danos e instrumentos regulatórios que incrementem o nível de segurança da informação e cognição de riscos por autoridades especializadas, além da imposição, pelo poder público, de um conjunto de obrigações às empresas, assim condicionando a atividade empresarial que utilize dados a comportamentos potencialmente éticos, tendo isto se traduzido no Capítulo VII da LGPD, intitulado “Da Segurança e das Boas Práticas” (ZANATTA, 2017, p. 188).

Frente a isto, em Audiência Pública realizada pela Comissão Parlamentar Especial (CPE), que analisava a LGPD em 3 de maio de 2017, a qual teve o foco no

tema “Responsabilidade Objetiva e Solidária”, Zanatta, representando o Instituto Brasileiro de Defesa do Consumidor (IDEC), evidenciou a hipossuficiência do usuário na atividade de risco que representa a coleta de dados, defendendo, assim, a responsabilidade objetiva e solidária, conforme o caso (COMISSÃO, 2018, p. 17).

A par do fenômeno da regulação do risco apresentado por Zanatta, tem-se o posicionamento de Mendes e Doneda (2018, p. 476), segundo o qual, deve-se levar em consideração, ao fixar o regime de responsabilização adequado, os riscos a direitos personalíssimos e fundamentais atrelados à atividade de tratamento de dados pessoais. Na visão dos autores, isso se transparece pelo fato da LGPD impor várias limitações ao tratamento de dados, estabelecendo bases legais para exercício da atividade, que somente poderá ser realizado nas hipóteses indicadas nos 10 incisos do art. 7 da LGPD (BRASIL, 2018a, n. p.), além de impor princípios, como da segurança que determina que no tratamento de dados haja 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, previsto no art. 6, inciso VI, da lei (BRASIL, 2018a, n. p.).

Ainda sobre o princípio da segurança, infere-se deste, a existência do dever de segurança dos agentes de tratamento ao exercer a atividade. Quanto a esse dever, Cavalieri Filho<sup>21</sup>, em 2003, já o relacionava como uma obrigação jurídica específica, dos agentes praticantes de atividade econômica reiterada, habitual e profissional, que se for violada gera o direito à indenização independente de culpa. Por força deste princípio, o Operador/Controlador competente está obrigado a fornecer as condições nas quais os riscos pertinentes à atividade de tratamento de dados não causem dano ao titular, vez que ocorrendo dano é o caso de responsabilização objetiva (CAVALIERI, 2003, p. 43).

Tais reflexões acerca da lei e os princípios por ela implementados, direcionam os autores a concluir que se optou por um regime geral de responsabilidade objetiva, relacionando a prática da atividade de tratamento de

---

<sup>21</sup> Em conclusão, tenho para mim que devemos visualizar no parágrafo único do art. 927 do novo Código Civil a mesma disciplina jurídica do art. 14 do CDC. Quem exercer atividade perigosa - entende-se, atividade habitual, reiterada, profissional - responderá objetivamente se o fizer com defeito, considerada como tal a atividade exercida sem a segurança legalmente exigida, sem a segurança legitimamente esperada (CAVALIERI FILHO, 2003, p. 43).

dados pessoais a um risco intrínseco, com potencial no nocivo aos seus titulares. Trata-se, dessa forma, de uma regulação que possui como fundamento principal a diminuição do risco, levando-se em conta que o tratamento de dados apresenta riscos inerentes aos seus titulares. Assim, justifica-se o legislador ter optado por um regime de responsabilidade objetiva, vinculando a obrigação de reparação do dano ao exercício de atividade de tratamento de dados pessoais (MENDES; DONEDA, 2018, p. 477).

Ao compreender o fenômeno risquificação (ZANATTA, 2017, p. 188), e os riscos a direitos de personalidade e liberdade intrínsecos à natureza da atividade de tratamento de dados pessoais, tem-se o posicionamento habitualmente encontrado na doutrina, exemplificado na pessoa do professor Leonardo Henrique de Carvalho Ventura (2018, n. p.), indicando que, referente ao regime adequado de responsabilidade civil, pela regra geral do direito civil brasileiro, a responsabilização seria de caráter objetivo, visto que está expresso de forma clara no parágrafo único do art. 927 do CC, que o causador do dano fica obrigado a repará-lo, independentemente de culpa nos casos em que a atividade desenvolvida pelo autor implicar, pela natureza da atividade e risco a direitos de outrem (VENTURA, 2018, n. p.).

