



ESCOLA DA MAGISTRATURA DO ESTADO DO RIO DE JANEIRO

A RESPONSABILIDADE CIVIL NO TOCANTE AOS DADOS PESSOAIS, À LUZ DA  
LGPD

Larissa Alves Carneiro

Rio de Janeiro  
2022

LARISSA ALVES CARNEIRO

A RESPONSABILIDADE CIVIL NO TOCANTE AOS DADOS PESSOAIS, À LUZ DA  
LGPD

Monografia apresentada como exigência para  
conclusão de Curso de Pós-Graduação *Lato  
Sensu* da Escola da Magistratura do Estado do  
Rio de Janeiro.

Orientador:

Prof. André Roberto de Souza Machado

Coorientadora:

Prof<sup>a</sup> Mônica Cavalieri Fetzner Areal

Rio de Janeiro

2022

LARISSA ALVES CARNEIRO

A RESPONSABILIDADE CIVIL NO TOCANTE AOS DADOS PESSOAIS, À LUZ DA  
LGPD

Monografia apresentada como exigência  
de conclusão de Curso da Pós-Graduação  
*Lato Sensu* da Escola da Magistratura do  
Estado do Rio de Janeiro.

Aprovada em \_\_\_\_\_ de \_\_\_\_\_ de 2022. Grau atribuído: \_\_\_\_\_

BANCA EXAMINADORA

Presidente: Desembargador Claudio Brandão de Oliveira. – Escola da Magistratura do Estado  
do Rio de Janeiro-EMERJ.

\_\_\_\_\_

Convidado: Prof. Bruno Magalhães de Mattos– Escola da Magistratura do Estado do Rio de  
Janeiro-EMERJ.

\_\_\_\_\_

Orientador: Prof. André Roberto de Souza Machado - Escola da Magistratura do Estado do  
Rio de Janeiro –EMERJ.

\_\_\_\_\_

A ESCOLA DA MAGISTRATURA DO ESTADO DO RIO DE JANEIRO – EMERJ – NÃO APROVA NEM REPROVA AS OPINIÕES EMITIDAS NESTE TRABALHO, QUE SÃO DE RESPONSABILIDADE EXCLUSIVA DO(A) AUTOR(A).

À Deus e à minha família, por tudo  
que fazem por mim.

## AGRADECIMENTOS

A Deus, por tornar tudo possível.

Ao professor e orientador André Roberto Machado, por responder com presteza e precisão a todas as perguntas possíveis e imagináveis durante a elaboração textual e pelos precisos *insights* que enriqueceram enormemente esta produção monográfica.

À Escola de Magistratura do Estado do Rio de Janeiro, por proporcionar um ambiente ideal de estudos, reflexões e amadurecimento profissional.

Aos meus pais, Renata e Ricardo, por todo amor, carinho e dedicação; por acompanharem cada um de meus passos e por terem me ensinado a importância do estudo e por me incentivarem em todas as minhas escolhas.

A Julio, pelo amor, por estar comigo nos bons e nos maus momentos, e ser meu parceiro de vida.

A todos meus familiares pela torcida, admiração e confiança em mim. Cada incentivo se torna fundamental para aguentar seguir firme na caminhada. Principalmente dos meus avós, tios e queridos primos, Rayanne e João.

Aos amigos de longa data, pela compreensão com a falta de tempo e atenção de minha parte, e por sempre apoiarem meus desafios e conquistas.

Aos amigos e colegas especiais que a EMERJ me deu, que cada um trilhe seu caminho de prosperidade e conquistas.

A todos os professores e funcionários, desde o início da alfabetização escolar, até à EMERJ que contribuíram para minha formação acadêmica e humana.

A todos os que, com palavras e atitudes, me ajudaram a chegar até aqui.

“A esperança tem duas filhas lindas, a indignação e a coragem; a indignação nos ensina a não aceitar as coisas como estão; a coragem, a mudá-las.”

Santo Agostinho

## SÍNTESE

Diante do recente cenário de pandemia houve uma radical ampliação das atividades virtuais, isso juntamente com a entrada em vigor da LGPD, tornou ainda mais relevante compreender a importância dos dados pessoais bem como os danos decorrentes da referida Lei. A presente pesquisa científica discute a possibilidade de responsabilidade civil pelo uso, devido ou indevido, dos dados pessoais dentro do ambiente virtual sobretudo no atual contexto diante da nova Lei Geral de Proteção de Dados (LGPD). Analisar-se-á qual o regime de responsabilidade civil tem sido aplicado nos casos concretos de violação aos dados pessoais. Buscará compreender as duas grandes correntes dessa responsabilização, a que entende a responsabilização como objetiva, dispensa a comprovação da culpa, e a que entende a responsabilização como subjetiva, necessita a comprovação da culpa. Além disso, há a discussão quanto ao dano, se já é presumido, ou seja, *in re ipsa*, ou se precisa ser comprovado a corrente que compreende que é preciso que ocorra um dano direto ao titular do dado e que esse seja comprovado para ser indenizado, não basta a mera exposição dos dados no vazamento, pois somente por meio de um regime eficaz de responsabilidade civil será capaz de garantir uma tutela efetiva à proteção dos dados pessoais.

**PALAVRAS-CHAVE:** Direito Digital; Proteção de Dados; Responsabilidade Civil.



## SUMÁRIO

INTRODUÇÃO.....	10
1. A RESPONSABILIDADE CIVIL NA INTERNET.....	13
<b>1.1. Pressupostos teóricos da Responsabilidade Civil.....</b>	<b>13</b>
<b>1.2. A Responsabilidade Civil na Internet.....</b>	<b>16</b>
<b>1.3. Responsabilidade Civil nas Relações de Consumo.....</b>	<b>27</b>
2. A RESPONSABILIDADE CIVIL E A LGPD.....	32
<b>2.1. Lei Geral de Proteção de Dados Pessoais: conceitos e definições introdutórias.....</b>	<b>32</b>
<b>2.2. Responsabilidade civil na LGPD.....</b>	<b>37</b>
<b>2.3. Pressupostos da Responsabilidade Civil na LGPD.....</b>	<b>42</b>
3. A EFETIVIDADE DA INDENIZAÇÃO DECORRENTE DA RESPONSABILIDADE CIVIL NA ÁREA DE PROTEÇÃO DE DADOS.....	48
<b>3.1. Responsabilidade Civil do Controlador e do Operador de Dados.....</b>	<b>48</b>
<b>3.2. Responsabilidade Civil Objetiva nos casos de vazamento de dados.....</b>	<b>54</b>
<b>3.3. Responsabilização se o dano causado ao titular de dados for comprovado.....</b>	<b>60</b>
<b>3.4. Casos de vazamento de dados e a atuação dos Tribunais Brasileiros frente à Responsabilidade Civil na Lei Geral de Proteção de Dados.....</b>	<b>65</b>
<b>3.5 A Responsabilidade Civil na prática de acordo com as Lei de Dados Pessoais Internacionais.....</b>	<b>73</b>
CONCLUSÃO.....	77
REFERÊNCIAS.....	80

## SIGLAS E ABREVIATURAS

ANPD – Autoridade Nacional de Proteção de Dados  
Art. – Artigo  
CEDIS - IDP – Centro de Direito, Internet e Sociedade  
CNPD – Comissão Nacional de Proteção de Dados Pessoais  
CRFB/88 – Constituição da República Federativa do Brasil de 1988  
CPC – Código de Processo Civil  
CPF – Cadastro de Pessoa Física  
CC – Código Civil  
CDC – Código de Defesa do Consumidor  
DJe – Diário da Justiça Eletrônico  
Dr. – Doutor  
DPO – *Data Protection Officer*  
DPDC – xxxx  
Ex-Min. – Ex-Ministro  
GDPR – *General Data Protection Regulation*  
ICP – Inquérito Civil Público  
IDP – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa  
LC – Lei Complementar  
LGPD – Lei Geral de Proteção de Dados  
Min. – Ministro  
MP – Ministério Público  
MPDFT – Ministério Público do Distrito Federal e Territórios  
OAB – Ordem dos Advogados do Brasil  
P. – Página  
PEC – Proposta de Emenda à Constituição  
PROCOB / SA – xxxx  
RE – Recurso Extraordinário  
Red. – Redator Rel. – Relator Res. – Resolução  
Resp – Recurso Especial  
RG – Registro Geral  
RIPD – Relatório de Impacto a Proteção de Dados  
SENACON – Secretaria Nacional do Consumidor  
STF – Supremo Tribunal Federal  
STJ – Superior Tribunal de Justiça  
TAC – Termo de Ajustamento de Conduta  
TJRJ – Tribunal de Justiça do Estado do Rio de Janeiro  
TRF – Tribunal Regional Federal  
TCU – Tribunal de Contas da União  
TJDFT – Tribunal de Justiça do Distrito Federal e Territórios  
URL – *Uniform Resource Locator*

## INTRODUÇÃO

A presente pesquisa científica discute a possibilidade de responsabilidade civil pelo uso, devido ou indevido, dos dados pessoais dentro do ambiente virtual sobretudo no atual contexto diante da nova Lei Geral de Proteção de Dados (LGPD). Procura-se demonstrar que a falta de cuidado no tratamento e uso dos dados pessoais gera consequências ao titular do dado violado, tais como o desrespeito ao seu direito à privacidade e a dignidade da pessoa humana, por isso, é importante apreciar se essas consequências são realmente passíveis de serem medidas e quantificadas em uma indenização por dano moral.

Diante do recente cenário de pandemia e isolamento social, houve uma drástica ampliação das atividades virtuais. Este fator, juntamente com a entrada em vigor da LGPD, tornou ainda mais relevante compreender a importância da proteção dos dados pessoais, os perigos da internet, bem como a responsabilidade civil por trás dos danos decorrentes da referida Lei.

A quantidade de ações com escopo indenizatório, com base na responsabilidade civil de fornecedores que tratam ou lidam com dados pessoais, ou seja, quase todas as empresas, de microempresas a multinacionais, sofreu um aumento vertiginoso. Com isso, a todo momento surgem novas situações de violações de dados pessoais que ensejam proteção legal, demarcando a necessidade de uma lei referencial que busque alcançar uma cultura de proteção de dados no Brasil para viabilizar a devida salvaguarda dos dados pessoais no país.

A Constituição Federal assegura diversos direitos aos indivíduos como à privacidade, à intimidade e a dignidade da pessoa humana, que podem ser feridos com o uso indevido dos dados pessoais. Do mesmo modo, a Constituição Federal também assegura como direito fundamental a Proteção de Dados Pessoais, através da promulgação da Emenda Constitucional 115/2022.

O tema recentemente passa a ser regulado pelo ordenamento jurídico pátrio, porém, ainda gera muitas dúvidas quanto a sua aplicabilidade e às consequências da nova Lei na prática, diante disso, favorece as seguintes reflexões: é possível indenização por dano moral diante de um caso de violação de dados pessoais? Quais os pressupostos da Responsabilidade civil na LGPD? Qual regime de responsabilidade civil tem sido aplicado na prática da LGPD?

O direito à proteção de dados pessoais é recente e controvertido tanto na doutrina quanto na jurisprudência e merece atenção, uma vez que sempre é delicada a intervenção do Poder Judiciário nas relações econômicas e sociais.

Para melhor compreensão do tema, busca-se apresentar o conceito de dados pessoais, o que é um tratamento de dados e as sanções previstas na Lei Geral de Proteção de Dados, tal esforço visa compreender como essas novas tutelas foram surgindo e sendo reivindicadas ao longo dos anos, bem como despertar a atenção para a possibilidade de indenização por danos morais aos titulares dos dados pessoais violados, pois além da violação de seus direitos, os dados pessoais têm um altíssimo valor econômico no mundo atual.

Inicia-se o primeiro capítulo do trabalho apresentando a repercussão da entrada em vigor da Lei Geral de Proteção de Dados, bem como seus conceitos básicos que se relacionam com a responsabilidade civil do tema, como “dados pessoais”, “titulares de dados”, “tratamento de dados”, “sanções administrativas” previstas na lei. Além disso, é feita uma análise de como as mudanças trazidas com a internet atribuíram novas características e peculiaridades a responsabilidade civil, este exame é realizado a partir da investigação do regime de responsabilidade civil que a LGPD prevê, de modo a traçar um paralelo desta com a responsabilidade civil do Código de Defesa do Consumidor.

Segue-se ponderando, no segundo capítulo, as responsabilizações e reparações de danos que existem por trás da Lei Geral de Proteção de Dados, buscou-se investigar qual é o regime de responsabilidade civil que a Lei prevê, se é objetiva ou subjetiva, e se os danos morais decorrentes da indevida utilização de dados pessoais são considerados *in re ipsa* ou se necessitam de comprovação.

Além disso, será analisado se as empresas serão responsabilizadas diante de um caso de vazamento de dados, mesmo quando tiverem feito o tratamento dos dados pessoais de forma correta, ou se só em casos que houver irregularidade no tratamento de dados feito pela empresa.

A responsabilidade civil na LGPD é tema extremamente importante de ser debatido, envolvendo diferentes pressupostos e vertentes, por isso, somente por meio de um regime eficaz de responsabilidade civil haverá possibilidade de garantir uma tutela efetiva à proteção dos dados pessoais. Com o intuito de analisar o tema e estabelecer diretrizes para a viabilidade da LGPD na prática, além de buscar conhecer os pressupostos teóricos da responsabilidade civil no ordenamento jurídico brasileiro, esse capítulo analisará os conceitos e definições de grande relevância para a Lei de Proteção de Dados, de modo a explorar a responsabilidade dos agentes de tratamento de dados pessoais, prevista na própria lei.

O terceiro capítulo busca compreender o quanto do regime de responsabilidade civil decorrente da LGPD tem sido aplicado nos casos concretos. Para tal, primeiramente deve ser observado se o dano a ser reparado é patrimonial ou extrapatrimonial, o que fará grande diferença na hora de requerer o ressarcimento. Em seguida, analisar-se-á os diferentes papéis

do controlador e do operador de dados, e suas respectivas responsabilidades dentro do processo de tratamento de dados.

Além disso, para responder a questão-problema exposta acima, é preciso compreender as duas grandes correntes dessa responsabilização: A primeira, que entende a responsabilização como objetiva, isto é, dispensa a comprovação do dano, de modo que o simples incidente de vazamento de dados já comprova o dever de indenizar, ou a segunda corrente, que compreende que é necessário um dano direto ao titular do dado e que esse seja comprovado para ser indenizado, logo, não basta a mera exposição dos dados no vazamento.

Para reforçar a pesquisa, também será feita uma análise de decisões dos Tribunais brasileiros acerca dos casos de violação dos dados pessoais, antes e posterior à vigência da LGPD, bem como um estudo comparativo com as legislações internacionais sobre o tema, e como a responsabilidade civil decorrente delas tem sido aplicada na prática em outros países.

A pesquisa é desenvolvida pelo método descritivo e por investigação bibliográfica, uma vez que o pesquisador pretende fazer uma investigação na nova Lei abordada, e nas responsabilizações decorrentes dela, para analisar o objeto da pesquisa, com o fito de compreender a responsabilidade civil e a violação de dados pessoais.

Para tanto, a abordagem do objeto desta pesquisa jurídica é necessariamente qualitativa, porquanto o pesquisador pretende se valer da bibliografia pertinente à temática, além de uma análise da legislação em si e da jurisprudência que começa a existir tratando da LGPD.

## 1. A RESPONSABILIDADE CIVIL NA INTERNET

A vida em sociedade pressupõe a existência de vários aspectos volitivos, como condutas, comunicações, estabelecimento de sociedades, pactuação de negócios jurídicos, e em meio a esse conglomerado de relações jurídicas surge a necessidade de se estabelecer sanções para descumprimento de expectativas, bem como proteger os atos e comportamentos que estejam em consonância com o ordenamento jurídico.

Diante disso, o presente capítulo analisa os pressupostos teóricos da responsabilidade civil no ordenamento jurídico brasileiro. Posteriormente, será abordada a responsabilidade civil na internet e suas especificidades no ambiente digital. Por fim, é feita uma análise da responsabilidade civil dentro da área consumeirista no ambiente digital.

### 1.1 Pressupostos teóricos da Responsabilidade Civil

Primeiramente, é importante ressaltar que o ferimento de expectativas ou dos negócios jurídicos pode ser decorrer de atos lícitos ou ilícitos, por ações ou omissões, que lesionam expectativas legítimas. Nesse diapasão, é necessária essa breve abordagem, que não visa exaurir o instituto da responsabilidade civil, mas tão somente traçar conceitos básicos para a análise do tema proposto.

Diante disso, as duas principais áreas da responsabilidade civil que serão abordadas nessa pesquisa, para a posterior análise da mesma dentro da Lei Geral de Proteção de Dados, são a contratual e a extra-contratual, como será visto a seguir.

Nessa linha de raciocínio, a responsabilidade civil pode ser conceituada como um dever de reparar ou compensar danos causados por atos lícitos ou ilícitos. Falar em responsabilidade civil significa reger as consequências de uma lesão com interesse jurídico. Esse instituto visa reparar os danos para restituir o *status quo ante*, ou seja, possibilitar o retorno à situação fática anterior à ocorrência do ato que originou os danos, se isso for possível.

Nesse contexto, Maria Helena Diniz<sup>1</sup> assevera:

A responsabilidade civil pressupõe uma relação jurídica entre a pessoa que sofreu o prejuízo e a que deve repará-lo, deslocando o ônus do dano sofrido pelo lesado para outra pessoa que, por lei, deverá suportá-lo, atendendo assim à necessidade moral, social e jurídica de garantir a segurança da vítima violada pelo autor do prejuízo. Visa, portanto, garantir o direito do lesado à segurança, mediante o pleno ressarcimento dos

---

<sup>1</sup> DINIZ, Maria Helena. *Curso de direito civil brasileiro*. 23. ed. refor. V. VII. São Paulo: Saraiva, 2009, p. 7 e 8.

danos que sofreu, restabelecendo-se na medida do possível *o status quo ante*, logo, o princípio que domina a responsabilidade civil na era contemporânea é o da *restitutio in integrum*, ou seja, da reposição completa da vítima à situação anterior à lesão, por meio de uma reconstituição natural, de recurso a uma situação material correspondente ou de indenização que represente do modo mais exato possível o valor do prejuízo no momento e seu ressarcimento, respeitando assim, sua dignidade.