Seguindo nessa linha argumentativa sobre o risco na atividade de tratamento de dados pessoais, há o esclarecedor parecer da CPE, formada na Câmara do Deputados em 25 de outubro de 2016, de relatoria do Deputado Orlando Silva, à qual possuía como finalidade examinar o PL nº 4.060/2012, tendo se manifestado com os seguintes termos:

A atividade de tratamento de dados pessoais constitui atividade de risco, o que atrai a incidência da responsabilidade objetiva ao agente de tratamento, ou seja, aquela segundo a qual não há necessidade de perquirir a existência de culpa para obrigar o causador do dano a repará-lo. Esta já é a regra geral do direito brasileiro para toda e qualquer atividade de risco, conforme previsto no parágrafo único do artigo 927 do Código Civil, como também constitui a base da responsabilização dos fornecedores nas relações de consumo (CÂMARA DOS DEPUTADOS, 2018, p. 41-42).

Já na visão de Bruno Miragem (2019, p. 26), é necessária uma responsabilização objetiva pelos seguintes fatores: (I) em relação ao tratamento de

dados pessoais - é necessário que se compreenda a existência de um dever de segurança imputável aos responsáveis pelo tratamento, relacionada à segurança legitimamente esperada daqueles que exercem a atividade em caráter profissional, e por esta razão presume-se que tenham a expertise suficiente para assegurar a integridade dos dados e a preservação da privacidade de seus titulares; (ii) a responsabilidade dos agentes de tratamento, decorrente do tratamento irregular dos dados pessoais do qual resulte o dano - não se deve perquirir se a falha se dá por dolo ou culpa, senão que apenas a constatação da irregularidade do tratamento é suficiente para atribuição da responsabilidade.

Conclui o autor, que as condições de imputação de responsabilidade do agente que causar dano em decorrência da atividade de tratamento de dados serão: a) a identificação de uma violação às normas que disciplinam o tratamento de dados pessoais; b) a existência de um dano patrimonial ou extrapatrimonial ao titular dos dados (MIRAGEM, 2019, p. 27). Como já demonstrado, na visão do mesmo, não se exige para a imputação de responsabilidade, a demonstração de dolo ou culpa, sendo correto compreender, que pela boa exegese da lei, somado ao risco inerente ligado a atividade desenvolvida, seria o caso de um regime de responsabilização no qual se responda objetivamente, desta forma, o titular dos dados que vier a sofrer o dano poderá demandar o operador ou controlador responsável pelo ato ilícito.

Tem-se ainda na doutrina outro fator que se deve levar em conta a favor do regime objetivo. Na visão de Schreiber (2020, p. 336), ao implantar o art. 44 - tratamento irregular -, exprime-se uma versão adaptada do conceito de defeito de serviço previsto no art. 14, parágrafo 1º do CDC. Logo, compreende-se a possibilidade de existir um “tratamento defeituoso”, frente a isto o autor fala que a LGPD emprega construção análoga, nesta matéria, àquela empregada na lei consumerista, na qual a responsabilidade dos agentes tutelados é de cunho objetivo nos casos mencionados.

Desta forma, pode-se conceber que os defensores do regime de responsabilização objetiva interpretam que, na essência, o tratamento de dados pessoais está intrinsecamente ligada a uma atividade de risco, vez que tem aptidão de causar danos materiais/morais, e violar direitos de liberdade, privacidade e personalidade. Partindo desse pressuposto, haveria incidência do parágrafo único



do art. 927 do CC, segundo o qual há obrigação de reparar o dano, independentemente de culpa, quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, em risco para os direitos de outrem (BRASIL, 2002, n. p.), sendo este o principal fundamento aos adeptos da corrente mencionada.

### *3.5.3 Um Sistema Especial de Responsabilidade Civil Objetiva Proativa em Segurança Baseado na RGPD*

Frente a já mencionada inércia legislativa sobre o regime geral previsto na legislação de dados, começa a emergir na doutrina uma nova espécie de responsabilização. Na visão de Moraes e Queiroz (2019, p. 126), o sistema de responsabilidade civil da LGPD, pautado nos arts. 42 a 45 apresenta-se como um regime especialíssimo, tendo como principal inovação legal o princípio da responsabilização de prestação de contas, previsto no art. 6, inciso X, traduzindo-se na demonstração pelo agente de tratamento que adotou medidas eficazes, além da observância e cumprimento com as normas de proteção de dados, já que o legislador pretendeu que junto com o ressarcimento, fosse prevenida a ocorrência de danos.

De acordo com os autores supracitados, a legislação brasileira de proteção, ao implementar o referido princípio, secundou o Regulamento Europeu, tendo como resultado uma quebra no paradigma em relação à responsabilização, que assim como no modelo europeu, o dever de prestação de contas assume papel fundamental. Essa nova sistemática de responsabilização é conceituada como “responsabilidade proativa”, e por tal mudança paradigmática exige-se das empresas, que utilizam dados em suas atividades econômicas, atitudes conscientes e proativas em relação ao uso e proteção destes dados. Logo, será necessário demonstrar “a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, ‘não descumprir a lei, não é mais suficiente’”. (MORAES; QUEIROZ, 2019, p. 129).

Seguindo nessa linha referente ao regime responsabilização especial pelo dever de segurança, há o posicionamento de Rafael Dresch e Lílian Stein (2020, n.

p.), para o qual, havendo tratamento de dados pessoais, caso essa atividade venha causar dano ao titular<sup>22</sup>, surge então a responsabilização do agente de tratamento. No entanto, a responsabilidade civil, nesses termos, não possuiu características do regime de responsabilidade civil subjetiva fundada na culpa, nem no modelo do regime de responsabilidade civil objetiva centrada no risco, pois o que se vislumbra é uma especial forma de responsabilidade civil objetiva, fundada na garantia da segurança no tratamento de dados pessoais (DRESCH; STEIN, 2020, n. p.).

Assim, pode-se concluir que as características inerentes deste regime especial de responsabilidade civil em questão se manifesta, principalmente, na regulação detalhada das obrigações comportamentais dos agentes de tratamento, com foco voltado ao gerenciamento de riscos, especialmente relacionado ao uso da inovação tecnológica, adaptando às especificidades da atividade de processamento de dados pessoais e aos requisitos de proteção que ele apresenta. Assim sendo, criou-se um modelo mais maduro de responsabilização civil, no qual se vai além da responsabilidade dos agentes, tendo-se em vista, especialmente, evitar danos aos titulares dos dados (MORAES; QUEIROZ, 2019, p.134).

### **3.6 Julgados Relacionados a Proteção de Dados**

Neste item, será investigado como a proteção de dados vem sendo analisada nas cortes superiores, iniciando pelo STF, visto a CF/88 já tratar da proteção dos direitos de personalidade, liberdade e autodeterminação informacional. Em seguida a pesquisa recairá sobre o STJ, já que esta é a corte de uniformização do ordenamento jurídico brasileiro. Assim, tem-se como método de pesquisa um levantamento junto aos *sites* dos tribunais mencionados, do termo “LGDP”, e pesquisas jurisprudenciais relacionadas ao objeto do presente estudo com objetivo de ver se há algo na jurisprudências sobre o regime

#### *3.6.1 Julgados do Supremo Tribunal Federal*

Pela recente entrada em vigência da LGPD, e dada a competência constitucional do tribunal, pouco se encontrou sobre questões de responsabilidade civil na busca realizada no *site* do STF. Apareceram apenas dois casos relacionados

---

<sup>22</sup> Dano em violação à Legislação ou dano por inobservância dos *standards* de conduta e *compliance*, deveres de segurança e boas práticas.

ao tema: o primeiro referente à Arguição de Descumprimento de Preceito Fundamental (ADPF) Nº 695 Medida Cautelar (MC) (SUPREMO TRIBUNAL FEDERAL, 2020, n. p.), de relatoria do Min. Gilmar Mendes, na qual se discute as especificidades do tratamento e compartilhamento de dados entre entidades do poder público.