É necessário abordar que a imputação da responsabilidade civil não tem por finalidade o enriquecimento indevido do lesado, tampouco a dilapidação do patrimônio do agente causador do dano. A intenção é restabelecer o equilíbrio violado, respeitando o princípio da razoabilidade.

A responsabilidade civil, quanto ao fato gerador, pode ser classificada em contratual e extracontratual, esses dois tipos de responsabilidade civil serão mais citados na análise da responsabilidade civil no âmbito da LGPD exposta nos próximos capítulos, contudo, faz-se válida apresentar definições de caráter introdutório

A primeira, a responsabilidade civil contratual, se origina por haver uma relação jurídica anterior entre os envolvidos, no qual um deles descumpre total ou parcialmente a avença. O contrato é a fonte do dever jurídico, ele já define o comportamento dos contratantes e o dever específico a cuja observância ficam adstritos. Por isso, baseia-se no contrato bem como nos artigos 389, 403 e 404 do Código Civil<sup>2</sup>, para identificar e fazer cumprir as suas responsabilizações, bem como as indenizações por perdas e danos causados.

Já a responsabilidade civil extracontratual surge quando um indivíduo viola um dever jurídico sem que haja um vínculo anterior com a pessoa que sofreu o dano. Neste caso, o referido dever jurídico estará previsto no ordenamento, e não no contrato, como os arts. 186, 187 e 927 do Código civil<sup>3</sup>, que disciplinam o ato ilícito e o dever de indenizar.

A responsabilidade civil também pode ser dividida como objetiva e subjetiva. Cavalieri Filho<sup>4</sup> ensina que “a ideia de culpa está diretamente ligada à responsabilidade, por isso que, em regra, ninguém pode sofrer punição legal sem que tenha faltado, no mínimo, com o dever de cautela em seu agir”. De acordo com a teoria clássica, o principal pressuposto da responsabilidade civil subjetiva é a culpa.

Pela responsabilidade civil subjetiva, o indivíduo causador do injusto só terá a imputação do dever de indenizar em seu desfavor se ficar provado que ele agiu com culpa, em sentido amplo, dolo ou culpa, em sentido estrito. Esta é a teoria adotada pelo art. 186 do Código

---

<sup>2</sup> BRASIL. *Código Civil*. 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: 23 mai. 2021.

<sup>3</sup> Ibid.

<sup>4</sup> CAVALIERI FILHO, Sérgio. *Programa de responsabilidade civil*. 9. ed. São Paulo: Atlas, 2009, p. 16.

Civil<sup>5</sup>.

Já na responsabilidade civil objetiva não há a necessidade da presença do elemento culpa. Esta poderá até existir no caso concreto, mas não terá relevância para a responsabilização do indivíduo causador da lesão.

Maria Helena Diniz<sup>6</sup> assevera que “é irrelevante a conduta culposa ou dolosa do causador da perda, uma vez que bastará a subsistência do nexos causal entre o agravo sofrido para que haja o dever de indenizar. [...] A obrigação de indenizar, em regra, não ultrapassa os limites traçados pela conexão causal”

Uma das teorias desenvolvidas para explicar a responsabilidade objetiva é a denominada teoria do risco. Ela está relacionada à cognição de que algumas pessoas, pela natureza das atividades praticadas, se predispõem a causarem danos, e por isso, caso eles se concretizem, devem ser reparados, ainda que não haja culpa. A responsabilidade civil é composta pela conduta, pela culpa/dolo e pelo nexos de causalidade, como será visto a seguir.

A conduta é o ato humano, comissivo ou omissivo ao qual surgem efeitos jurídicos quando tem importância para o ordenamento. Já para a culpa, em sentido amplo, é necessário que o agente atue por ação ou omissão voluntária, ou negligência, imprudência ou imperícia - culpa em sentido estrito.

O Dano, por sua vez, segundo Cavalieri Filho<sup>7</sup>:

Conceitua-se, então, o dano como sendo a subtração ou diminuição de um bem jurídico, qualquer que seja a sua natureza, quer se trate de um bem patrimonial, quer se trate de um bem integrante da própria personalidade da vítima, como a sua honra, a imagem, a liberdade, etc. Em suma, dano é lesão de um bem jurídico, tanto patrimonial como moral, vindo daí a conhecida divisão do dano em patrimonial e moral.

Por fim, o nexos de causalidade é o vínculo entre a conduta - ação ou omissão - e o fato que gerou a lesão, ou seja, uma relação entre o acontecimento e o comportamento que o produziu, sua causa.

Partindo desses pressupostos do instituto da Responsabilidade Civil no direito atual, será analisada a responsabilização dentro do ambiente virtual e suas peculiaridades, bem como nas relações de consumo.

---

<sup>5</sup> BRASIL, op.cit., nota 2.

<sup>6</sup> DINIZ, op. cit., p. 130 a 132.

<sup>7</sup> CAVALIERI FILHO, op. cit., p. 71.



## 1.2 A Responsabilidade Civil na Internet

A Responsabilidade Civil na internet é um tema bastante discutido e diante do recente cenário de pandemia e isolamento social, aradical ampliação das atividades virtuais e maximização da vida online, houve grande crescimento da ocorrência de problemas e crimes virtuais, ganhando ainda mais destaque a responsabilização nas redes sociais.

Nesse contexto, aumenta de forma abrupta a quantidade de ações com escopo indenizatório que têm como objeto crimes contra honra no ambiente virtual ou indenizações por danos morais causados nas redes sociais, e ensejam a responsabilidade civil de usuários e provedores. Há aumento também do pleito de responsabilização de fornecedores de produtos e serviços online, previstos no Código de Defesa do Consumidor.

A internet não é mais vista como uma “terra sem lei”, e cada vez mais os internautas conhecem e reivindicam seus direitos no ambiente online. O mundo virtual na realidade é um prolongamento do mundo real e, por isso, precisa de normas para regulamentar os fatos jurídicos que nele ocorrem.

A internet tem proporcionado um maior espaço para a conexão entre grupos, além da dinamização da circulação de informações, e com isso uma maior ação coletiva<sup>8</sup>, pois amplia a arena de debate e a circulação de informações. Porém, no novo cenário, observam-se coisas que, se antes causavam algum espanto, hoje são curtidas e compartilhadas, o que pode acenar para uma forte intolerância dentro da sociedade. Contudo, surge também uma nova arena para a incidência de danos extrapatrimoniais, com o aumento da comunicação entre internautas, ampliam-se os riscos.

Como visto, no ano de 2012, a falta de legislação específica no país dificultou a apuração dos crimes virtuais, uma vez que as leis aplicadas eram as mesmas dos crimes de forma geral. Dessa forma, tornava-se muito difícil a identificação dos sujeitos e a obtenção de provas para a condenação criminal quanto aos crimes virtuais.

A partir de 2014, houve a criação da lei para regulamentar este tipo de atividade, ela ficou conhecida como “Marco Civil da Internet”<sup>9</sup>. Ele surgiu com uma grande campanha, permitindo, de forma inovadora, o debate e contribuição popular em sua criação por meio de um site.

Antes do Marco Civil, haviam duas leis que tratavam de assuntos na internet, porém

---

<sup>8</sup> RECUERO, Raquel. *Redes Sociais na Internet*. Porto Alegre: Sulina, 2009, p. 191.

<sup>9</sup> BRASIL. *Lei nº 12.965*, de 23 de abril de 2014. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm)>. Acesso em: 26 mai. 2021.

de forma muito mais restrita, a Lei Azeredo<sup>10</sup> e a Lei Carolina Dieckmann<sup>11</sup>. Essas iniciativas regulatórias, sobretudo o Marco Civil da Internet (Lei nº 12.965/2014) surgiram com o propósito de prover mecanismos direcionados ao reequilíbrio das relações levadas a efeito no plano virtual.

Quando foi criado, em 2014, o “Marco Civil da Internet” possuía a finalidade de acabar com a censura e a remoção de textos, desde que não viole o direito dos outros<sup>12</sup>. Além disso, aborda a ideia de que a internet pertence a todos em uma escala global, e não apenas a um país, sendo uma ferramenta utilizada para várias atividades, exercendo sempre uma finalidade social, na qual a coletividade expõe opiniões e onde os direitos humanos devem ser respeitados, e todos podem e devem exercer sua cidadania<sup>13</sup>.

A nova lei tratou de diversas questões como os direitos e garantias dos usuários, neutralidade da rede, retirada de conteúdo lesivo, guarda de registros e responsabilidade civil. Porém, mesmo após a criação do Marco Civil, muitos outros pontos relacionados à internet continuam sendo debatidos, como quanto aos conteúdos ofensivos postados.

No tocante ao provedor de conexão, segundo o art. 18 do Marco Civil<sup>14</sup>, ele não tem nenhuma responsabilidade pelos danos decorrentes de conteúdos gerados por terceiros. A função do provedor é de ser um mero transportador dos dados dos usuários, por isso não pode responder pelo que é passado através deles.

Já os provedores de aplicação, são aqueles que fornecem os serviços de internet, também é previsto na Lei em seu artigo 19. Esse é o caso das redes sociais, o usuário do provedor será o único responsabilizado pelo fato, num primeiro momento. Indaga-se se o provedor não teria que analisar o conteúdo que passa por sua estrutura, contudo, de acordo com o Marco Civil entende-se que não, conforme o seu art. 9º, parágrafo 3º, que veda que os provedores monitorem, filtrem e analisem as informações<sup>15</sup>, porém, essa posição já é mitigada

---

<sup>10</sup> BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112735.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112735.htm)>. Acesso em: 26 mai. 2021.

<sup>11</sup> BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm)>. Acesso em: 26 mai. 2021.

<sup>12</sup> Hoje em dia essa questão ganha outro contorno, não é o tema do nosso presente trabalho, mas é muito discutido até que ponto os provedores de internet podem fazer censuras a conteúdos publicados em sua plataforma, como pode ser visto na Medida Provisória 1068/2021,. O assunto ganhou destaque desde a MP das Fake News e hoje, através do Projeto de Lei 2630/2020.

<sup>13</sup> ARAUJO, Adriana Baker Goveia.; WESTINEBAID, Ana Augusta R. Uma análise jurídica sobre o marco civil da internet. *Colloquium Socialis*, Presidente Prudente, v. 01, n. Especial, p.655-661 jan/abr 2017. Disponível em: <<http://www.unoeste.br/site/enep/2016/suplementos/area/Socialis/Direito/UMA%20AN%20C3%81LISE%20JURIDICA%20SOBRE%20O%20MARCO%20CIVIL%20DA%20INTERNET.pdf>> Acesso em: 26 mai. 2021.

<sup>14</sup> BRASIL, op. cit., nota 9.

<sup>15</sup> CAPANEMA, Walter Aranha. A responsabilidade civil na Internet: Uma Análise da Lei 12.965/2014. *Revista da EMERJ*, Rio de Janeiro, v. 20, n. 78, p. 107 - 123, Janeiro/Abril. 2017.

como será dito adiante.

Passando a uma análise desse dispositivo, por exemplo, observa-se que ele é muito contestado quanto à responsabilidade civil do provedor, por ser considerado como injusto em privilegiar o direito à liberdade de expressão, sobrepondo-o aos outros direitos de igual hierarquia. O artigo 19<sup>16</sup> não veda a solução extrajudicial de remoção de conteúdos de ódio pelo provedor, porém, ao limitar sua responsabilidade, flexibilizou a obrigação desses que não quiserem atuar de forma mais ativa nos casos.

O que acontecia anteriormente, nesses casos, é que a partir do momento que o provedor tivesse ciência do ilícito ou de alguma denúncia de usuários, deveria, primeiramente, tentar resolver diretamente a questão de acordo com as regras internas do site e o ordenamento jurídico do país, principalmente nos casos de publicações que incluam discursos de ódio.

Em seguida, o próximo passo seria prosseguir à abertura de um procedimento administrativo interno, que garanta o contraditório e ampla defesa a quem for denunciado, para possibilitar, assim, uma decisão no final. Caso alguma das partes discorde dessa decisão administrativa, orienta-se que busque o Poder Judiciário para se insurgir. Evidentemente nem todos os provedores agem dessa forma, trata-se apenas de uma prática comum por parte deles, sobretudo antes da regulamentação do tema através do Marco Civil<sup>17</sup>.

Se anteriormente os provedores se responsabilizavam e intermediavam eventuais conflitos existentes em sua plataforma, sob pena de serem responsabilizados solidariamente junto com seus emissores, agora, com a nova Lei, houve a mudança de responsabilidade. Ou seja, no caso de se manterem inertes, transferirão para a vítima a obrigação de sanar uma eventual conduta ilícita na internet. Essa por sua vez, terá que buscar o Poder Judiciário. Com o abarrotamento do Judiciário, essa mudança deixou as vítimas mais desprotegidas quanto aos crimes de ódio na internet, por exemplo.

Antes do advento da Lei nº 12.965/2014, havia uma divergência<sup>18</sup> sobre o assunto, mas o STJ<sup>19</sup> compreendia a responsabilidade dos provedores de internet como sendo subjetiva, era configurada com a mera notificação do provedor, ou seja, ele era responsável solidariamente com aquele usuário que gerou o conteúdo ofensivo.

Podendo a notificação ser até extrajudicial, e o provedor só responderia se fosse

---

<sup>16</sup> BRASIL, op. cit., nota 9.

<sup>17</sup> Ibid.

<sup>18</sup> Ibid.

<sup>19</sup> Esse entendimento foi aplicado pela Quarta Turma ao julgar recurso na demanda entre um provedor e uma jovem que se sentiu ofendida por publicações na internet (REsp 1.512.647), no sentido de que o provedor de aplicação precisa ser notificado judicialmente para que se configure alguma responsabilidade pela veiculação de conteúdo ofensivo.

negligente com a denúncia, uma vez feita a denúncia ele tinha que agir, assim, do contrário, seria responsabilizado por aquele conteúdo. Além disso o conteúdo ofensivo poderia ser de qualquer natureza, e não apenas sexual.

Como pode ser visto, antes o STJ entendia como uma responsabilidade subjetiva mas tinha muito menos requisitos do que com a vinda do Marco Civil da Internet, com ele a responsabilidade do provedor só começa após a notificação judicial. Sendo assim, a responsabilidade do provedor ficou até mais restrita, não havendo a quantidade de requisitos que essa nova lei introduziu, como por exemplo, a necessidade da notificação por meio de ordem judicial, a menos que o conteúdo seja de nudez ou sexual.

Ressalta-se que essa questão ainda se encontra em debate no Supremo atualmente, pois se o dispositivo determina a responsabilização dos provedores apenas aos atos judiciais de remoção, ainda não se construiu um consenso se isso seria violador ou não dos direitos constitucionais, como o Direito à imagem e à privacidade. O tema segue sendo debatido no Recurso Extraordinário nº 1.037.396, que discute a constitucionalidade ou não do art.19 do Marco Civil da Internet e a possibilidade de se condicionar a retirada de perfil falso ou tornar indisponível o conteúdo apontado como ofensivo, somente após a ordem judicial específica.

Observa-se que, com o Marco Civil, criou-se uma proteção intensa para as sociedades empresárias que administram os sites e redes sociais, reduzindo, em contrapartida o grau de proteção aos usuários que a jurisprudência brasileira já vinha fixando. Conforme expresso no artigo 19 do Marco Civil<sup>20</sup>, o descumprimento da decisão judicial passa a ser uma condição necessária para que os provedores sejam responsabilizado<sup>21</sup>.

No caso da remoção de difamações e ofensas na Internet, esta só é obrigatória após determinação judicial, e não basta mais a mera notificação do ofendido para a retirada, como era possível anteriormente. Passa-se a ter a possibilidade de retirada de conteúdo repetitivo sem necessidade de nova ordem judicial caso a justiça já tenha determinado a remoção do mesmo conteúdo anteriormente e ele ressurgir, nesse caso, os provedores têm 48 horas para efetuar a remoção, mediante mera notificação.

Vale ressaltar a importância de mecanismos internos de solução extrajudicial dos conflitos no meio digital, de forma que seria mais célere e proporcional a cada caso por meio de uma autorregulação eficaz, presentes em diretrizes de “Termos de Uso” das próprias

---

<sup>20</sup> BRASIL, op. cit., nota 9.

<sup>21</sup> VAINZOF, Rony. Da responsabilidade por danos decorrentes de conteúdo gerado por terceiros. In: Del Masso, Fabiano; Abrusio, Juliana; Filho, Marco Aurélio Florêncio (coords.). *Marco Civil da internet lei 12.965/2014*. São Paulo: Revista dos Tribunais. 2014.

plataformas de serviços.

Diante de um caso de crime de ódio nas redes sociais, por exemplo, para que seja removido e punido o emissor é necessário que haja a denúncia, que pode ser feita por qualquer pessoa. Primeiramente, ao se deparar com um caso de crime cibernético deve-se guardar todas as provas e indícios possíveis. Por isso, é extremamente importante a captura de fotos das denúncias ou “*prints screens*”. Em seguida, o procedimento correto é registrar as denúncias com a maior riqueza de detalhes possível e não compartilhar ou replicar comentários ofensivos ou que incitem ao crime.

Quanto a denúncia, esta pode ser feita no próprio site em que foi proferida a mensagem, ou se não tiver tal opção, existe o site “SaferNet Brasil”<sup>22</sup>, que recolhe denúncias anônimas relacionadas a crimes de pornografia infantil, racismo, apologia e incitação a crimes contra a vida. Outra opção para fazer a denúncia é o Canal do Cidadão do Ministério Público Federal, que recebe denúncias de diferentes tipos, inclusive cibercrimes. Nele, a pessoa pode optar por manter os seus dados em sigilo ou não, e a recomendação da Procuradoria-Geral da República é que os cidadãos apresentem o maior número de provas, justamente para que o processo possa ter seu objetivo alcançado.

Sendo assim, a responsabilização de indivíduos que causem danos extrapatrimoniais na internet é um tema muito delicado mas que precisa ser debatido, somente com as denúncias, os avanços tecnológicos, o Governo e as instituições privadas, poderá haver uma identificação mais precisa e que gere responsabilização imediata aos indivíduos nas redes digitais.

Iniciativas como a criação do Marco Civil da Internet, surgiram visando promover mecanismos direcionados ao reequilíbrio das relações levadas a feito no plano virtual. E é exatamente sobre esse prisma que o art. 19 é visto como inconstitucional, pois exige da parte mais vulnerável que ela recorra a via judicial para ter seu pleito direcionado aos provedores de comunicação. Além disso, as redes sociais virtuais criaram um novo formato para armazenar dados, tratam-se de banco de dados de caráter pessoal a serviço do caráter privado, cujos interesses econômicos são predominantes, mas permanece a obrigação de respeitar a Dignidade da pessoa humana e a Liberdade de Expressão<sup>23</sup>.

No tocante mais especificamente à responsabilidade civil na internet, o Marco Civil não regula todos os casos de responsabilização, mas apenas os casos relacionados com os

---

<sup>22</sup> SAFERNET. *Safernet Brasil*. 2005. Disponível em: <<https://new.safernet.org.br/content/institucional>>. Acesso em: 10 jun. 2021.

<sup>23</sup> MARTINS, Guilherme Magalhães. Vulnerabilidade e responsabilidade Civil na Internet: a inconstitucionalidade do artigo 19 do Marco Civil. *Revista de Direito do Consumidor*. v. 137/2021, Set - Out / 2021. Rio de Janeiro, p. 33 a 59.

provedores diante dos danos decorrentes de conteúdos criados por terceiros. O Marco Civil busca promover qualquer papel que os intermediários do conhecimento e informação em circulação na Internet possam desempenhar na preservação de direitos. A premissa fundamental é a de que os intermediários, como os sites YouTube e Facebook, não devem ter qualquer penalidade pela razoabilidade e responsabilidade dos seus usuários, pois isso violaria a liberdade de expressão.

Os provedores de internet são pessoas jurídicas classificadas de 2 formas, segundo o art. 5º do Marco Civil<sup>24</sup>: podem ser “de conexão”, são aqueles que prestam serviço, geralmente remunerado, de permitir o acesso do usuário à Internet, ou podem ser “de aplicação” - são todas as funcionalidades que existem na Internet, como sites, aplicativos, serviços e jogos, podendo ser gratuitos ou remunerados através de publicidade ou venda de dados dos usuários.<sup>25</sup>

O provedor de conexão à internet tem apenas a função de transporte dos dados dos usuários. Logo, não responde pelo conteúdo da comunicação que realiza, conforme expõe o art. 18 do Marco Civil<sup>26</sup>. Além disso, a referida lei deixa claro que caso o dano seja causado por terceiro, o provedor está isento de responsabilidade.

Já a responsabilidade civil do provedor de aplicação é regulamentada nos artigos 19, 20 e 21 do Marco Civil<sup>27</sup>. Nos dois primeiros, há a regra geral, e a responsabilidade do servidor só surgirá na hipótese de não cumprimento de uma ordem judicial de indisponibilidade do conteúdo. Porém, tal *mandamus* precisa corresponder a dois requisitos: (i) ser específico, ou seja, indicar precisamente qual o conteúdo lesivo; e (ii) conceder prazo razoável para a indisponibilização do mesmo.

Outro ponto relevante nessa determinação / processo judicial é que a lei não exige que o ofendido indique o endereço na internet (URL) exato em que está hospedado o material. A indicação é apenas recomendada. O motivo é a existência de conteúdos, como jogos onlines e aplicativos, que não estão disponíveis nos modos tradicionais de endereço. Há também a possibilidade de ocorrência de endereço dinâmico: uma informação que estava na página principal de um site de jornal, em pouco tempo se desloca para outra página do site. Ressalta-se que a exigência do URL constitui uma formalidade excessiva, pois facilita a nulidade da decisão que determinou a indisponibilidade do conteúdo em virtude de simples erro material, desencadeado por eventual acréscimo ou retirada de algum caractere.

---

<sup>24</sup> BRASIL, op. cit., nota 9.

<sup>25</sup> CAPANEMA, op. cit.

<sup>26</sup> BRASIL, op. cit., nota 9.

<sup>27</sup> Ibid.

Outro fator muito relevante na hora de avaliar um dano na internet é não se esquecer do tamanho de sua dimensão e facilidade de circulação: um dia de exposição da ofensa nas redes pode ser suficiente para trazer uma grande propagação da notícia e causar gravíssimos constrangimentos.

Diante disso, o tempo que os provedores têm para retirarem esses conteúdos do ar após a decisão judicial também é debatido, e por mais que haja a demanda de uma rápida ação por parte dos servidores, quanto mais tempo o conteúdo se mantiver disponível nas redes, via de regra, maiores serão seus danos<sup>28</sup>.

Destaca-se que, nesses casos de ordem judicial para a remoção do conteúdo, o mesmo será indisponibilizado, ou seja, armazenado, ficando inacessível aos usuários da Internet, pois, caso ele fosse apagado não poderia ser usado como prova pelas demais outras vítimas. Nesses casos, pode-se dizer que a responsabilidade civil surge a partir de um fato processual, ou seja, do não atendimento da ordem judicial. Sendo assim, observa-se que a responsabilidade, com base no art. 19 do Marco Civil<sup>29</sup>, provavelmente será subjetiva. Restará objetiva apenas nos casos de relação de consumo.

O art. 19 do Marco Civil é questionado quanto a sua constitucionalidade, ele prevê que o provedor de aplicações da Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente<sup>30</sup>.

Anderson Schreiber fala sobre o tema:

A menção à ‘ordem judicial’ golpeia de morte toda a inspiração do notice and takedown. Como já se destacou, a limitação à responsabilidade civil dos chamados ‘provedores de aplicações’ somente pode se justificar como estímulo à sua atuação proativa, capaz de evitar a propagação do dano independentemente do tempo e custo necessários à propositura de uma ação judicial. Se a vítima da lesão ao seu direito fundamental precisa recorrer ao Poder Judiciário, pleiteando uma ordem judicial, a ser expedida à empresa, o art. 19 lhe é inteiramente inútil pela simples razão de que a possibilidade de recorrer ao Poder Judiciário sempre existiu no direito brasileiro e o descumprimento de ordem judicial, independentemente de qualquer consideração sobre responsabilidade civil, configura crime de desobediência<sup>31</sup>.

Diante disso, não há necessidade de se promover o contraditório com o provedor final. Os dados, objeto da ordem, não foram por ele produzidos e não lhe pertencem. Por isso, quando

<sup>28</sup> CAPANEMA, op. cit.

<sup>29</sup> BRASIL, op. cit., nota 9.

<sup>30</sup> MARTINS, op. cit.

<sup>31</sup> SCHREIBER, Anderson. Marco Civil da Internet: Avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiros. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. *Direito & Internet III*; Marco Civil da Internet. T. II. São Paulo: Quartier Latin, 2015.

alguma publicação ou conteúdo é determinado indisponível, o provedor tem o dever de comunicar ao usuário autor do material indisponibilizado as razões, para que este possa promover, caso assim entenda, as medidas judiciais em defesa de seus direitos, como previsto no art. 20 do Marco Civil da Internet<sup>32</sup>.

No que tange a comunicação dos motivos e fundamentos da indisponibilização ao seu usuário criador do conteúdo, deve haver algum canal de comunicação com ele, como endereço de e-mail e/ou telefone. Nesses casos, é dever do provedor informar também a extensão exata do conteúdo bloqueado.

O cumprimento desses requisitos é necessário para que o usuário autor do conteúdo tenha elementos para, eventualmente, impugnar judicialmente a restrição a si submetida. Vale ressaltar, porém, que não há na lei uma sanção para o provedor de aplicação que descumpra esse dever de comunicação no momento da retirada de algum conteúdo. O entendimento predominante, nesse sentido, é que ele só não esteja obrigado a cumprir essa norma em caso de previsão judicial ou legal expressa.

A advocacia está na era dos meios alternativos de solução de conflitos, como a arbitragem e a mediação, e o Marco Civil vêm para judicializar questões que podiam ser mais facilmente resolvidas de forma administrativa ou por meios mais ágeis. Seguindo os ditames do art. 19, a vítima passa a ter mais um ônus, de ter que recorrer ao Judiciário para retirar o conteúdo, o que faz com que o mesmo fique mais tempo nas redes.

Justamente por isso, o artigo 19 não é visto como inconstitucional, porém, ele diminui o exercício do direito fundamental à dignidade da pessoa humana. Consoante ao tema, pode ser visto no trecho do voto do Desembargador Francisco Eduardo Loureiro em causa envolvendo a responsabilidade civil da Google Brasil por conteúdo postado por terceiros, em referência ao artigo 19 do Marco Civil:

AÇÃO DE OBRIGAÇÃO DE FAZER C/C PEDIDO DE INDENIZAÇÃO – Empresa autora que postula a exclusão de site fraudulento criado em seu nome na Internet para venda de mercadorias, e a reparação dos danos morais sofridos – Sentença de extinção do feito sem resolução de mérito, sob o argumento de que o Google não tem legitimidade ad causam passiva – Desacerto – Réu, na condição de provedor de aplicações, é parte legítima para responder pelos pleitos decorrentes de conteúdo ilícito gerado por terceiros, nos termos do Marco Civil da Internet e da anterior jurisprudência consolidada (...) Previsão do art. 19 da Lei n. 12.965/14, no sentido de que o provedor de aplicações só pode ser responsabilizado civilmente por ato de terceiro após o descumprimento de ordem judicial específica determinando a remoção de conteúdo ilícito, não deve ser interpretada literalmente, pena de ser considerada inconstitucional (...) Ação parcialmente procedente – Recurso parcialmente provido<sup>33</sup>.

<sup>32</sup> BRASIL, op. cit., nota 9.

<sup>33</sup> BRASIL. Tribunal de Justiça de São Paulo. *Apelação nº 101139195.2015.8.26 . 0005. Relator: Desembargador*



Além disso, o STJ vem consolidando o entendimento de que é necessário que a parte indique precisamente o endereço das páginas (URL) onde o conteúdo lesivo encontra-se armazenado ou disponibilizado, para impor a remoção desse conteúdo ao provedor responsável pelo local. Isso ocorre por conta da impossibilidade técnica de o provedor controlar todo o conteúdo inserido no espaço virtual<sup>34</sup>.

Já o artigo 21 do Marco Civil<sup>35</sup> regulamenta a responsabilidade civil em caso de conteúdo de divulgação sexual. O dispositivo tem o intuito de coibir uma prática crescente na internet: a chamada *Revenge porn* (pornografia de vingança). Trata-se da disponibilização de conteúdos (fotos, vídeos ou qualquer outro material de caráter sexual) com o objetivo de causar dano à imagem, à honra e à intimidade da vítima<sup>36</sup>.

Desta forma, percebe-se um procedimento menos formal para a configuração da responsabilidade do provedor de aplicação: no caso do artigo 19, ela se configura pelo não atendimento da ordem judicial. Já no art. 21, ambos do Marco Civil<sup>37</sup>, basta apenas uma notificação enviada pela vítima ou seu representante legal com o pleito dessa exclusão, e caso não cumprida pode ensejar a responsabilidade do provedor em consequência de tal omissão. Vale destacar que essa notificação pode ser realizada inclusive em qualquer meio de comunicação inequívoca, como e-mail, redes sociais, aplicativos de mensagem, ou outros, que solicite a indisponibilização de algum material de cunho sexual.

Porém, não há um prazo específico para essa remoção, por ausência de previsão legal. A vítima poderá fazê-lo em sua notificação, mas deverão ser observados dois requisitos, estabelecidos no parágrafo único do artigo 21<sup>38</sup>, sob pena de nulidade: a identificação do material infringente e a verificação da legitimidade do pedido. Esse último consiste na comprovação ao provedor de aplicação de que o material diga respeito à intimidade da vítima.

No caso de inobeservância desses requisitos o entendimento majoritário é de que não há nulidade, mas sim mera irregularidade. Vale ressaltar que a responsabilidade do provedor de aplicação conforme o art. 21<sup>39</sup> só surge de forma subsidiária, ou seja, em decorrência de

---

Francisco Eduardo Loureiro. Disponível em: < <https://tj-sp.jusbrasil.com.br/jurisprudencia/350317872/apelacao-apl-10113919520158260005-sp-1011391-9520158260005>>. Acesso em: 03 jun. 2022.

<sup>34</sup> TEFFÉ, Chiara Spadaccini de. Direito à imagem na internet: estudo sobre o Tratamento do Marco Civil da internet para os casos de divulgação não autorizada de imagens íntimas. *Revista de Direito Civil Contemporâneo*. v. 15/2018, p. 93 a 127. Disponível em: < <http://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/413>>. Acesso em: 07 jun. 2022.

<sup>35</sup> BRASIL, op. cit., nota 9.

<sup>36</sup> CAPANEMA, op. cit.

<sup>37</sup> BRASIL, op. cit., nota 9.

<sup>38</sup> Ibid.

<sup>39</sup> Ibid.

ausência de bens para a reparação da vítima, ou no caso de não identificação do infrator<sup>40</sup>.

Segundo Walter Capanema<sup>41</sup>, podem ser identificados dois danos nessa hipótese: o primeiro do agente que divulgou o conteúdo danoso a imagem da vítima, e o segundo do provedor de aplicação que se recusa a atender a notificação de indisponibilização. Não há razão para subsidiariedade entre as hipóteses, conforme previsão da lei. Sendo assim, a responsabilidade civil na Lei nº 12.965/2014<sup>42</sup> privilegia os provedores de aplicação e deixa os usuários mais desprotegidos, sobretudo nos casos de violações de intimidade.

Passa-se a um breve paralelo entre a responsabilidade civil do Marco Civil da Internet e do Código de Defesa do Consumidor: nesta, a responsabilidade civil surge com o fato danoso, enquanto aquela exige que haja a conduta do consumidor na promoção de uma ação judicial ou notificação em face do provedor para que a responsabilidade seja configurada.

Em consequência, o questionamento que surge é justamente a indagação do motivo pelo qual os provedores de aplicação (que são também fornecedores de produtos e serviços) tenham um modelo de responsabilidade diferente dos demais, podendo ser até mais oneroso ao consumidor. Por isso, o Marco Civil é visto como uma legislação mais protetiva aos provedores, com a exposição dos consumidores e internautas<sup>43</sup>.

Os artigos 19 e 21 do Marco Civil<sup>44</sup> passaram a ter a constitucionalidade questionada, por violar a proteção ao consumidor, já consolidada na Constituição Federal. O tema controvertido gera bastantes discussões e ricas análises dentro desse escopo de responsabilizações.

Se por um lado os provedores alegam que é impossível a fiscalização dos usuários, impedindo-os de causarem danos, por outro eles lucram imensamente pelos conteúdos gerados por esses mesmos usuários. Logo, deveriam também arcar com esses danos. Normalmente esses sites são gratuitos, mas auferem suas receitas por diversos modos, como pela exibição de publicidade aos seus usuários, venda de dados pessoais a terceiros, bem como com a cessão de direitos autorais dos trabalhos realizados na plataforma<sup>45</sup>.

Diante disso, existem meios de investimento em modos de segurança inteligente, até mesmo com o uso de Inteligência Artificial, para utilização de ferramentas sofisticadas de análise de todos os tipos de conteúdo enviado por seus usuários.

---

<sup>40</sup>CAPANEMA, op. cit.

<sup>41</sup> Ibid.

<sup>42</sup> BRASIL, op. cit., nota 9.

<sup>43</sup> CAPANEMA, op. cit.

<sup>44</sup> BRASIL, op. cit., nota 9.

<sup>45</sup> CAPANEMA, op. cit.

Segundo entendimento de parte dos doutrinadores do tema, como Walter Capanema<sup>46</sup>, deveria ser preservada a responsabilidade civil prevista no CDC<sup>47</sup>, devendo os provedores de aplicação responderem objetivamente pelos conteúdos gerados por terceiros. Como já dito anteriormente, é possível que os provedores façam filtragens de mensagens, ainda que de modo prévio, com intuito de atender seus critérios mínimos de convivência previstos em seus Termos de uso/ Termos de serviço.

Esses Termos de uso são de aceitação obrigatória para criação do perfil nas redes sociais, são como verdadeiros contratos de adesão, sem possibilidade de negociação das cláusulas, cabendo aos usuários aderirem ou não aos mesmos. Eles dispõem acerca da responsabilidade dos usuários pelas informações prestadas e por sua conduta na rede, como uma tentativa de eximir totalmente a responsabilidade dos provedores de conteúdo que administram tais sites, porém, a maioria dos usuários nem sequer chega a ler tais informações.

Assim, pode-se constatar com segurança que o sistema protetivo do Código de Defesa do Consumidor é bem diverso do que o tratado pelo Marco Civil, pois neste há a requisição da configuração do dano e a judicialização da demanda, com o repasse do ônus ao usuário ofendido, o que acende alertas para que os operadores e aplicadores do Direito sigam acompanhando e protegendo os interesses dos usuários.

No caso dos Blogger, que são provedores de aplicação que permitem a criação de blogs e sites, ou ainda, do Youtube e do Facebook, que disponibilizam conteúdos e vídeos criados por seus usuários, a responsabilização vai variar de acordo com cada característica, no caso dos provedores de aplicação, que lucram com o conteúdo gerado e suas páginas (seja com publicidade ou troca de dados), devem também arcar com os danos causados por eles. Os provedores alegam ser impossível fiscalizar todos os usuários o tempo todo, para impedir que ocorra esses danos.

Sendo assim, pode ser responsabilizado exclusivamente o usuário infrator, como também pode ser responsabilizado o provedor do site sem mesmo analisar se houve dolo ou culpa, o que seria a aplicação de uma responsabilidade civil objetiva. Ou pode ser responsabilizado o provedor do site só quando o próprio for devidamente notificado sobre as irregularidades realizadas em seu âmbito e permanece inerte, tratando-se de uma responsabilidade civil subjetiva que, como visto, é o posicionamento majoritário.