Nesta ADPF de autoria do Partido Socialista Brasileiro, vale destacar, que o Ministro Gilmar Mendes ao proferir seu voto, em 24 de junho de 2020, nada de relevante disse sobre o tema, limitando-se a deliberar sobre e o compartilhamento de dados pessoais pelo Serviço Federal de Processamento de Dados (SERPRO) à Agência Brasileira de Inteligência (ABIN), com fundamento normativo no Decreto nº. 10.046, de 9 de outubro de 2019.

Já o segundo caso é relacionado às Ações Diretas de Inconstitucionalidade (ADI) 6387 (SUPREMO TRIBUNAL FEDERAL, 2020, n. p.) de autoria do Partido Socialista Brasileiro junto com o Conselho Federal da OAB, que possui como relatora a Min Rosa Weber. A ação trata do compartilhamento de dados pessoais entre as empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP (as chamadas Telecoms) e a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE.

Ao voto proferido em 24 de abril, a Ministra Rosa Weber nada disse sobre a responsabilidade civil dos agentes de tratamento, tendo suas principais considerações sido sobre risco do compartilhamento, destacando não haver garantias de tratamento adequado e seguro dos dados compartilhados. Tais motivos levaram a ministra a deferir medida cautelar para que o IBGE se abstinhasse de requerer os dados objeto da questão em análise.

### *3.6.2 Julgados do Superior Tribunal de Justiça*

O STJ é a corte máxima do ordenamento brasileiro em sede de jurisdição infraconstitucional, tendo a competência de uniformizar a Lei Federal em todo o território nacional. Trata-se do local ideal para localizarem-se julgados pertinentes à culpa na responsabilização dos agentes de tratamento, matéria sem previsão expressa na Constituição Federal. Entretanto, considerando o recente início da

vigência da LGPD, pode não ter havido ainda tempo para a Corte se manifestar sobre esse aspecto específico. Não obstante, há vários acórdãos sobre a proteção de dados pessoais em geral.

Em artigo doutrinário, o Ministro do STJ Ricardo Villas Bôas Cueva noticia o julgamento do Recurso Especial (REsp) 22.337-8/RS, de relatoria do ministro Ruy Rosado como tendo sido a primeira oportunidade na qual a questão da utilização de dados pessoais foi tratada pelo STJ, mediante a análise do art. 43 do CDC, que garante ao titular o acesso a seus registros, além do direito de corrigir informações existentes nestes bancos de dados. Prevaleceu a tutela consumerista do direito ao acesso e retificação dos dados, fundamentando-se a decisão do STJ na matriz constitucional de proteção à intimidade e vida privada (CUEVA, 2019, p. 2819).

Ainda segundo o CUEVA (2019, p. 2840), em 2001 o REsp 306.570 de relatoria da Ministra Eliana Calmon, que reconheceu ter o titular de conta bancária direito à privacidade em relação aos seus dados pessoais. Mais adiante, em 2010, no REsp 1.168.547/RJ, de relatoria do Ministro Luis Felipe Salomão, além de fixar-se o moderno conceito de privacidade já mencionado, inovou a Corte ao introduzir a necessidade de consentimento do titular nos casos de divulgação de informações que lhe digam respeito, vez que, o mesmo tem direito de dispor sobre suas próprias informações. Por este julgado, a tutela da privacidade passou a ter como ponto de referência o consentimento do titular nas atividades relacionadas a dados pessoais (CUEVA, 2019, p. 2840).

Já no julgamento do REsp 1.348.532/SP<sup>23</sup> de relatoria do Ministro Luis Felipe Salomão, no qual assentou-se a ilegalidade de cláusula prevista em contrato de serviço de cartão de crédito, que autorizava o banco contratante a compartilhar dados dos seus clientes com outras entidades financeiras e entidades mantenedoras de cadastros negativos e positivos de consumidores. Nestes termos, extrai-se a ementa do voto, que possui o seguinte teor:

É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros

---

<sup>23</sup> REsp 1.348.532/SP, rel. Min Luis Felipe Salomão, 4a T., j. 10.10.2017, DJe 30.11.2017.

positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada. De fato, a partir da exposição de seus dados financeiros, abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição.