Cada vez mais há sofisticadas ferramentas, com o uso até da inteligência artificial, para

---

<sup>46</sup> Ibid.

<sup>47</sup> BRASIL. *Código de Defesa do Consumidor*. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/18078compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm)>. Acesso em: 05 jun. 2021.

análise de todo e qualquer conteúdo enviado por seus usuários, que já fazem um bloqueio inicial automático de certos conteúdos que possam ter conotação ofensiva. Além disso, é possível com a simples solicitação de remoção pelos usuários, que o mesmo seja removido, não havendo necessidade de judicialização de todos os casos para incorrer em responsabilização e remoção.

Como exposto, em várias situações o conflito de interesses exigirá uma delicada ponderação entre o direito à imagem e as liberdades de expressão e de informação, devendo ser analisado em cada caso concreto qual direito fundamental deverá prevalecer para que se promova uma proteção compatível com a dignidade da pessoa humana.

Diante disso, é preciso fazer um bom uso dos dispositivos legais nos casos concretos, à luz dos princípios constitucionais, pois, como será visto no decorrer da presente pesquisa, a jurisprudência tem sido determinante para as diretrizes da aplicação da responsabilidade civil no âmbito virtual.

### **1.3 Responsabilidade Civil nas Relações de Consumo**

A responsabilidade civil também precisa ser estudada no âmbito consumerista e suas especificidades no ambiente digital, para ser compreendida na sua integralidade. O avanço tecnológico, bem como a ampliação da vida virtual, fizeram com que as relações de consumo na internet se expandissem de modo assustador.

Os internautas, diante das muitas ofertas disponibilizadas nas redes, que podem ser concretizadas sem muito esforço, isto é, com um mero *clique*, realizam diversas compras sem as devidas cautelas, o que pode gerar problemas posteriormente.

Com o advento do Código de Defesa do Consumidor, Lei nº 8.078/1990, passou a existir a responsabilidade objetiva dos fornecedores de produtos e prestadores de serviços, o que tornou mais fácil para o consumidor a obtenção da reparação integral quanto aos danos a ele causados<sup>48</sup>.

A responsabilidade civil objetiva prescinde de demonstração de culpa, pois retira do indivíduo lesado o ônus de provar quem lhe causou o dano frente a eventuais vícios ou defeitos de produto ou serviço. No caso das relações de consumo, além de objetiva, a responsabilidade civil é solidária, ou seja, permite que o consumidor possa exigir a reparação de quaisquer dos fornecedores que façam parte da cadeia de consumo, conforme expresso nos artigos 7º,

---

<sup>48</sup> TARTUCE, Flávio; NEVES, Daniel Assumpção. *Manual de Direito do Consumidor*. 7. ed. São Paulo: Forense, 2018, p. 129 a 139.

parágrafo único e 25, § 1º do CDC.<sup>49</sup>

Contudo, apesar dessa ampla responsabilização dos fornecedores que causam eventuais danos consumeiristas, é possível que ela não ocorra se houver o rompimento do nexo de causalidade, como estabelece os artigos 12, § 3º, I a III e 14, §3º, inciso I e II, do CDC<sup>50</sup>, prevendo hipóteses de afastamento do nexo de causalidade e, conseqüentemente, de extinção da responsabilidade civil do fornecedor.

Pode-se dizer que o Código de Defesa do Consumidor<sup>51</sup> prevê quatro situações básicas de responsabilidade civil: (i) responsabilidade pelo vício do produto, nos artigos 18 e 19, (ii) responsabilidade pelo fato (defeito) do produto, artigos 12 e 13, (iii) responsabilidade pelo vício do serviço, no art. 20 e (iv) responsabilidade pelo fato/defeito do serviço, prevista no artigo 14. Nesse ponto cabe esclarecer que, por fato entende-se a extensão do dano.

Passando a uma breve análise de cada um destes, na responsabilidade pelo vício do produto, o problema restringe-se ao próprio produto, sem ocasionar prejuízos colaterais, e é dividido em duas modalidades, o vício de qualidade e o vício de quantidade, pelos quais os fornecedores responderão de forma solidária em uma eventual ação indenizatória.<sup>52</sup>

Porém, há duas exceções à regra da responsabilidade solidária. A primeira é referente aos vícios de qualidade, menciona os produtos comercializados *in natura* e está prevista no § 5º do art. 18 do CDC<sup>53</sup>. Nela, o fornecedor imediato, ou seja, o comerciante, será o responsável perante o consumidor, salvo se o produtor puder ser claramente identificado. A segunda exceção refere-se aos vícios de quantidade: o comerciante também será responsável quando fizer a pesagem ou a medição e o instrumento utilizado para isso não estiver de acordo com os padrões oficiais, segundo o art. 19, § 2º, do CDC.<sup>54</sup>

Já a responsabilidade civil pelo defeito do produto transpõe os limites do produtor, que não oferece a segurança que dele se espera, ocasionando danos colaterais de natureza material, moral ou estética, e também gera ao fornecedor uma responsabilidade objetiva. Conforme preconiza o art. 13 do CDC<sup>55</sup>, a exceção fica a cargo da responsabilidade mediata, logo

<sup>49</sup> BRASIL, op. cit., nota 47.

<sup>50</sup> Ibid.

<sup>51</sup> Ibid.

<sup>52</sup> RODRIGUES, Marcel André. *A responsabilidade civil e o Código de Defesa do Consumidor*. Disponível em: <<https://marcelandre.jusbrasil.com.br/artigos/126510917/a-responsabilidade-civil-e-o-codigo-de-defesa-do-consumidor>>. Acesso em: 23 mai. 2021.

<sup>53</sup> BRASIL, op. cit., nota 47.

<sup>54</sup> Ibid.

<sup>55</sup> Ibid.

subsidiária, do comerciante que disponibilizou um produto que venha a apresentar um defeito e causar um acidente de consumo<sup>56</sup>.

No tocante à responsabilidade civil por vício do serviço, entende-se ocorrer vício no serviço quando o mesmo é prestado de forma inadequada para os fins que razoavelmente deles se esperam ou não atendam as normas regulamentares da atividade contratada.

Por último, a responsabilidade civil por fato do serviço, restará configurada diante de um serviço defeituoso, que cause um acidente de consumo e resulte em prejuízo ao consumidor. Em todos os casos, os fornecedores poderão ser solidária e objetivamente responsabilizados.

Passando a análise dessas responsabilizações no ambiente digital, primeiramente conceitua-se o *e-commerce*, ou comércio eletrônico, como o conjunto de relações travadas entre fornecedores e consumidores, realizadas em um estabelecimento empresarial virtual<sup>57</sup>.

O ordenamento jurídico brasileiro não tem nada que regule especificamente as relações virtuais, sendo também aplicável nesses casos o Código de Defesa do Consumidor<sup>58</sup>. A oferta do produto, nos moldes do art. 31 do CDC, deve ser correta, clara e precisa, deve conter informações sobre as características, qualidades, quantidade, preço, garantia, prazo de validade e origem, entre outras informações.

Além disso, os fabricantes dos produtos devem estar identificados pelo nome e endereço, de acordo com o art. 33 do CDC. Se essas informações forem falsas, será um caso de vício do produto, nos termos do art. 18 do CDC, ou do serviço, conforme art. 20, do CDC. Inclusive se o sítio eletrônico não contiver informações claras e em destaque, especialmente no que tange a cláusulas limitativas dos direitos do consumidor, essas serão consideradas como não escritas, como dispõe o art. 46 do CDC<sup>59</sup>.

Nos casos das propagandas nos websites, seja feita no site do próprio anunciante ou por outro site, também há diferença no tratamento, apenas o anunciante será responsabilizado pela propaganda enganosa ou abusiva, com base nos artigos 36 e 37 do CDC. Sendo assim, a propaganda veiculada em outro site, que não o do fornecedor do produto, aquele que a hospedou não responde pelo fornecedor do produto<sup>60</sup>.

Do mesmo modo, o provedor de acesso à internet não responde por eventual

---

<sup>56</sup> CARVALHO, Rhayra Melo Ribeiro de. *Responsabilidade civil no Direito do Consumidor*. Disponível em: <<https://jus.com.br/artigos/50652/responsabilidade-civil-no-direito-do-consumidor>>. Acesso em: 23 mai. 2021.

<sup>57</sup> NEVES, Thiago Ferreira Cardoso. *O Comércio Eletrônico e o Direito do Consumidor*. Disponível em: <[https://www.emerj.tjrj.jus.br/revistaemerj\\_online/edicoes/revista64/revista64\\_154.pdf](https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista64/revista64_154.pdf)>. Acesso em: 02 jun. 2021.

<sup>58</sup> BRASIL, op. cit., nota 47.

<sup>59</sup> Ibid.

<sup>60</sup> NEVES, op. cit.

propaganda enganosa ou abusiva dos produtos adquiridos em seus websites. Com o intuito de ampliar a proteção dos consumidores no comércio eletrônico, foi editado o Decreto nº 7.962/2013<sup>61</sup> com o intuito de proteger o consumidor, assegurando-lhe o amplo acesso à informação, bem como fazendo com que os fornecedores ajam com mais transparência e boa-fé<sup>62</sup>.

Traçando um paralelo entre ambas as legislações deve-se comparar o texto do art. 43 da LGPD<sup>63</sup> com o dos artigos, 12, parágrafo terceiro e art. 14, parágrafo 3º do CDC<sup>64</sup>, quanto as hipóteses de não responsabilização, inciso I do art. 43, os agentes de tratamento não serão responsabilizados se provarem que não realizaram o tratamento de dados. O que pode ser claramente comparado com o inciso I, do art. 12, § 3º da normativa consumerista, que afirma que os fornecedores não serão considerados responsáveis quando existirem provas de que não foi ele que introduziu o produto no mercado<sup>65</sup>.

A segunda hipótese de afastamento da responsabilidade, conforme o art. 43, II<sup>66</sup>, ocorre quando o tratamento for realizado pelos agentes de tratamento, sem, no entanto, haver violação à legislação de proteção de dados. Isso pode se analisar com um paralelo ao que dispõe o inciso II do art. 12, §3º, e o inciso I do art. 14, § 3º, do CDC<sup>67</sup>.

Além disso, culpa exclusiva do titular ou de terceiros também é uma excludente de responsabilização por parte do agente de tratamento, conforme previsto no inciso III do art. 43, da LGPD<sup>68</sup>, bem como do fornecedor de produtos ou serviços de serem responsabilizados quando o consumidor ou um terceiro for o único e exclusivo culpado pela ocorrência do dano, de acordo com o art. 12, § 3º, III e art. 14, § 3º, III do CDC<sup>69</sup>.

Diante disso, observam-se muitas semelhanças entre ambas as legislações quanto a responsabilização dos agentes de tratamento ou fornecedores e vendedores de produtos. Como também no tocante a possibilidade de inversão do ônus da prova a favor do titular dos dados em uma eventual ação judicial, seguindo os mesmos requisitos previstos no CDC, art. 6º, VIII,

<sup>61</sup> BRASIL. *Decreto nº 7.962*, de 15 de março de 2013. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/decreto/d7962.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm)>. Acesso em: 05 jun. 2021.

<sup>62</sup> NEVES, op. cit.

<sup>63</sup> BRASIL. *Lei nº 13.709*, de 14 de agosto de 2018. 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: 05 jun. 2021.

<sup>64</sup> BRASIL, op. cit., nota 47.

<sup>65</sup> SOARES, Jéssica. O Direito do Consumidor e a sua relação com a Lei Geral de Proteção de Dados (LGPD) à Luz da Responsabilidade Civil. In: PINHEIRO, Ana Cristina Augusto (Coord.). *Temas Contemporâneos para TCC*. V. 04. Rio de Janeiro: Processo, 2021, p. 17 a 32.

<sup>66</sup> BRASIL, op. cit., nota 63.

<sup>67</sup> BRASIL, op. cit., nota 47.

<sup>68</sup> BRASIL, op. cit., nota 63.

<sup>69</sup> BRASIL, op. cit., nota 47.

que é a verossimilhança das alegações e a hipossuficiência técnica do titular/consumidor<sup>70</sup>.

---

<sup>70</sup> SOARES, op. cit.



## 2. A RESPONSABILIDADE CIVIL E A LGPD

A Lei Geral de Proteção de Dados entrou em vigor visando proteger o Direito à privacidade, a intimidade e, sobretudo, regulamentar o tratamento de dados pessoais no país. Diante disso, a responsabilidade civil na LGPD<sup>71</sup> é tema extremamente importante de ser debatido, envolvendo diferentes pressupostos e vertentes. Somente por meio de um regime suficientemente preciso de responsabilidade civil haverá garantia plena de uma tutela efetiva à proteção dos dados pessoais.

Com o intuito de melhor esclarecer o tema e estabelecer diretrizes para a colocação da LGPD na prática, o presente capítulo analisa os conceitos e definições de grande relevância para essa nova legislação, também visando explorar a responsabilidade dos agentes de tratamento de dados pessoais, prevista na própria lei, bem como conhecer os pressupostos teóricos da responsabilidade civil no ordenamento jurídico brasileiro.

### 2.1 Lei Geral de Proteção de Dados Pessoais: conceitos e definições introdutórias

Inicialmente pretende-se evidenciar alguns conceitos da Lei Geral de Proteção de Dados<sup>72</sup>, para posteriormente analisar a responsabilidade civil dentro da nova Lei, sem a pretensão de fazer uma abordagem geral da própria, apenas estabelecer algumas definições importantes para o desenrolar da presente pesquisa.

O art. 5º da LGPD traz uma série de conceitos importantes, inicia tratando do que é um dado pessoal, refere-se as informações relacionadas a pessoa natural identificada ou identificável, podendo ser um dado privado ou público, cujo agente incumbido de seu tratamento pode ser responsabilizado quando proceder indevidamente. Ou seja, trata-se de um conceito amplo que engloba não apenas informações diretamente ligadas a pessoa, como o número do RG, CPF ou endereço, mas também inclui informações que por si só não identificam o indivíduo titular do dado, mas quando combinadas com outros dados pode identificar, como, por exemplo a geolocalização<sup>73</sup>.

Já o dado pessoal sensível possui uma maior proteção, conforme previsão legal, se refere aqueles dados que trazem informações críticas sobre o titular, como por exemplo, as

---

<sup>71</sup> BRASIL, op. cit., nota 63.

<sup>72</sup> Ibid.

<sup>73</sup> FONSECA, Edson Pires da. *Lei Geral de Proteção de Dados Pessoais – LGPD*. Salvador: JusPodivm, 2021, p. 53.

preferências políticas, sexuais, seu estado de saúde, informações genéticas e biométricas, conforme estipulado no art. 5º, II, da LGPD<sup>74</sup>. Ele traz uma faceta ainda mais profunda da intimidade do titular do dado, por isso requer uma proteção mais cautelosa e restritiva.

A lei também identifica os dados anonimizados, que são aqueles que em razão da utilização de meios técnicos, não possibilitam mais a identificação do seu titular, há uma desconexão permanente entre o titular e o dado, logo, ele deixa de ser um dado pessoal, afastando-se da incidência da nova legislação de proteção de dados.

Ressalta-se que o bem jurídico que a LGPD<sup>75</sup> se propõe a tutelar não é apenas a privacidade por si só, mas sim o dado pessoal, seja ele público ou privado, esteja ele no ambiente de intimidade ou não. Sendo assim, vai muito além de uma proteção à intimidade apenas, protegendo os dados que causarão maior impacto no ordenamento jurídico brasileiro.

Pois enquanto acreditarem que o problema da responsabilidade civil na proteção de dados é um problema de privacidade exclusivamente, levanta-se outro debate, inquerindo sobre o que fazer no caso de um sujeito que não causou o vexame, ou seja, não foi responsável pelo vazamento do dado da pessoa, não expos o dado, não causou dano. Logo, esse dado vazado poderia ser considerado um dado público não tendo mais que obedecer as definições de privacidade e proteção previstas na LGPD<sup>76</sup>, tal possibilidade se mostra problemática.

Se após um vazamento de dados o que for feito dali em diante, pela empresa que vazou ou por outras empresas, não pudesse mais ser responsabilizado, pois uma vez que o dado se torna público e todos os que fizerem uso dele dali em diante não pudessem mais ser responsabilizados, anularia a utilidade e necessidade das leis de proteção de dados.

A questão chave para responsabilizar é saber se o agente de tratamento tem legitimidade para tratar esse dado, se o fez legitimamente ou não, se houve tratamento diverso do legítimo, já é um fator que levanta a responsabilidade civil na LGPD, como será visto de modo mais claro adiante.

Além disso, autores como Bruno Bioni e Doneda<sup>77</sup>, afirmam que os dados pessoais são direito da personalidade independentemente da privacidade, sendo essa apenas um dos elementos que integram o conjunto de proteção, não sendo o único. Esses autores defendem a autonomia da proteção de dados pessoais relativamente ao direito da privacidade, considerando as limitações do consentimento e da autodeterminação, como também pelo fato de a natureza

---

<sup>74</sup> BRASIL, op. cit., nota 63.

<sup>75</sup> Ibid.

<sup>76</sup> Ibid.

<sup>77</sup> MARTINS, op. cit.

do direito da personalidade ser inalienável, irrenunciável e de permanente interesse para toda a coletividade, ou seja, assegurando maior relevância e garantia à proteção de dados pessoais.<sup>78</sup>

Além disso, o tratamento autônomo da matéria é uma tendência mundial e encontra-se expresso em diversos ordenamento jurídicos, inclusive como um direito fundamental. No Brasil, como pode ser visto com a aprovação da Proposta de Emenda à Constituição Federal (PEC) 17/2019<sup>79</sup>, em outubro de 2021, que tem como objeto a alteração da Carta Magna para a inclusão da proteção aos dados pessoais entre os direitos fundamentais, inclusive nos meios digitais.

Após ampla discussão entre especialistas da área, e por ser o direito à proteção de dados uma questão ampla, pois abarca todos os dados que dizem respeito a uma pessoa natural, independentemente da sua esfera íntima, privada, familiar ou social, indo além da tutela da privacidade, deve ser reconhecido como um direito fundamental autônomo, com vinculação direta à proteção da personalidade.