Por último, tem-se como principal referência e paradigma, o julgamento do Recurso Especial 1.457.199/RS em 12/11/2014, de relatoria do Ministro Paulo de Tarso Sanseverino, no qual discutia-se a legalidade dos sistemas de *credit score*. Ao proferir seu voto, esmiuçou as questões legais e sociais relacionadas à utilização de dados pessoais no cenário nacional e internacional. Cabendo grande destaque para as considerações relacionadas à responsabilidade civil do fornecedor do serviço e responsável pelo banco de dados, asseverando que:

O desrespeito aos limites legais na utilização do sistema “credit scoring”, configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados (SUPERIOR TRIBUNAL DE JUSTIÇA, 2014, p. 1-2).

Desta forma, pode-se observar que, o STJ em relação à responsabilização civil, manifestou-se pelo regime objetivista e solidário, nos casos dos dados do titular vierem a ser utilizados em desconformidade com os preceitos legais, ensejando ainda, danos morais pela má e indevida utilização das informações pessoais do indivíduo.

Assim, verificou-se da análise jurisprudencial, que ainda não há nada em específico na corte sobre a responsabilidade civil dos agentes de tratamento. Entretanto, esta, já vem se posicionando pelo resguardo dos dados além da responsabilização objetiva nos casos de desrespeito aos direitos atrelados aos

dados dos titulares. Frente a isto, nos resta esperar o tempo hábil para que a questão em análise seja apreciada pela corte, e assim fixando entendimento jurisprudencial sobre o regime adequado na responsabilização do agente de tratamento na relação jurídica com o titular dos dados.

#### **4 CONSIDERAÇÕES FINAIS**

Pelo presente trabalho, vislumbrou-se proporcionar elucidações sobre questões relacionadas à responsabilização civil dos agentes de tratamento de dados pessoais, dando ênfase, especificamente, na análise sobre qual regime de responsabilidade vigente no ordenamento jurídico brasileiro melhor se adequa com os objetivos da LGPD.

Inicialmente, foram feitas considerações no sentido de imergir o leitor no mundo da proteção de dados pessoais, demonstrando os desdobramentos sociais decorrentes dessa nova atividade econômica, sua contextualização no cenário internacional e nacional, além dos principais conceitos e definições relacionadas à tutela jurídica dos dados pessoais.

Constatou-se que o tema se revela como um delicado desafio a ser enfrentado pelo direito contemporâneo, pois estamos a viver na era da Sociedade da Informação, onde há uma série de quebra de paradigmas em razão da tecnologia aliada a um alto grau de conectividade entre os atores sociais, ocasionando uma gigantesca produção de dados diariamente. Frente a isto, observou-se que tais dados, a depender da forma de seu tratamento, tem aptidão de revelar informações relacionadas aos direitos fundamentais de privacidade, autodeterminação informacional e livre desenvolvimento da personalidade. Logo a proteção de dados pessoais consiste na tutela jurídica para o correto uso destas informações, juntamente com a possibilidade de o titular dos dados determinar se terá seus dados tratados além da forma que seus dados serão utilizados.

Após a contextualização, passou-se a analisar a LGPD, indicando sua definição, seus fundamentos e princípios, além de apresentar as figuras do controlador, operador e encarregado e suas respectivas responsabilidades. Ficando

evidenciado que ao exercer a atividade de tratamento de dados, o agente de tratamento competente deve obedecer todos os dez princípios mencionados na lei, constatou-se ainda, que o controlador é o principal responsável na cadeia da atividade de tratamento de dados, vez que é dele a tomada de decisão sobre a finalidade dos dados, vindo o operador atuar sob as suas ordens, e responder apenas se infringidas ou atuar em dissonância com a normatização.