Diante dessa aprovação, o tratamentos de dados pessoais deve ser compatibilizado com a dignidade da pessoa humana, pois através dos ditames da Constituição Federal, a privacidade e a dignidade poderão ser projetadas como elementos constitutivos da cidadania, para que o titular dos dados não seja reduzido a fins mercadológicos, tampouco seja discriminado ou classificado.

A LGPD, no art. 5º, incisos VI, VII e IX<sup>80</sup>, traz em seu texto as definições dos agentes de tratamento. O controlador é definido no inciso V como sendo a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”, ou seja, é quem toma as decisões acerca do tratamento de dados, responsável pela definição de como será realizado mediante o estabelecimento dos critérios, requisitos e parâmetros que irão nortear o tratamento.

Enquanto que o operador é toda “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”, conforme previsto no inciso VII, será quem operacionaliza o tratamento de dados, executando o que foi estabelecido pelo controlador.

Sendo possível inclusive, dependendo do tratamento, a função de operador e

---

<sup>78</sup> DONEDA, Danilo. *Da privacidade à Proteção de Dados Pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2020, p. 290.

<sup>79</sup> BRASIL. Senado Federal. *Proposta de emenda à Constituição Federal nº. 17 de 2019*. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1633717204657&disposition=inline>>. Acesso em: 04 jun. 2022.

<sup>80</sup> DONEDA, op. cit., p. 290.

controlador serem realizadas pela mesma pessoa. Como o controlador que dirá quais as instruções do tratamento, caberá a ele também auditar se o operador estará realizando o tratamento em conformidade como previsto, podendo inclusive o operador responder solidariamente junto com o controlador pelos danos causados no tratamento, nos casos de descumprimento à LGPD<sup>81</sup> e às instruções do controlador, como será tratado adiante<sup>82</sup>.

Já a figura encarregada, ou DPO – *Data Protection Officer*, segundo o regulamento europeu - na LGPD, no inciso VIII do art. 5º<sup>83</sup>, ele é definido como a “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)”. Contudo, a sua atuação poderá ser dispensada a depender da natureza, do porte do negócio e do volume de dados tratados.

O encarregado possuirá autonomia e estabilidade para atender as demandas dos titulares, interagir com a autoridade nacional e orientar funcionários e contratados quanto as práticas de proteção de dados pessoais.

Diante disso, controlador e operador são os principais agentes de tratamento responsáveis por realizarem as diversas operações referentes aos dados pessoais. Compete, via de regra, ao controlador a decisão sobre o tratamento e ao operador a execução das determinações do controlador. Contudo, um erro muito comum para quem não está acostumado a lidar com a Lei Geral de Proteção de Dados Pessoais, é achar que o operador e o controlador de dados pessoais são pessoas físicas, o que não é verdade. Salienta-se que o agente de tratamento não se refere a pessoa física, seja um funcionário da empresa ou o próprio sócio, que está com “a mão na massa” necessariamente, eles estão ali apenas representando a empresa, são um *longa manus* dela, o controlador e agente podem ser a própria empresa como pessoa jurídica, que responderá como tal.

O tratamento de dados envolve diversas operações relacionadas aos dados pessoais, conforme conceitua o art. 5º da LGPD<sup>84</sup>:

Art. 5º

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

---

<sup>81</sup> Ibid.

<sup>82</sup> FONSECA, op. cit., p. 142.

<sup>83</sup> BRASIL, op. cit., nota 63.

<sup>84</sup> Ibid.

Observa-se que praticamente toda e qualquer forma de manipulação pode ser considerada como tratamento de dados pessoais, logo, deve haver submissão às regras da nova lei. O tratamento de dados contempla todo o ciclo de vida do dado pessoal, desde a coleta até o descarte.

Diante disso, qualquer empresa que colete e utilize dados pessoais, seja de seus clientes – como em um *e-commerce* ou em uma loja física - ou de funcionários, ou parceiros comerciais, e outros, será também um agente de tratamento de acordo com a definição trazida pela LGPD. Ainda que o negócio principal da empresa não seja o tratamento de dados pessoais, no mínimo, ela trata os dados dos seus funcionários, e por vezes também dos clientes e parceiros comerciais<sup>85</sup>.

Ressalta-se que a LGPD não faz distinção entre os as formas de armazenamento de dados, como é possível observar no texto do primeiro artigo da lei<sup>86</sup>:

Art. 1º 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.

Por mais que atualmente vivencie-se a era digital, na qual geralmente os dados já nascem, são tratados, e descartados totalmente por meios digitais, a lei é igualmente aplicada aos dados em estado *off-line*. Sendo assim, cadastros e fichas manuais, de papel, que são armazenadas em arquivos físicos também precisam ter seu sistema de armazenamento e tratamento de dados pessoais revistos, pois necessitam se adequar à LGPD do mesmo modo que os dados virtuais.

Além disso, a nova lei possui caráter extraterritorial, pois será aplicada independentemente do país sede da empresa que realizou o tratamento de dados e de onde os dados se originam, desde que se encontre em uma das duas hipóteses previstas no art. 3º, incisos I, II e III da LGPD<sup>87</sup>, que dizem:

Art. 3º I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais, objeto do tratamento tenham sido coletados no território nacional.

Assim, após a compreensão de alguns conceitos básicos, iniciará a seguir a análise da responsabilidade civil dentro da Lei Geral de Proteção de Dados e dos pressupostos necessários

---

<sup>85</sup> FONSECA, op. cit., p. 84.

<sup>86</sup> BRASIL, op. cit., nota 63.

<sup>87</sup> Ibid.

para proporcionar adequada proteção aos direitos dos titulares de dados quanto a responsabilização pelos danos sofridos em decorrência do tratamento de seus dados pessoais.

## 2.2 Responsabilidade Civil na LGPD

Dando prosseguimento a análise acerca da responsabilidade civil na proteção de dados com a análise da própria LGPD quanto a responsabilidade dos agentes de tratamento. A letra legislativa que centraliza a pesquisa passa a abordar o tema na Seção III do Capítulo IV, intitulada “Da Responsabilidade e do Ressarcimento de Danos”<sup>88</sup>.

Contudo, as normas expressas na referida seção não serão aplicadas em todos os casos que envolvam responsabilidade civil, pois a própria lei encarrega-se de expressamente reconhecer, em seu art. 45, a aplicação de legislação específica sobre o tema, como por exemplo, na área consumerista.

Nesse sentido, sempre que o titular de dados pessoais figurar também como consumidor em sentido estrito ou por equiparação, poderá invocar o sistema de responsabilização previsto no artigo 13, do Código de Defesa do Consumidor<sup>89</sup> e demais legislações correlatas, como já citado no capítulo anterior.

Em seus artigos 42 a 45<sup>90</sup> a lei estabelece regras referentes à responsabilidade civil dos agentes de tratamento de dados pessoais. Essas regras são pautadas em três princípios norteadores da lei: o da segurança, o da prevenção e o da responsabilização e prestação de contas, todos eles previstos no artigo 6º da LGPD, indicando o caminho que o legislador quis adotar para estabelecer a responsabilidade civil na LGPD. Também pode ser visto no artigo 46 da referida Lei, dispositivos que dizem respeito ao tratamento da segurança de dados, governança e sanções administrativas adequadas em caso de incidentes de segurança<sup>91</sup>.

Analisando, o princípio da prestação de contas estabelece a necessidade de atender à transparência a ser adotada pelo agente de tratamento de dados acerca dos procedimentos que são tomados para a segurança no procedimento com os dados. Os titulares devem ser comunicados de todas as medidas de segurança que serão adotadas, sendo assim um dever ativo dos agentes de tratamento.

---

<sup>88</sup> Ibid.

<sup>89</sup> BRASIL, op. cit., nota 47.

<sup>90</sup> BRASIL, op. cit., nota 63.

<sup>91</sup> MULHOLLAND, Caitlin. *A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?* Disponível em: <<https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco>>. Acesso em: 26 mai. 2021.

Com isso, surge a necessidade de prestação de contas, onde serão evidenciadas as medidas que estão sendo tomadas para uma atuação em conformidade com as boas práticas exigidas pela lei. O princípio da segurança versa justamente sobre a proteção trazida pela lei e o seu objetivo, enquanto o princípio da prevenção sugere a busca pelo tratamento dos dados de forma preventiva, sem que haja um incidente que alerte para a necessidade disso<sup>92</sup>.

O *caput* do art. 42<sup>93</sup> preconiza controlador e operador como possíveis responsáveis solidários diante de danos de ordem material ou moral, individual ou coletiva, eventualmente infligidos aos indivíduos, importante ressaltar mais uma vez as diferenças entre controlador e operador, sobretudo no que tange a distribuição de responsabilidade previstas na LGPD.

O controlador detém o poder de decisão e, por isso, a ele são atribuídas maiores responsabilidades. Já o operador, age de acordo com os comandos do controlador, e poderá responder de forma solidária por eventuais danos, podendo, inclusive, ser equiparado ao próprio controlador na hipótese de descumprir as obrigações previstas na lei ou as instruções por ele transmitidas.

No tocante à figura do encarregado, em que pese apesar da LGPD não os mencionar expressamente, é provável que, quando ele atuar como um terceiro destacado das figuras do controlador e do operador, é possível que também seja responsabilizado de forma solidária por eventual dano causado em casos específicos. Assim, pode-se dizer que esse artigo não faz menção a culpa ou dolo para a responsabilização.

Analisando brevemente os incisos do art. 42<sup>94</sup>, no inciso I, a responsabilidade parece ser subjetiva, isto é, pressupõe culpa do operador. Já no inciso II, prevê-se a responsabilidade solidária dos controladores envolvidos, quando tiver mais de um no mesmo tratamento.

Também chama atenção, no artigo 42, a pluralidade de danos que a Lei prevê expressamente, “dano patrimonial, moral, individual ou coletivo”. O dano trata-se de uma lesão a um bem jurídico protegido, o dano patrimonial, é compreendido como uma lesão a um interesse jurídico passível de valoração econômica, quanto o moral, trata-se de uma lesão a um bem jurídico relacionado à personalidade humana. Isso serviu para evitar dúvidas quanto à ampla proteção, não reservada apenas aos titulares propriamente ditos, mas também a terceiros, e até mesmo a própria coletividade, que a nova Lei visa abranger, conforme será visto **a respeito**

---

<sup>92</sup> Ibid.

<sup>93</sup> BRASIL, op. cit., nota 57.

<sup>94</sup> Ibid.

dos danos coletivos da LGPD adiante<sup>95</sup>.

Desse modo, a LGPD já se preveniu quanto as diferentes espécies de danos que podem resultar do tratamento de dados pessoais, e os cita expressamente, sem deixar dúvidas quanto à ampla proteção reservada do tratamento de dados pessoais, evitando dúvidas quanto o que se deve compreender como ampla proteção. Afinal, por mais que a primeira vítima de um tratamento ilegal de dados pessoais seja o próprio titular, que tem sua privacidade violada, e por isso merece reparação pelo dano moral sofrido, o tratamento ilegal gera efeitos mais amplos atingindo interesses transindividuais. Por isso, o regime de responsabilidade civil da LGPD incide não sobre o interesse do lesado, mas sim pela atividade lesiva, ela incidirá sobre qualquer dano decorrente do exercício da atividade<sup>96</sup>.

Partindo da definição do que é tratamento de dados pessoais, exposta no art. 5º, X da LGPD, percebe-se, pelo extenso rol de hipóteses exemplificativas, que o legislador trouxe uma noção abrangente de tratamento de dados, protegendo assim a maioria dos problemas que envolvem os dados pessoais, veja<sup>97</sup>:

Art.5º, X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Como dito, os casos de vazamento de dados geralmente atingem várias pessoas ao mesmo tempo, por isso a lei<sup>98</sup> já prevê, no art. 42, parágrafo 3º, que as ações de reparação por danos coletivos que tenha por objetivo a responsabilização dos agentes de tratamento, podem ser propostas coletivamente em juízo.

Por mais que o dano moral seja individual, o ordenamento jurídico brasileiro já autoriza a propositura de ações judiciais coletivas voltadas a reparação de danos morais individuais, desde que sejam resultado da lesão de direitos individuais homogêneos, que decorram de uma origem comum, como previsto no art. 81, III, do CDC<sup>99</sup>. Esclarece-se que essa origem comum não requer uma unidade factual e temporal, como por exemplo uma propaganda enganosa veiculada em vários órgãos de imprensa e que é exposta por vários dias, ou seja, em um largo espaço de tempo e em vários lugares diferentes, também será um caso de

---

<sup>95</sup> SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 319 a 337.

<sup>96</sup> Ibid.

<sup>97</sup> BRASIL, op. cit., nota 57.

<sup>98</sup> Ibid.

<sup>99</sup> BRASIL, op. cit., nota 47.



origem comum do dano, sendo passível de uma ação coletiva<sup>100</sup>.

Diante disso, pode uma única ação coletiva ser promovida por todos os titulares que tiverem seus dados pessoais expostos ao público por um erro de tratamento ou falha ou violação do sistema de dados de uma empresa. A ação pode ser coletiva, porém, os danos seguirão sendo individuais.

Diferentemente dos danos coletivos, previstos , no *caput* do art. 42, como dito acima, neles não se trata de uma ação coletiva tratando de direitos individuais com origem em comum, mas sim da lesão a um interesse supraindividual, ou seja, que não pertence a cada vítima, mas sim a toda a coletividade, de modo determinado ou indeterminado, sendo, portanto, indivisível a seus titulares<sup>101</sup>. Esses danos coletivos já são previstos e tratados também no art. 81 do CDC, incisos I e II. Um exemplo de dano coletivo abarcado pelo regime protetivo instituído pela LGPD, seria o causado pela propagação de *fake news* em períodos eleitorais, pois gera impacto sobre o direito supraindividual à informação adequada e verídica.

Destaca-se no art. 42, parágrafo 4º, da LGPD<sup>102</sup>, a previsão do direito de regresso, no qual aquele que reparar o dano tem direito de regresso contra os demais responsáveis, proporcionalmente as suas respectivas participações no evento danoso. Isso, assegura que o titular do dado possa cobrar integralmente pelo dano sofrido a qualquer um dos responsáveis envolvidos.

O artigo 43<sup>103</sup> da referida Lei, como já citado anteriormente, prevê as hipóteses de afastamento da responsabilidade dos agentes de tratamento mediante o rompimento do nexo de causalidade, em três hipóteses diferentes. O inciso I dele estabelece que os agentes de tratamento não serão responsabilizados se provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído.

Já a segunda hipótese de afastamento, art. 43, II<sup>104</sup>, ocorre quando o tratamento de dado foi realizado pelo próprio agente, porém, ser ter ocorrido violação à legislação de proteção de dados. Esse inciso denota a observação de uma responsabilidade civil subjetiva na lei, pois pode eximir o agente de tratamento de sua responsabilidade no caso mesmo que o dano seja comprovado, responsabilizando-o apenas no caso do mesmo violar a legislação de proteção de dados. Sendo assim, se o agente provar que agiu adequadamente durante o tratamento do dado, ele não terá responsabilidade pela ocorrência de algum incidente. Adiante será analisado de

---

<sup>100</sup> SCHREIBER, op. cit.

<sup>101</sup> Ibid.

<sup>102</sup> BRASIL, op. cit., nota 57.

<sup>103</sup> Ibid.

<sup>104</sup> Ibid.

forma mais profunda essa teoria.

O inciso III do art. 43<sup>105</sup> prevê a culpa exclusiva do titular do dado ou de terceiro, outra hipótese de afastamento da responsabilidade civil dos agentes de tratamento. O artigo 44 determina o que é o tratamento irregular e em quais casos ele gera responsabilização, que são: quando houver violação da lei ou quando houver legítima expectativa do titular por aquele tratamento.

Por sua vez, esses dois casos que levam ao conceito de tratamento irregular devem ser analisados considerando, dentre outras circunstâncias, o modo como o tratamento é realizado, o resultado e os riscos razoavelmente esperados pelo tratamento e as técnicas de tratamento de dados disponíveis à época em que este foi realizado<sup>106</sup>.

Porém, o parágrafo único do artigo 44<sup>107</sup> estabelece que o controlador ou o operador será obrigado a indenizar os danos decorrentes da violação da segurança dos dados quando deixarem de adotar as medidas de segurança previstas no art. 46, da LGPD, que diz o seguinte: aquelas "aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

Contudo, o art. 44 pode ser interpretado de modo amplo e ser visto de forma muito aberta, pois não há especificação na lei do que seria um tratamento irregular de dados pessoais. Por isso, o intérprete tem que recorrer a outros elementos interpretativos.

Além disso, no seu parágrafo único, art. 44, há uma hipótese adicional de responsabilização do operador e do controlador mesmo quando adotarem as medidas regulares de tratamento e seguirem as normas de segurança, podendo ainda assim serem responsabilizados pelos danos decorrentes do tratamento de dados. Resalta-se que, do ponto de vista teleológico, o propósito da LGPD é de conferir ampla proteção a autodeterminação informativa, buscando revestir de segurança e previsibilidade o tratamento conferido aos dados pessoais no Brasil<sup>108</sup>.

Diante disso, conclui-se, inicialmente, que a LGPD<sup>109</sup> remete a uma responsabilidade objetiva baseada no risco, enquanto o artigo 44 inverte esse entendimento quando conceitua o tratamento irregular como aquele que viola a segurança, ou seja, apenas quando o controlador

---

<sup>105</sup> Ibid.

<sup>106</sup> MULHOLLAND, op. cit.

<sup>107</sup> BRASIL, op. cit. nota 57.

<sup>108</sup> SCHREIBER, op. cit.

<sup>109</sup> Ibid.

deixar de seguir as normas de segurança<sup>110</sup>. Trata-se aí, a rigor, de responsabilidade subjetiva, pois depende do descumprimento do dever jurídico previsto no art. 46 da Lei.

Antes de ser analisada as diferentes correntes sobre os tipos de responsabilidade civil contidos na LGPD, importante compreender o papel do nexo causal nessa responsabilização, pois por mais que a responsabilidade objetiva dispense a culpa do agente, nem ela, e nem nenhum outro tipo de responsabilidade civil, dispensa a aferição do nexo de causalidade.

O nexo causal, que é a relação de causa e consequência, é originariamente um conceito lógico, e não jurídico. Contudo, o direito é que vem mitigando essa relação de causalidade, considerada como apta a produzir a obrigação de indenizar.

O ordenamento jurídico brasileiro adota diversas teorias no tema, como a Teoria da causalidade direta e imediata, que limita o dever de indenizar às consequências direta e imediatamente derivadas da conduta culposa. Bem como há outras teorias da causalidade que geram um cenário jurídico flexível no tocante ao nexo causal<sup>111</sup>.

Quanto ao tratamento de dados especificamente, a questão continua sendo extremamente complexa, gerando muitas possibilidades de interpretação e pressupostos, sobretudo por conta das especificidades da área, há casos, por exemplo, em que a fonte originária de dados pessoais expostos indevidamente nem sempre será passível de identificação, bem como o caminho percorrido pelos dados pessoais após um vazamento, não pode ser demonstrado de maneira afirmativa, sempre será uma probabilidade.

No tocante a Inversão do ônus da prova, prevista no art. 42, parágrafo 2º da LGPD, é possível o juiz conceder quando forem verossímeis os fatos alegados, quando houver hipossuficiência para fins de produção de prova e quando a prova pelo titular for excessivamente onerosa.

Diante do exposto, a responsabilidade civil na Lei Geral de Proteção de Dados é um tema com muitos desdobramentos e discussões, como será visto a seguir, os diferentes argumentos e classificações defendidas por diversos doutrinadores.

### **2.3 Pressupostos da Responsabilidade Civil na LGPD**

Pode-se identificar duas situações de responsabilidade civil na LGPD: a) Violação de normas jurídicas, do microssistema e proteção de dados; b) Violação das normas técnicas, voltadas à segurança e proteção de dados pessoais. Em ambas, só será caracterizada a

---

<sup>110</sup> MULHOLLAND, op. cit.

<sup>111</sup> SCHREIBER, op. cit.

responsabilidade civil se a violação de normas jurídicas ou técnicas lesar a algum titular de dados ou a uma coletividade<sup>112</sup>.

A LGPD estabelece regras referentes à responsabilidade civil dos agentes de tratamento de dados pessoais, nos seus artigos 42 a 45, como visto, porém, também inaugura um debate doutrinário a respeito da natureza da obrigação de indenizar, se é subjetiva ou objetiva, tendo em vista que o legislador não deixou claro qual foi a espécie de responsabilidade adotada.

Diante disso, identificar qual o regime de responsabilidade civil instituído pela LGPD não é tarefa simples. Por mais que o art. 42, como visto anteriormente, remeta a compreensão de uma responsabilidade civil objetiva, a lei não é explícita e nem inclui o termo “independente de culpa”, algo que nem o Código de Defesa do Consumidor e o Código Civil fizeram, o que abre interpretação para abranger também uma responsabilidade subjetiva<sup>113</sup>.

A responsabilidade subjetiva será aquela pautada na culpa, que por si só já é um termo que abre margem a mais de uma interpretação, hoje é vista como a violação a um dever jurídico. Segundo o artigo 44 da Lei, o tratamento irregular é entendido como aquele que viola a segurança, ou seja, apenas quando o controlador deixar de seguir as normas de segurança, estipuladas no art. 46. Sendo assim, trata-se aí, de uma responsabilidade subjetiva, pois depende do descumprimento dos deveres jurídicos previsto na lei.

Como dito pela autora Caitlin Mulholland<sup>114</sup>, o Capítulo VI da LGPD - artigos 46 a 54<sup>115</sup> - são *standards* de conduta a serem seguidos pelos agentes de tratamento de dados para a segurança, sigilo, boas práticas e governança de dados, e seriam esses os fundamentos para o reconhecimento de uma responsabilidade subjetiva.

Observa-se também, que a LGPD adota o fundamento da responsabilidade civil objetiva, impondo aos agentes de tratamento a obrigação de indenizar os danos causados aos titulares de dados, independente da comprovação de conduta culposa ou dolosa por parte do agente de tratamento de dados.

Porém, o debate sobre o tema se estende além do texto legal e avança pela doutrina, podendo ser a obrigação de indenizar de natureza subjetiva, ou seja, baseada na falta a um dever de conduta imposto ao agente de tratamento, ou objetiva, pautada no risco da atividade desenvolvida pelos agentes, conforme será analisado a seguir.

---

<sup>112</sup> CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. *Cadernos Jurídicos*, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

<sup>113</sup> Ibid.

<sup>114</sup> MULHOLLAND, op. cit.

<sup>115</sup> BRASIL, op. cit., nota 63.

Segundo as autoras Gisela Sampaio e Rose Meireles<sup>116</sup>, a LGPD adotou claramente a teoria subjetiva da responsabilidade civil, só sendo responsabilizado o agente de tratamento de dado se provada a conduta culposa dele na ocasião do dano. E essa deve ser fundamentada na omissão na adoção de medidas de segurança para o tratamento adequado dos dados, ou no descumprimento das obrigações impostas na lei. Os artigos 46 a 54 da LGPD, são vistos pelas autoras como *standards* de conduta a serem seguidos pelos agentes de tratamento de dados em respeito a segurança, sigilo, boas práticas e governança de dados, e isso que embasa a responsabilidade subjetiva.

A violação da lei é elemento subjetivo da obrigação de indenizar. Ao analisar-se o artigo 43, da LGPD, o inciso II, se observa que ele indica a adoção de uma excludente tipicamente relacionada às hipóteses de responsabilidade civil subjetiva ao estatuir que só não serão responsabilizados se, ainda que exista o dano, não houver violação da legislação de proteção de dados, segundo a corrente defendida pelas autoras supracitadas, não haverá obrigação de indenizar quando o agente de tratamento demonstrar que observou os *standards* esperados e o incidente ocorreu sem ser por culpa de sua atividade<sup>117</sup>.

O legislador ainda cria uma série de deveres e cuidados que devem ser seguidos pelo controlador e pelo operador, para só assim serem responsabilizados, também de acordo com Gisela Sampaio da Cruz Guedes e Rose Melo Venscelau Meireles<sup>118</sup>, a lei dá pistas de que realmente adotou o regime da responsabilidade subjetiva. Como na Seção “Responsabilidade e Ressarcimento de danos” que trás condições que, se não cumpridas, o agente será responsabilizado.

Outro ponto de destaque que as autoras levaram é a Lei trazer um capítulo dedicado a “segurança e boas práticas”, nele a LGPD trás uma série de deveres que devem ser observados pelo agentes de tratamento de dados, estabelecendo *standards* de conduta que devem ser seguidos pelo agente de tratamento de dados, sendo assim, a Lei de modo geral adotou a responsabilização subjetiva.

Esse *standard* de conduta que a Lei apresenta pode ser visto também nos princípios da responsabilização e da prestação de contas, o que só corrobora com isso, pois só será responsabilizado o agente que não cumprir com o comportamento esperado de acordo com a Lei. Logo, não será analisado só o dano em si, como também o que tais agentes fizeram para

---

<sup>116</sup> GUEDES, Gisela Sampaio da Cruz; TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde. *Fundamentos do Direito Civil* V.4. Rio de Janeiro: Forense, 2020, p. 231.

<sup>117</sup> MULHOLLAND, op. cit.

<sup>118</sup> GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, "Término do tratamento de dados", IN: TEPEDINO; FRAZÃO; OLIVA, op. cit., p. 231.

evitar o dano ou diminuir seus efeitos<sup>119</sup>.

Gisela Sampaio e Rose Melo<sup>120</sup> também citam o artigo 43, inciso II, da Lei como outra demonstração da responsabilidade subjetiva da lei, pois, de acordo com ele, os agentes de tratamento de dados só não serão responsabilizados, quando provarem que, embora tenham realizado o tratamento dos dados, não violaram a legislação de proteção de dados. Assim, esse inciso remete à ideia de culpa como fundamento da responsabilidade civil, se distanciando do que prega um regime de responsabilidade objetiva.

Enquanto que os incisos I e III, do art. 43 da LGPD, tratam do nexo de causalidade entre o agente e o dano, para esse ser eximido de responsabilização, o inciso II vai além, mesmo havendo o nexo de causalidade entre o agente e o dano, a responsabilidade dele pode ser afastada se ele conseguir provar que cumpriu todos os deveres impostos pela legislação, incluindo as medidas de segurança recomendadas. Portanto, provando que observou o *stantard* esperado, mesmo que o incidente ocorra, não será em razão de conduta culposa, refletindo ainda mais forte a responsabilidade subjetiva pilar da Lei<sup>121</sup>.

Outro entendimento sobre o tema é dos autores Maria Celina Bodin de Moraes e João Quinelato<sup>122</sup>, que acreditam que a LGPD adota a chamada Teoria Ativa ou Proativa da Responsabilidade Civil. Essa Teoria indica a necessidade de olhar-se a responsabilidade civil de um ponto de vista positivo, sustentado pela necessidade da adoção de posturas pelos agentes de tratamento de dados que tutelem a prevenção de danos, nesse caso a obrigação de indenizar é a exceção.

De acordo com esses autores, os dados pessoais constituem conteúdos do direito à privacidade, por isso, a coleta e tratamento deve ser precedida de medidas rigorosas e eficazes de proteção, especialmente em relação aos dados de cunho sensível. A responsabilidade proativa da qual tratam, está justificada no art. 6º, X, da LGPD, que propõe a responsabilização com prestação de contas feita pelos agentes de tratamento de dados pessoais, inclusive, tendo eles que demonstrar as medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados<sup>123</sup>.

Nesse caso, o legislador não pretendeu só a responsabilização para ser ressarcido, mas também prevenir e evitar a ocorrência de dano. Por isso, não basta que o agente só cumpra a

---

<sup>119</sup> Ibid.

<sup>120</sup> Ibid.

<sup>121</sup> Ibid.

<sup>122</sup> 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.

<sup>123</sup> MULHOLLAND, op. cit.

lei, há um conjunto de condutas que o agente deve preventivamente cumprir, como analisar adequadamente como irá ocorrer o processamento de dados pessoais, implementando medidas adequadas e eficazes para sua segurança<sup>124</sup>.

Desse modo, a prestação de contas é a demonstração, pelos envolvidos, de que adotaram medidas de segurança eficazes e são capazes de se comprovar a observância e cumprimento das normas de proteção de dados, como também a eficácia dessas medidas. Sendo assim, a prevenção e prestação de contas, são fatores de máxima importância.

O RIPD, Relatório de Impacto a Proteção de Dados, é um modelo de responsabilidade proativa, pois trás a prevenção de danos em matéria de proteção de dados. Esse documento visa a conformidade regulatória, a ser elaborada pelo operador no intuito de demonstrar suas ações no tratamento de dados, nele estão indicadas as medidas que devem ser adotadas para mitigar riscos, documento que, inclusive, deve ser gerado antes do início do tratamento de dados.

Outra corrente sobre o tema é defendida por Danilo Doneda e Laura Mendes<sup>125</sup>, que consideram que a atividade de tratamento de dados possui um risco intrínseco, na medida em que há uma potencialidade danosa considerável em caso de violação desses direitos, que são, por sua natureza, integrantes dos direitos personalíssimos e dos direitos fundamentais.

Tendo em vista um dos principais fundamentos da LGPD, que é a diminuição dos riscos e danos, embasado no art. 6º, III, é que os autores alegam que o legislador optou por um regime de responsabilização objetiva, vinculado ao exercício da atividade de tratamento de dados pessoais a um risco inerente, que potencialmente será danoso aos seus titulares<sup>126</sup>.

Por isso, tanto o artigo 42, quanto o artigo 44, da LGPD, adotam o fundamento da responsabilidade civil objetiva, impondo aos agentes de tratamento a obrigação de indenizar pelos danos causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador.

Além disso, as atividades desenvolvidas pelo agente de tratamento é evidentemente uma atividade que impõe riscos aos direitos dos titulares de dados, que, por sua vez, são intrínsecos, inerentes à própria atividade e resultam em danos a direito fundamental. Os danos decorrentes de vazamento de dados são, por si só, quantitativamente elevados e qualitativamente graves, podendo ainda atingir direitos difusos, o que já justificaria a adoção

---

<sup>124</sup> FRANZOLIN, Cláudio José; VALENTE, Victor Augusto Estevam. Alguns apontamentos sobre a responsabilidade ativa mediante a prestação de contas e a prevenção de danos por meio de conformidades. *Revista de Direito do Consumidor*. V. 133. Ano 30. p. 75-106. São Paulo: RT, jan./fev. 2021. Disponível em: <<https://dspace.almg.gov.br/handle/11037/4015>>. Acesso em: 26 mai. 2021.

<sup>125</sup> MENDES, Laura Schertel; DONEDA, D. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555, 2018.

<sup>126</sup> MULHOLLAND, op. cit.

da responsabilidade civil objetiva, tal como no caso dos danos ambientais e dos danos causados por acidentes de consumo.

Além disso, é feita uma analogia entre a nova Lei e o CDC, como já visto neste trabalho, que embasa também a compreensão da LGPD se pautar na responsabilidade objetiva. Inclusive, a nova Lei visa limitar o tratamento dos dados para diminuir os riscos de vazamento, contudo, o próprio tratamento se mostra um processo repleto de riscos intrínsecos<sup>127</sup>.

No tocante ao tratamento de dados sensíveis, o tema passa a ser menos divergente, sendo amplo entendimento que nesses casos de incidentes envolvendo esses dados se aplica a responsabilidade objetiva, podendo ser aplicado até o art. 927, do Código Civil<sup>128</sup> para isso.

Outro ponto dentro do tema que merece ser abordado, é a responsabilidade civil pelas operações de dados após o término do tratamento. A Lei Geral de Proteção de Dados prevê expressamente, em seu art. 16, a possibilidade de conservação dos dados pessoais após o término de seu tratamento, num rol taxativo, não podendo ocorrer nos demais casos, nos quais o controlador deve descartá-los tão logo ocorra o encerramento do tratamento nos termos do art. 15 da LGPD, podendo ser responsabilizado caso não o faça, presente os pressupostos da responsabilidade civil vistos acima<sup>129</sup>.

Diante de tudo apresentado, buscou-se apenas a indicação na lei dos indicativos do pressupostos de responsabilidade na LGPD, mas há divergência interpretativa. das diversas correntes e fortes argumentos acerca dos pressupostos. pode-se dizer que o tema seguirá sendo debatido e enfrentado, sobretudo na jurisprudência daqui em diante, para que seja aplicada o regime de responsabilização mais adequado em cada caso. Contudo, fazendo uma leitura sistêmica parece que o legislador quis trazer na lei um regime de responsabilidade civil subjetiva, mas isso está longe de ser uma questão de fácil solução, tanto que será tratado com mais profundidade o tema no capítulo seguinte.

---

<sup>127</sup> GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, "Término do tratamento de dados", IN: TEPEDINO; FRAZÃO; OLIVA, op. cit., p. 236.

<sup>128</sup> BRASIL, op.cit., nota 2.

<sup>129</sup> GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, "Término do tratamento de dados", IN: TEPEDINO; FRAZÃO; OLIVA, op. cit., p. 236.



### 3. A EFETIVIDADE DA INDENIZAÇÃO DECORRENTE DA RESPONSABILIDADE CIVIL NA ÁREA DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados<sup>130</sup> visa regulamentar o tratamento de dados pessoais no país. Como visto ao longo deste processo, a responsabilidade civil na LGPD é tema extremamente importante de ser analisado, inclusive para compreender seus reflexos na prática. Por isso, o presente capítulo busca compreender qual o regime de responsabilidade civil decorrente da LGPD tem sido aplicado nos casos concretos.

Para tal, é preciso compreender se o dano a ser reparado é patrimonial ou extrapatrimonial, o que fará grande diferença na hora de requerer seu ressarcimento. Bem como entender os diferentes papéis do controlador e do operador de dados, e suas respectivas responsabilidades dentro do processo de tratamento de dados.

Para tanto, é necessário que se compreendam as duas grandes correntes dessa responsabilização, isto é, (i) a que entende a responsabilização como objetiva, na qual o simples incidente de vazamento de dados já comprova o dever de indenizar, dispensando a comprovação do dano, ou (ii) a corrente que compreende que é preciso que ocorra um dano direto e comprovado ao titular do dado para que o mesmo seja indenizado, deste modo, não bastando a mera exposição dos dados no vazamento.

No presente capítulo, também será feita uma análise da jurisprudência brasileira acerca dos casos de violação dos dados pessoais, antes e posterior a LGPD, bem como um estudo comparativo com as legislações internacionais sobre o tema, e como a responsabilidade civil decorrente delas tem acontecido na prática em outros países.

#### **3.1 Responsabilidade Civil do Controlador e do Operador de Dados**

Antes de adentrar a efetividade da indenização dos danos decorrentes da violação de dados pessoais, é necessário identificar qual dano há de ser reparado. Como previsto no art. 42 da LGPD<sup>131</sup>, tanto os danos patrimoniais quanto os extrapatrimoniais devem ser ressarcidos, controlador e operador que causarem dano patrimonial, moral, individual ou coletivo, durante o exercício de atividade de tratamento de dados pessoais, são obrigados a agir no intuito de repará-los.

O primeiro passo antes de buscar uma reparação é identificar esses danos na prática.

---

<sup>130</sup> BRASIL, op. cit., nota 63.

<sup>131</sup> Ibid.

O dano patrimonial é mais facilmente identificado pela maior possibilidade de, na maioria das vezes, atestar sua deterioração, contudo, os danos extrapatrimoniais possuem especificidades que dificultam a identificação e comprovação.

Os danos extrapatrimoniais ou morais, sendo configurados quando a ofensa se dá em relação à dignidade da pessoa humana, caracterizada pela lesão de direitos de cunho personalíssimo, portanto, não quantificáveis economicamente, referem-se a toda mácula à bens jurídicos não-patrimoniais ou imateriais pela sua própria natureza subjetiva.