Em sua terceira parte, o presente trabalho teve voltou-se para um tema intrínseco do direito civil brasileiro, e assim transpassou pelos principais conceitos da responsabilidade civil no ordenamento jurídico brasileiro, apontando seus pressupostos e classificações pertinentes ao tema estudado. Observou-se que nas relações no âmbito da LGPD, o vínculo jurídico entre as partes será abundantemente extranacional, vez que aos agentes de tratamento é imputado observar as várias normativas impostas ao realizar a atividade com dados pessoais, para não acarretar dano ao titular.

Na parte seguinte, adentrou-se na questão central do presente trabalho, pois sua premissa era tentar desvendar o regime de responsabilidade estabelecido na LGPD no tocante a voluntariedade da conduta causadora do dano, se deve ser mediante a verificação de culpa, nos moldes da responsabilidade subjetiva, ou por presunção de culpa, por força do regime objetivista.

Chegou-se à conclusão de que a lei é inerte quanto à definição do regime, abrindo-se margem na doutrina para discussão. Logo, os defensores do regime de responsabilidade civil subjetiva partem dos seguintes pressupostos: tratamento de dados pessoais não configura atividade de risco, os atores respeitaram todos os standards, regras e deveres de segurança e boa governança implementadas pela lei, além da necessidade de um processo de conhecimento nas situações em que necessite de uma cognição técnica específica. Em consequência disto, os agentes terão maior liberdade no tratamento de dados, pois serão regidos pelos parâmetros gerais de responsabilidade civil existente no CC, sendo necessário verificar a culpa, o dano e o nexo de causalidade, em uma longa fase instrutória, para posterior verificação do ato antijurídico, dando ensejo ao ressarcimento de danos ao titular do dado que suportou o dano.

Do outro lado observa-se que os defensores do regime de responsabilização objetiva interpretam que o tratamento de dados pessoais está intrinsecamente vinculado a uma atividade de risco, vez que tem aptidão de causar danos materiais/morais, e violar direitos de liberdade, privacidade e personalidade, por força disto haveria incidência do parágrafo único do art. 927 do CC, segundo o qual há obrigação de reparar o dano, independentemente de culpa, quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, em risco para os direitos de outrem. Por esse prisma, verifica-se maior rigorosidade no uso dos dados, tendo como fim maior segurança e proteção do titular, juntamente com maior facilidade de ressarcimento de dano no caso de um regime geral pautado no modelo de responsabilidade objetiva.

Na pesquisa científica realizada, encontrou-se ainda uma terceira corrente doutrinária. segundo esta, a legislação brasileira de proteção de dados pessoais secundou o RGPS. Logo, o sistema de responsabilidade civil pautado nos arts. 42 a 45 da LGPD apresenta-se como um regime especialíssimo, inovando ao dispor no seu texto legal sobre o princípio da responsabilização de prestação de contas, tendo como resultado uma quebra no paradigma em relação à responsabilização. As características inerentes deste regime especial de responsabilidade civil se manifestam, principalmente, na regulação detalhada das obrigações das condutas dos agentes de tratamento, tendo como foco o gerenciamento dos riscos relacionado ao uso da inovação tecnológica, adaptando às especificidades da atividade de tratamento de dados pessoais aos requisitos de proteção tais informações necessitam, assim criando um modelo de responsabilização civil, no qual se vai além da responsabilidade dos agentes, tendo-se em vista, especialmente, evitar danos aos titulares dos dados.

O presente trabalho passou a se debruçar nas jurisprudências do Supremo Tribunal Federal e Superior Tribunal de Justiça. No STF pode-se observar a existência da ADPF 695 e da ADI 6387, entretanto não se verificou discussões ligadas especificamente ao regime de responsabilidade civil, haja vista a competência constitucional da corte, as matérias discutidas em sua maioria são relacionadas ao compartilhamento de dados no setor público.



Nos julgados do STJ, restou demonstrado que a corte possui vasta jurisprudência consolidada referente aos dados pessoais e seus desdobramentos com os direitos de privacidade, de proteção ao consumidor, além da necessidade de consentimento e compartilhamento de dados. Tendo como destaque o julgado do REsp 1.457.199/RS 2014 de relatoria do Ministro Paulo de Tarso Sanseverino, o qual está intrinsecamente conexo ao objeto do estudo, pois assevera que nos casos da utilização do dados em desrespeito aos limites legais o regime de responsabilização civil é da responsabilidade objetiva e solidária.