Para compreender melhor o que seria esse dano observa-se o que diz os doutrinadores, Pablo Stolze e Rodolfo Pamplona Filho<sup>132</sup>:

O dano moral consiste na lesão de direitos cujo conteúdo não é pecuniário, nem comercialmente redutível a dinheiro. Em outras palavras, podemos afirmar que o dano moral é aquele que lesiona a esfera personalíssima da pessoa (seus direitos da personalidade), violando, por exemplo, sua intimidade, vida privada, honra e imagem, bens jurídicos tutelados constitucionalmente.

Dentro do âmbito da proteção de dados, os danos extrapatrimoniais podem ser causados, por exemplo, pela exposição de dados pessoais, sobretudo, de dados sensíveis dos titulares de dados. Ocorrendo ainda dentro do ambiente virtual, se espalham rapidamente e por diversas localidades, gerando consequências de dimensões imensuráveis, deixando rastros incalculáveis e um difícil cenário para buscar a restauração da imagem do titular, bem como a reparação do dano causado.

Os agentes dentro do processo de dados são o Controlador - podendo ser pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais - , Operador - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador - e Encarregado pela Proteção de Dados - pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)<sup>133</sup>.

Para compreender a responsabilidade dos agentes de tratamento de dados, primeiramente, analisa-se o art. 42<sup>134</sup> da Lei, de acordo com ele tanto controlador quanto operador são considerados sujeitos responsáveis, sendo o Controlador a pessoa a quem competem as decisões referentes ao tratamento de dados pessoais, como já mencionado. Enquanto o operador é o indivíduo que realiza o tratamento de dados pessoais em nome do

<sup>132</sup> STOLZE, Pablo; PAMPOLHA FILHO, Rodolfo. *Novo Curso de Direito Civil: Responsabilidade Civil*. 10. ed. São Paulo: Saraiva, 2013, p. 97.

<sup>133</sup> FONSECA, op. cit., p. 141.

<sup>134</sup> BRASIL, op. cit., nota 63.

Controlador.

A LGPD não fala da responsabilidade civil do encarregado, contudo ela poderá questionar quando essa função for exercida por uma pessoa natural ou jurídica destacada, sem ser o controlador ou o operador, e por estarem todos dentro da mesma cadeia de produção, poderá o encarregado ser responsabilizado de forma solidária<sup>135</sup>.

Dentro da discussão da responsabilidade civil é preciso estar atento também a vulnerabilidade e a segurança da informação. A vulnerabilidades, quando descobertas, devem ser catalogadas, permitindo que os responsáveis pela segurança da informação da empresa adotem medidas técnicas para prevenir tais incidentes.

Diante disso, ocorrendo um dano pelo não atendimento de alguma norma técnica, relativa a vulnerabilidade, que já seja conhecida e documentada, será evidente a negligência do agente de tratamento. Mas, se o dano não decorrer de uma vulnerabilidade documentada, eximem-se de qualquer responsabilização. Portanto, por mais que o agente de tratamento tenha o dever de segurança e proteção de dados em toda e qualquer hipótese, a obrigação de segurança é de meio e não de resultado.

A base para tal entendimento está no artigo 44 da LGPD, em seu parágrafo único, restringe a responsabilidade do controlador ou operador aos casos em que houvessem deixado de adotar as medidas expostas no art. 46 da respectiva Lei. Nesse artigo, estão previstas medidas de segurança que devem ser adotadas no tratamento de dados<sup>136</sup>.

Controlador e operador, via de regra, respondem individualmente pelos danos que efetivamente causarem em razão do tratamento de dados pessoais, como previsto no art. 42, *caput*. Contudo, essa responsabilidade pode ser solidária, no parágrafo 1º do mesmo artigo, prevê hipóteses específicas disso, tendo assim o legislador deixado claro sua busca para que às vítimas tenham uma devida efetiva diante de incidentes de proteção de dados.

Uma obscuridade que pode ser levantada diante da análise desse art. 42 é que por mais que esteja prevista uma responsabilidade solidária entre controlador e operador, não é dito com que outro responsável se daria essa solidariedade.

Veja as hipóteses em que o operador responderia solidariamente, previstas no inciso I, artigo 42, da LGPD<sup>137</sup>:

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;

<sup>135</sup> CAPANEMA, op. cit., nota 105.

<sup>136</sup> SCHREIBER, op. cit., p. 331.

<sup>137</sup> BRASIL, op. cit., nota 63.

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.

Observa-se que ambas as hipóteses configuram caso de violação à legislação de proteção de dados, por isso, o operador já responderia diretamente pelo *caput* do art. 42 da LGPD, e sendo provada autônoma sua conduta, só ele responderia pelo incidente, com nada a ser responsabilizado na conduta do controlador.

Apenas no caso das supracitadas hipóteses do inciso I, quando se referirem ao controlador, pode ser configurado um caso de responsabilização solidária. Contudo, segundo Anderson Schreiber<sup>138</sup>, interpretando a norma, mesmo quando a lesão for causada por fato imputável exclusivamente ao operador, o controlador pode ser chamado a responder solidariamente, devido a posição que ocupa dentro do processo de tratamento, de modo a garantir a efetiva indenização da vítima.

Ambos os casos previstos no mesmo inciso se referem a responsabilidade civil subjetiva, ou seja, pressupõe culpa por parte do operador. Com isso, caso o dano ocorresse por um defeito na segurança do tratamento realizado pelo operador, estaria configurada a responsabilidade objetiva e, portanto, estaria excluída a responsabilidade solidária do controlador, pois, a solidariedade tem fonte legal ou negocial, não podendo ser presumida, de acordo com o art. 265 do Código Civil<sup>139</sup>.

Ressalta-se que essa solidariedade foi colocada na lei com o intuito de proteger o efetivo ressarcimento da vítima e não de punir o controlador. Como no caso da inversão do ônus da prova a favor do titular de dados, sendo verossímil as alegações, e havendo hipossuficiência para fins de produção de prova, ou quando essas forem excessivamente onerosas, pode o juiz determinar essa inversão, como já visto no presente trabalho.

Passando para a análise do inciso II do artigo 42 da LGPD, percebe-se que não é tão eficaz na prática, já que o *caput* do mesmo artigo trata rigorosamente da responsabilidade dos agentes, sendo esse inciso até desnecessário nesse aspecto. Contudo, é de extrema importância tal inciso pois prevê a responsabilidade solidária entre os controladores, ou seja, identifica a possibilidade de diversos controladores serem responsabilizados solidariamente pelo mesmo incidente, desde que devidamente envolvidos<sup>140</sup>.

Além de prever a solidariedade passiva, a lei também dispõe sobre direito de regresso,

---

<sup>138</sup> SCHREIBER, op. cit., p. 332.

<sup>139</sup> BRASIL, op. cit., nota 2.

<sup>140</sup> SCHREIBER, op. cit., p. 333.

no seu artigo 42, parágrafo 4<sup>o</sup><sup>141</sup>, que diz: “aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso”. Sendo assim, o devedor solidário que satisfaz o crédito tem o direito de exigir de cada um dos seus codevedores a parte que lhe cabe na responsabilidade solidária. Com isso, o titular do dado pessoal pode pleitear, em juízo, a integralidade do dano perante qualquer dos responsáveis, posteriormente que será analisado a responsabilidade e valor devido por cada um entre eles.

Ademais, como também previsto na lei, por mais que possam exercer o direito de regresso, a responsabilidade de cada um dos devedores será quantificada com base na sua contribuição causal para o dano, examinando o nexo de causalidade e as excludentes de responsabilidade civil.

Nos casos que o controlador é um ente público, a Lei Geral de Proteção de Dados dedicou o Capítulo IV “Do tratamento de dados pessoais pelo Poder Público”, com inegáveis reflexos em seu sistema de responsabilidade civil. Nesses casos, a lei dispensou um conjunto de deveres específicos em decorrência do tratamento de dados pessoais e traçou normas reguladoras do uso compartilhado de suas bases de dados entre órgãos da administração pública e entre este e um ou mais entes privados.

A Lei não trata especificamente da responsabilidade civil dos entes públicos quando da verificação de danos decorrentes de tratamento de dados pessoais, porém, ao analisar na prática, a responsabilidade civil do ente público se dá com fundamento na teoria do risco administrativo<sup>142</sup>.

Nos tempos atuais, a preocupação de responsabilidade do poder público é ainda maior, pois espera-se do poder público um planejamento de políticas públicas baseado em dados, de modo a garantir a eficiência em sua implementação, desde que leve em consideração o risco decorrente.

O Supremo Tribunal Federal<sup>143</sup> já se manifestou sobre o tema, dizendo que a responsabilidade estatal no espectro das atividades de tratamento de dados pessoais é analisada segundo os critérios da responsabilidade objetiva para os atos comissivos e, por outro lado, segundo os pressupostos da responsabilidade subjetiva em se tratando de ato omissivo, como no caso da não observância das normas de prevenção e de segurança da informação a

---

<sup>141</sup> BRASIL, op. cit., nota 63.

<sup>142</sup> CAPANEMA, op. cit., nota 112.

<sup>143</sup> TASSO, Fernando Antonio. *A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor*. Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 97-115, jan.-mar./2020. Disponível em: <[https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii\\_1\\_interface\\_entre\\_a\\_lgpd.pdf?d=637250344175953621](https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_a_lgpd.pdf?d=637250344175953621)>. Acesso em: 04 jun. 2022. p.105.

oportunizar o vazamento de dados pessoais dos cidadãos.

Já nos casos em que o controlador for pessoa física ou pessoa jurídica de direito privado, há de se analisar o sistema de configuração da responsabilidade civil não somente observando o critério pessoal, como também é importante destacar a relação jurídica subjacente, tal como será feito, no próximo capítulo, em uma interpretação sistemática dos diplomas jurídicos existentes no ordenamento jurídico brasileiro, como já tratados pela jurisprudência.

Importante ressaltar que também é viável a responsabilização dos agentes de tratamento nos casos de violação e reparação de danos coletivos, ou seja, quando um vazamento atingir diversas vítimas. O art. 42, parágrafo 3º da Lei<sup>144</sup>, prevê inclusive que, nesses casos, a reparação pode ser exercida coletivamente em juízo, de acordo com o já previsto na legislação brasileira acerca dessa temática. Passa-se agora à análise do Código de Defesa do Consumidor<sup>145</sup>, no seu artigo 81, III, prevê a propositura de ações judiciais coletivas voltadas à reparação de danos morais individuais, desde que resultem da lesão a interesses individuais homogêneos, ou seja, que decorram de uma origem em comum<sup>146</sup>.

Nesses casos, a ação será coletiva, mas os danos continuarão sendo individuais, diferentemente do dano coletivo, que também pode ser visto no campo do tratamento de dados pessoais. A própria LGPD explicita isso, no *caput* do art.42, como diversos dados pessoais venham a ser utilizados mas não para a finalidade informada ao titular no momento da obtenção do consentimento, mas sim para outro propósito, nesses casos, podendo também ser requerida a reparação por meio de ações coletivas, e como não haja uma regulamentação geral para elas no Brasil, a Lei da Ação Civil Pública é que exerce essa função na maioria dos casos.<sup>147</sup>

Sendo assim, após a análise quanto ao dano patrimonial e extrapatrimonial decorrente dos incidentes de segurança, e depois de entender os diferentes papéis do controlador e do operador de dados, bem como suas respectivas responsabilidades dentro do processo de tratamento de dados, a seguir observa-se a questão-problema exposta: a responsabilidade civil da LGPD é objetiva, dispensa a comprovação do dano, isto é, o simples incidente de vazamento de dados já comprova o dever de indenizar, ou é subjetiva, sendo preciso que ocorra um dano direto ao titular do dado e que esse seja comprovado para ser indenizado, não bastando a mera exposição dos dados no vazamento?

---

<sup>144</sup> Ibid.

<sup>145</sup> BRASIL, op. cit., nota 47.

<sup>146</sup> SCHREIBER, op. cit., p. 335.

<sup>147</sup> Ibid.

### 3.2 Responsabilidade Civil Objetiva nos casos de vazamento de dados

A proteção de dados como direito autônomo se faz necessária com as novas situações factuais que ensejam proteção legal, por decorrerem do puro e simples tratamento de dados pessoais, como, por exemplo, o perfilamento racial, as listas negras de trabalhadores que já demandaram na Justiça do Trabalho contra seus patrões, testes genéticos pré-admissionais e identificações biométricas em gravações de vídeo de espaços públicos.

Ao analisar esses casos isoladamente, constata-se que eles não violam intimidade ou a vida privada, contudo, no contexto do tratamento de dados, e com a utilização massiva de dados pessoais, esses passam a ser produtores de novos valores passíveis de proteção, pois repercutem em direitos e garantias fundamentais, como a igualdade, o livre exercício profissional, a dignidade da pessoa humana e a liberdade de expressão<sup>148</sup>.

Observando a responsabilidade civil no âmbito da LGPD a primeira impressão quanto ao sistema adotado pela lei protetiva é de uma certa imprecisão. Pelos doutrinadores da área, é travado um embate entre posições que afirmam ter a lei estabelecido um sistema baseado na responsabilidade objetiva ou subjetiva, sendo respeitáveis e necessário analisar os posicionamentos em ambos os sentidos.

Primeiramente, analisa-se a responsabilidade civil objetiva, é aquela que prescinde do elemento culpa. Carlos Roberto Gonçalves traz a seguinte definição sobre:

A classificação corrente e tradicional, pois, denomina objetiva a responsabilidade que independe de culpa. Esta pode ou não existir, mas será sempre irrelevante para o dever de indenizar. Indispensável será a relação de causalidade entre a ação e o dano, uma vez que, mesmo no caso de responsabilidade objetiva, não se pode acusar quem não tenha dado causa ao evento.<sup>149</sup>

Uma das teorias desenvolvidas para explicar a responsabilidade objetiva é a denominada Teoria do Risco, essa prevê que toda pessoa que exerce alguma atividade com risco de dano para terceiros deve ser obrigada a repará-lo caso este venha a se concretizar, ainda que não possua culpa sobre o resultado danoso.

O Código Civil de 1916 inaugurou, dentre as hipóteses de responsabilidade objetiva, a responsabilidade objetiva, da mesma forma, o Código de Defesa do Consumidor (1990) previu a responsabilidade objetiva por fato do produto ou serviço e, posteriormente, o Código Civil consagrou cláusula geral de responsabilização civil daquele que desenvolve atividade de

---

<sup>148</sup> TASSO, op. cit., p.105.

<sup>149</sup> GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro: Responsabilidade Civil*. 7. ed. V.4. São Paulo: Saraiva, 2012, p. 18.

risco, no parágrafo único do artigo 927, onde acolhe expressamente a Teoria do Risco. Ela também pode ser vista no art. 931 e em outros dispositivos de Leis específicas.

A legislação de proteção de dados visa a diminuição de riscos de dano, como pode ser visto no artigo 6, III da lei, que fala da necessidade que impõe a limitação do tratamento ao mínimo necessário de obtenção e interferência nos dados pessoais.

Esse, dentre outros trechos, demonstram a finalidade da lei e dos princípios por ela adotados, como o da necessidade, minimização, responsabilidade e prestação de contas, entre outros, que levam a conclusão que os legisladores optaram por um regime de responsabilidade objetiva, vinculando o exercício da atividade de tratamento de dados pessoais a risco inerente, possível de lesar seus titulares.

Como pode ser constatado, a lei prevê essa mitigação de riscos, ou seja, preza pelo reconhecimento prévio dos riscos relacionados à atividade que o controlador ou operador desenvolve, bem como também estima a ação de tomar medidas para evitar o dano, estabelecendo que a estes cabe agir de modo a se resguardarem para evitar que ocorram situações nas quais tenham que reparar os danos, por meio da gestão de riscos relacionados à atividade desenvolvida.

Como já visto, o art. 44 da Lei trata das hipóteses em que se reconhece que haverá tratamento irregular de dados, que são nos casos em que o agente deixar de observar a legislação ou não oferecer a segurança que o titular dele pode esperar. Isso leva ao conceito de tratamento irregular de dados que deve ser analisado considerando o modo como o tratamento é realizado, bem como o resultado e os riscos razoavelmente esperados pelo tratamento.

Nesse sentido, o parágrafo único do art. 44 prevê que o controlador ou o operador serão obrigados a indenizar os danos decorrentes da violação dos dados quando esses deixarem de adotar as medidas de segurança previstas no art. 46 da LGPD.

Além disso, o art. 42 traz o operador e o controlador podendo responder solidariamente pelos danos causados ao titular. Além disso, haverá a possibilidade de inversão do ônus da prova a favor do titular de dados, semelhante ao que ocorre nas relações de consumo hoje em dia, em favor do consumidor.

Sendo assim, observa-se que tanto o artigo 42 quando o artigo 44 da Lei adotam o fundamento da responsabilidade civil objetiva, isto é, impondo aos agentes de tratamento a obrigação de indenizar os danos causados aos titulares, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador.



Autores como Danilo Doneda e Laura Schertel Mendes<sup>150</sup> defendem essa corrente, considerando que a atividade de tratamento de dados encerra um risco intrínseco, na medida em que há uma potencialidade danosa considerável em caso de violação desses direitos, que por sua vez são direitos personalíssimos e fundamentais. Por isso, do art. 42 observa-se que o legislador optou por um regime de responsabilidade objetiva, vinculando a obrigação de reparação do dano ao exercício de atividade de tratamento de dados pessoais.

No mesmo sentido, Caitlin Mulholland<sup>151</sup> argumenta pela adoção do regime objetivo:

[...] o legislador quis identificar nessa hipótese situações danosas que decorrem especificamente de incidentes de segurança que são, por sua vez, acontecimentos que se relacionam ao risco inerente ao desenvolvimento da atividade de tratamento de dados, como vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados. Neste sentido, esses riscos devem ser necessariamente situados como intrínsecos à atividade de tratamento de dados e, portanto, considerados, em última análise, como hipótese de fortuito interno, incapazes de afastar a obrigação dos agentes de tratamento de indenizar os danos causados pelos incidentes.

Maria Cecília Oliveira Gomes<sup>152</sup> também defende a responsabilidade objetiva, ela diz que uma vez que o risco é inerente ao tratamento de dados, deve-se identificá-lo, compreendê-lo e avaliar seu impacto para assim mitigá-lo, de modo a preservar e proteger os direitos dos titulares de dados, o que nem sempre é feito em algumas metodologias baseadas em risco. Isso serve para demonstrar conformidade ao regulamento de dados, e não para avaliar possíveis violações aos direitos dos titulares, pois esses já foram violados com o vazamento.