Por fim, chegou-se à conclusão que ao realizar uma leitura estrita da sessão sobre responsabilidade civil contida na LGPD, depreende-se que o regime escolhido foi o de responsabilização subjetiva, haja vista a necessidade de previsão expressa nos casos de responsabilização objetiva.

Entretanto, fica claro que a lei vem com o objetivo de proteger direitos e garantias fundamentais do titular, frente os riscos da atividade de tratamento de dados com fins econômicos, somando-se a isto, tem-se vasta produção doutrinária e jurisprudencial, convergindo no sentido que, sendo uma atividade de risco, há a incidência do parágrafo único 927. Logo, em última análise no contexto jurídico observado, faz-se mister optar pelo regime de responsabilidade objetiva dos agentes tratamento no âmbito da relação jurídica tratador - titular.

## 5 REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais**. A função e os limites do consentimento. Rio de Janeiro: Forense, 2019. Edição do Kindle.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Emendas Constitucionais de Revisão. Brasília, 1988. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 12 jan. 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 1990. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 25 fev. 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, 2002. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/2002/L10406compilada.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm). Acesso em: 20 fev. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018a. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 12 jan. 2021.

BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018.** 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. Brasília, 2018b. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Mpv/mpv869.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm). Acesso em: 15 fev. 2021.

CÂMARA DOS DEPUTADOS. **Comissão Especial Destinada a proferir parecer ao Projeto de Lei nº 4060/2012.** Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Sala de Comissão, 2018. Disponível em: [https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1663305&filename=](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=). Acesso em: 14 mar. 2021.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos: Direito Digital e proteção de dados pessoais**, São Paulo, 2020, v. 21, p. 163-170. Disponível em: <https://core.ac.uk/download/pdf/322682320.pdf>. Acesso em: 8 fev. 2021.

CAVALIERI FILHO, Sérgio. Responsabilidade Civil no Novo Código Civil Revista da EMERJ, v. 6, n. 24, 2003. Disponível em: [https://www.emerj.tjrj.jus.br/revistaemerj\\_online/edicoes/revista24/revista24\\_31.pdf](https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista24/revista24_31.pdf). Acesso em: 25 mar. 2021.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil.** 10. ed. São Paulo: Atlas, 2012.

COMISSÃO, Especial Destinada a Proferir Parecer ao Projeto de Lei nº 4060, de 2012 (Tratamento e Proteção de Dados Pessoais) Projeto de Lei nº 4.060, de 2012 (Apenso PLs nos 5.276/16 e 6.291/16). 2018. Disponível em: [https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1663305&filename=](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=). Acesso em: 24 fev. 2021.

CORRÊA, Leonardo. É importante não perder o foco da segurança jurídica no âmbito da LGPD. **Conjur**, 2019. Disponível em: <https://www.conjur.com.br/2019-mar-03/leonardo-correa-seguranca-juridica-ambito-lgpd>. Acesso em: 3 mar. 2021.

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

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro: Responsabilidade Civil**. 19 ed. São Paulo: Saraiva, 2005.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

DRESCH, Rafael de Freitas Valle; STEIN, Lílian Brandt. Migalhas de Proteção de Dados. Direito fundamental à proteção de dados e responsabilidade civil. **Migalhas**, 2020. Disponível em:  
<https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/336997/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil>. Acesso em: 12 fev. 2021.

GONÇALVES, Carlos Roberto. **Direito Civil brasileiro, Responsabilidade**. 7ª ed. São Paulo. Saraiva, 2011. v. 7.

GONÇALVES, Carlos Roberto. **Responsabilidade civil**. 19 Ed. Saraiva Educação SA, 2020.

GUEDES, Gisela Sampaio da Cruz. Regime de responsabilidade adotado pela lei de proteção de dados brasileira. **Caderno Especial LGPD**, p. 167-182. São Paulo: Ed, RT, 2019.

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

KAUER, Gisele. Controlador, operador e encarregado: Quem é quem na LGPD. **Infra News Telecom**, [20--]. Disponível em:  
<https://www.infranewstelecom.com.br/controlador-operador-encarregado-quem-e-quem-na-lgpd/>. Acesso em: 14 mar. 2021.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, ano 27, n. 120, nov.-dez., p. 469-483, 2018. Disponível em:  
<https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116/991>. Acesso em: 13 mar. 2021.

MIRAGEM, Bruno. A lei geral de proteção de dados (lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, v. 1009, 2019. Disponível em:  
<https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>. Acesso em: 14 mar. 2021.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *In*: **Cadernos Adenauer**, v. 3, Ano XX, 2019. Disponível em:  
<https://civilistica.emnuvens.com.br/redc/article/view/448>. Acesso em: 5 mar. 2021.

PEREIRA, Caio Mário da Silva. **Responsabilidade civil**. 3. ed. Rio de Janeiro: Forense, 1992.

PESTANA, Márcio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais)**. [20--]. Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 12 jan. 2021.

PROTECÇÃO DOS DADOS PESSOAIS. **Eur-lex**, 2014. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=CELEX:31995L0046>. Acesso em: 12 fev. 2021.

QUEIROZ, Luiz. Sai a primeira decisão judicial com base na LGPD contra uso indevido de dados pessoais. **Capital Digital**, 2020. Disponível em: <http://www.capitaldigital.com.br/sai-a-primeira-decisao-judicial-com-base-na-lgpd-contra-uso-indevido-de-dados-pessoais/>. Acesso em: 4 mar. 2021.

RUARO, Regina Linden; BUBLITZ, Michelle Dias; MACEDO, Fernanda dos Santos. A Privacy Norteamericana e a Relação com o Direito brasileiro. **Revista Jurídica CESUMAR**. Mestrado, 2013.

SCHREIBER, Anderson. **Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais**. Tratado de Proteção de Dados Pessoais . Editora Forense, 2020

SILVA, De Plácido. **Vocabulário jurídico**. 18.ed. Rio de Janeiro: Forense, 2001.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Documento: 1364998** - Inteiro Teor do Acórdão - Site certificado - DJe: 17/12/2014. Disponível em: <https://bdjur.stj.jus.br/jspui/bitstream/2011/114173/REsp1457199.pdf>. Acesso em: 3 mar. 2021.

SUPREMO TRIBUNAL FEDERAL - DF. **Medida Cautelar na arguição de descumprimento de preceito fundamental 695**. Brasília, DF, 2020. Disponível em: <https://www.conjur.com.br/dl/gilmar-manda-plenario-analise.pdf>. Acesso em: 23 mar. 2021.

SUPREMO TRIBUNAL FEDERAL. Arguição de Descumprimento de Preceito Fundamental. **ADPF 695**, 2021. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693>. Acesso em: 3 mar. 2021.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. **Processo Digital nº: 1080233-94.2019.8.26.0100**. Procedimento Comum Cível - Indenização por Dano. São Paulo, 2020. Disponível em: <https://www.conjur.com.br/dl/compartilhar-dados-consumidor-terceiros.pdf>. Acesso em: 2 jan. 2021.

VENOSA, Sílvio de Salvo. **Direito Civil: Responsabilidade Civil**. 13 ed. São Paulo: Atlas, 2013.

VENOSA, Sílvio de Salvo. **Direito civil: responsabilidade civil**. 10. ed. São Paulo: Atlas, 2010. v. IV.

VENTURA, Leonardo Henrique de Carvalho. Considerações Sobre a Nova Lei Geral de Proteção de Dados Pessoais. **Jus.com.br**, 2018. Disponível em: <https://jus.com.br/artigos/68966/consideracoes-sobre-a-nova-lei-geral-de-protecao-d-e-dados-pessoais>. Acesso em: 13 out. 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. Direito à privacidade. **Harv. L. Rev.**, v. 4, p. 193, 1890. Disponível em: [https://heinonline.org/hol-cgi-bin/get\\_pdf.cgi?handle=hein.journals/hlr4&section=31](https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/hlr4&section=31). Acesso em: 25 jan. 2021.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? **I Encontro da Rede de Pesquisa em Governança da Internet**. Rio de Janeiro, 2017.