A autora defende uma análise preventiva de riscos tendo como norte as liberdades civis e direitos fundamentais dos titulares de dados, buscando a mitigação de danos, explicitando a natureza intrínseca do risco na atividade de tratamento de dados, isso pode ser observado na análise dos princípios e fundamentos que demandam dos agentes de tratamento uma atuação preventiva para o cumprimento das normas de proteção de dados pessoais.

O entendimento predominante no Superior Tribunal de Justiça atualmente sobre o tema é favorável à responsabilidade civil objetiva, inclusive já é anterior a vigência da LGPD, como pode ser visto no Resp nº 1758799 (2017/0006521-9 de 19/11/2019)<sup>153</sup>. Neste caso citado, determinado consumidor ajuizou ação de indenização por danos morais em face da PROCOPB

<sup>150</sup> MENDES; DONEDA, op. cit.

<sup>151</sup> MULHOLLAND, op. cit.

<sup>152</sup> GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In: PALHARES, Felipe (coord.). *Temas Atuais de Proteção de Dados*. São Paulo: Thomsom Reuters Brasil, 2020, p. 245-273.

<sup>153</sup> BRASIL. Superior Tribunal de Justiça. *Resp. nº 1758799 MG 2017/0006521-9*, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 12/11/2019, T3 - TERCEIRA TURMA, Data de Publicação: DJe 19/11/2019). Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/859849413/recurso-especial-resp-1758799-mg-2017-0006521-9/inteiro-teor-859849423?ref=serp>>. Acesso em: 08 jun. 2022.

S/A, em maio de 2013. A empresa ré tinha como atividade principal o desenvolvimento de programas de computador sob encomenda e como atividades secundárias as de cobranças e fornecimento de informações cadastrais. Ocorre que os dados pessoais do consumidor, como nome, idade, endereço, signo, e CPF, estavam disponíveis no banco de dados da empresa, ao qual qualquer pessoa poderia ter acesso por meio do cadastro e pagamento de um valor irrisório.

Segundo a decisão, o compartilhamento de informações de banco de dados deverá ser notificado aos consumidores de antemão sobre a utilização de seus dados, caso contrário, estarão sujeitos a multas por danos morais aos consumidores eventualmente afetados.

O fato das informações serem fornecidas pelo consumidor no ato da compra, ou até mesmo serem divulgadas em redes sociais, não omite a responsabilidade do gestor do banco de dados de comunicar sobre o compartilhamento dos dados do consumidor. Veja<sup>154</sup>:

RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial (...) 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência - CDC e Lei 12.414/2011 - dentre as quais se destaca o dever de informação (...) 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor - dentre os quais se inclui o dever de informar - faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais (...) 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento (...) de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa. (...) Recurso especial conhecido em parte e, nessa extensão, desprovido.

Essa decisão do STJ, segundo a Ministra relatora Nancy Andriighi, em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, deve ser observada a regra do inciso V do artigo 5º da Lei nº 12.414/2011, na qual assegura-se ao cadastrado o direito de ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais. O dano moral, nesses casos de compartilhamento das informações sem prévia informação, é presumido, ou seja, *in re ipsa*, sendo desnecessário ao consumidor comprovar prejuízo<sup>155</sup>.

<sup>154</sup> Ibid.

<sup>155</sup> BRASIL. Superior Tribunal de Justiça. *Compartilhamento de informações de banco de dados exige notificação prévia ao consumidor*. Disponível em: <<https://www.stj.jus.br/sites/portallp/Paginas/>

Já a autora Maria Celina Bodin de Moraes<sup>156</sup> acredita que a LGPD adotou um regime de responsabilização civil “proativo”, que seria um regime especial refletido na determinação do disposto no inciso X, art. 6º da LGPD, pois é exigido do agente de tratamento não apenas o ressarcimento dos danos causados mas, principalmente, que se previna contra a ocorrência desses danos.

Segundo a autora, não basta descumprir a Lei, é preciso que as empresas proativamente previnam a ocorrência de danos. Essa responsabilidade civil “proativa” está baseada em um sistema de prestação de contas, semelhante ao conceito de “*accountability*”, no qual o cerne desse instituto não está mais na reparação do dano, mas sim na prevenção de forma eficaz.

Dessa forma, nesse novo formato do instituto da Responsabilidade civil, o seu ponto central não está mais na reparação do dano, mas sim na prevenção de forma eficaz. Isso pode ser extraído do inciso X do art. 6º, de acordo com a própria Lei de proteção de dados, não basta apenas não descumprir a lei, é preciso uma postura proativa das empresas em prevenir a ocorrência de danos<sup>157</sup>.

Contudo, essa postura da LGPD, na medida em que dispõe de mecanismos de responsabilidade preventiva, que tendem a impedir a causação do dano, acaba por subordinar a reparação ao regime da responsabilidade civil subjetiva com todas as dificuldades a ele inerentes, sendo em suma, uma postura contraditória a Lei.

Além disso, contraditória também por permitir que a responsabilidade civil decorrente de um mesmo fato objetivamente considerado, como um caso de violação de normas de proteção de dados, pode gerar tratamento diferenciado conforme a natureza do agente envolvido, sendo, desta forma, subjetiva para agentes privados e objetiva para entes de direito público, já que a responsabilidade desses entes não é explicitamente regulada, ela observará a Teoria do Risco Administrativo, como expresso no art. 37, parágrafo 6º da CF/88.<sup>158</sup>

Ao analisar a Lei, tal posicionamento parece se adequar ao pretendido pelo legislador, que destacou nos princípios da lei a prevenção de danos como o valor máximo a ser perseguido pelos agentes de tratamento, como pôde ser observado no capítulo referente aos direitos dos titulares de dados. A LGPD não adotou de modo explícito as medidas proativas, mas ela pode ser vista tacitamente, como nos princípios da Privacidade por Concepção (*Privacy by design*) e

---

Comunicacao/Noticias/Compartilhamento-de-informacoes-de-banco-de-dados-exige-notificacao-previa-ao-consumidor.aspx>. Acesso em: 08 jan. 2022.

<sup>156</sup> MORAES, Maria Celine Bodin de. *LGPD: um novo regime de responsabilização dito “proativo”*, Civilistica.com, Rio de Janeiro, ano 8, n. 3, 2019. Disponível em: <<http://civilistica.com/lgpd-um-novo-regime/>>. Acesso em: 4 jun. 2022.

<sup>157</sup> Ibid.

<sup>158</sup> NOVAKOSKI; NASPOLINI, op. cit., p. 170.

da Privacidade por Padrão (*Privacy by default*). Ambos se relacionam com a ideia de coleta mínima de dados para a realização das finalidades informadas ao titular de dados.

A privacidade por padrão ou *Privacy by Default* estabelece a ideia de que nenhuma ação precise ser tomada por parte do titular de dados para proteger sua privacidade, pois a proteção de dados pessoais deve ser o padrão, a regra, para o fornecimento de produtos e serviços que utilizam dados pessoais.

A proatividade também pode ser extraída do Princípio da Necessidade, segundo ele o tratamento deve ser limitado ao mínimo necessário para a realização das suas necessidades e também no princípios de mitigação de risco e adoção de mecanismos preventivos para evitar danos aos titulares de dados.

Um caso concreto em que pode ser observado esse tipo de responsabilização foi o da Companhia do Metropolitano de São Paulo - Metrô de São Paulo, quanto a implementação do sistema de reconhecimento facial, objeto do processo nº 1006616-14.2020.8.26.0053. Na ação, é questionada a implementação dessa tecnologia, apontando o potencial violador de direitos constitucionais pelo sistema de reconhecimento facial, como direito à privacidade e à autodeterminação informativa, amparado no Código de Defesa do Consumidor (CDC) e na Lei Geral de Proteção de Dados Pessoais (LGPD), antes mesmo da entrada em vigor da lei<sup>159</sup>.

No caso destaca-se a menção ao risco que é feita com o pedido de produção antecipada de prova e o Metrô-SP não teria revelado a finalidade do tratamento, tampouco a forma de obtenção de consentimento, o que causou mais preocupação ainda nos casos de pais e responsáveis pelos dados pessoais de crianças e adolescentes, além do fato da empresa não informar as ações de mitigação do risco envolvido ou a proposta de compartilhamento da base de dados com outras entidades, públicas ou privadas.

Diante do apresentado sobre a responsabilidade civil “proativa” presente na LGPD, constata-se que o legislador buscou proteger os direitos dos titulares de dados de maneira ativa, ora apontando para a atuação preventiva dos agentes de tratamento, ora apontando para o risco envolvido no tratamento de dados pessoais, buscando a efetiva proteção destes.

Portanto, no tratamento de dados, os riscos, conforme vistos, são intrínsecos a essa atividade, de modo que o reforço do legislador ao princípio da prevenção é compreensível. O sistema de proteção privilegia a prevenção e a reparação de danos, do mesmo modo que na responsabilidade civil atual o que se busca é a máxima reparação do dano e a proteção da vítima.

---

<sup>159</sup> ALVES, Rodrigo da Costa. *Regimes de responsabilidade civil dos agentes de tratamento na lei geral de proteção de dados pessoais – lei nº 13.709/18*. Monografia curso de Direito, Faculdade de Direito – FD/UNB, Universidade de Brasília – UNB. Brasília, p. 47. 2020.

A adoção do regime de responsabilidade civil objetivo parece ser o meio mais adequado para se garantir a proteção dos direitos dos titulares de dados pessoais. Porém, a crescente expansão dos danos trouxe para a responsabilidade civil não só o dilema de como repará-lo, mas levantou a questão se de fato a reparação seria a solução, como será observado mais a fundo no próximo capítulo.

### 3.3 Responsabilização se o dano causado ao titular de dados for comprovado

Analisando a responsabilidade subjetiva, que consiste no dever jurídico de reparar o dano, decorre da violação de um dever jurídico antecedente, qual seja o *neminem laedere*. Afinal de contas, a ideia de não prejudicar a outrem é a base do conceito de responsabilidade civil da maneira adotada pelo ordenamento pátrio.

O princípio *neminem laedere*<sup>160</sup>, nos dá exatamente esta idéia de responsabilidade civil, todavia, é necessária a existência de dano para que exista o dever de reparação pelo agente causador, como disposto no art. 927 do Código Civil<sup>161</sup>.

A teoria subjetiva preconiza que o elemento culpa constitui, em regra, um dos pressupostos necessários para a responsabilidade civil. No Código Civil, constatou-se essa teoria a partir da leitura do artigo 186, que diz: “Art. 186. Aquele que, ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente”. (aqui seria viável ter uma nota de rodapé para a citação do CV?)

Anteriormente, a responsabilidade civil subjetiva foi suficiente para a resolução de todos os casos. Contudo, com o passar do tempo, tanto a doutrina quanto a jurisprudência passaram a entender que este modelo de responsabilidade, baseado na culpa, não era suficiente para solucionar todos os casos existentes.

Na responsabilidade civil subjetiva, o agente causador do dano somente será responsabilizado se a vítima provar que este agiu com culpa em sentido amplo, abrangendo o dolo e a culpa *strictu sensu*. Caso não logre êxito em provar a existência de culpa, o agente não será responsabilizado e a vítima deverá suportar o dano.

Por isso, a responsabilidade civil subjetiva tem por fundamento central a análise do juízo de reprobabilidade da conduta do infrator, ensejadora do prejuízo. Presentes os elementos

<sup>160</sup> VIVIAN, Wilson de Alcântara Buachi. *Princípio alterum non laedere (neminem laedere), dignidade humana e boa-fé*. 2016. Disponível em: <<https://ambitojuridico.com.br/cadernos/direito-civil/principio-alterum-non-laedere-neminem-laedere-dignidade-humana-e-boa-fe/>>. Acesso em: 03 jun. 2021.

<sup>161</sup> BRASIL, op. cit., nota 2.

conduta, dano e nexo de causalidade entre este e aquela, mister se provar a existência do elemento culpa.

Vale citar que este declínio da responsabilidade civil subjetiva se deu principalmente em função da evolução da sociedade industrial e o conseqüente aumento dos riscos de acidentes de trabalho. Pois, nem sempre é possível a demonstração da culpa exigida pela teoria subjetiva, conforme destaca Cavalieri Filho:

Por essa concepção clássica, todavia, a vítima só obterá a reparação do dano se provar a culpa do agente, o que nem sempre é possível na sociedade moderna. O desenvolvimento industrial, proporcionado pelo advento do maquinismo e outros inventos tecnológicos, bem como o crescimento populacional geraram novas situações que não podiam ser amparadas pelo conceito tradicional de culpa.<sup>162</sup>

Para sanar a dificuldade na comprovação da culpa e diante da resistência dos autores subjetivistas em aceitar a responsabilidade objetiva, a culpa presumida foi o mecanismo encontrado para a proteção da vítima. Conceito esse que pode ser compreendido pela análise de autores como Arnaldo Wald, Brunno Pandori Giancoli e Cavalieri:

O fundamento da responsabilidade, entretanto, continuou o mesmo – a culpa; a diferença reside num aspecto meramente processual de distribuição do ônus da prova. Enquanto no sistema clássico (de culpa provada) cabe à vítima provar a culpa do causador do dano, no de inversão do ônus probatório atribuí-se ao demandado o ônus de provar que não agiu com culpa (presunção *juris tantum*).<sup>163</sup>

Porém, a culpa presumida não era suficiente para a solução de tal dificuldade da vítima de, em determinados casos, provar a existência de culpa por parte do agente causador do dano. Assim, foram desenvolvidos vários trabalhos para solucionar essa questão, o que levou a concepção da responsabilidade civil objetiva, que é aquela que prescinde do elemento culpa. Esse elemento poderá até existir no caso concreto, entretanto será totalmente irrelevante para a responsabilização do agente causador do dano, não necessitando ser comprovada para a configuração do dever de indenizar.<sup>164</sup>

A Lei Geral de Proteção de Dados cumpre o papel inovador do critério binário de imputação consistente na culpa ou no risco, ao prever que, no contexto do tratamento de dados pessoais, há deveres antes não enunciados explicitamente, mas agora tratados de forma

<sup>162</sup> CAVALIERI FILHO, Sérgio. *Programa de responsabilidade civil*. 7. ed. São Paulo: Atlas, 2007, p. 16.

<sup>163</sup> AMORIM, Filipo Bruno Silva. *O sistema da responsabilidade no Código Civil de 2002: prevalência da responsabilidade subjetiva ou objetiva?*. Disponível em: <<https://jus.com.br/artigos/22841/o-sistema-da-responsabilidade-no-codigo-civil-de-2002-prevalencia-da-responsabilidade-subjetiva-ou-objetiva>>. Acesso em: 03 jun. 2022.

<sup>164</sup> MENDONÇA, Rafael Dantas Carvalho de. *A responsabilidade Civil no direito brasileiro*. Disponível em: <<https://conteudojuridico.com.br/consulta/Artigos/51542/a-responsabilidade-civil-no-direito-brasileiro>>. Acesso em: 04 jun. 2022.

categórica pela Lei, impondo aos agentes de tratamento, os deveres de prevenção de incidentes, vigilância e segurança nas operações de tratamento de dados pessoais.

Por isso, para compreender os deveres impostos aos indivíduos que ostentam a especial condição de agentes de tratamento, é mister a compreensão do sistema de responsabilidade civil na Lei Protetiva, sob os pressupostos da responsabilidade subjetiva.

Destaca-se que em todas as situações jurídicas nas quais o legislador incluiu a regra da responsabilidade subjetiva no direito privado, foi feito de modo expresso e inequívoco, como empregando a expressão “independentemente da existência de culpa”, expressão encontrada, por exemplo, nos artigos 12 e 14 do Código de Defesa do Consumidor ou singelamente se referindo à obrigação de reparar o dano “independentemente de culpa”, como na cláusula geral do artigo 927, parágrafo único do Código Civil.<sup>165</sup>

Por sua vez, a LGPD não apresenta qualquer artigo que se valha da expressão “independentemente de culpa” ou “independentemente da existência de culpa”, a indicar de modo inequívoco que o regime jurídico adotado fora o da responsabilidade objetiva, sendo esse um dos principais motivos para sustentar a existência de responsabilidade subjetiva na lei.

Outro forte argumento a indicar a escolha da regra da responsabilidade subjetiva consiste no fato de que a Lei é pródiga na imposição de uma série de deveres de ação e de abstenção aos agentes de tratamento, como pode ser observado desde os princípios de Proteção de Dados até as medidas de segurança, técnicas e administrativas, previstas na Lei. Essas estão aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito desde a concepção do produto ou serviço (*privacy by design*); passando pela adoção das melhores práticas de segurança da informação; pelo dever de comunicação de incidente à Autoridade Nacional e ao titular dos dados, e, finalmente, pela publicação das regras e boas práticas de governança.

Observa-se que tais regras não consistem em meras recomendações que visam evitar incidentes de segurança. O legislador vai além disso, estabelece um *standard* de conduta e cobra que essas regras sejam cumpridas, por isso, a prescrição exaustiva e detalhada dos deveres seriam determinantes na hora da responsabilização de um agente de tratamento diante de um caso de violação. Ao contrário do que aconteceria se o regime de responsabilidade civil adotado pela LGPD fosse de caráter exclusivamente objetivo, pois resultaria em redundância na conclusão de que o cumprimento dos deveres se tornaria inócuo se, qualquer que fosse o

---

<sup>165</sup> TASSO, op. cit., p. 107.

incidente, a responsabilidade pela reparação estivesse configurada, tratando-se de um contrassenso.<sup>166</sup>

O próprio art. 42 da Lei dispõe que a reparação do dano será “em razão do exercício de atividade de tratamento de dados pessoais” causado “em violação à legislação de proteção de dados pessoais”. Na mesma intenção dispõe o art. 43 ao excluir a responsabilização em certos casos. A mesma lógica da responsabilidade civil encontra-se presente no artigo 44 ao prever que o tratamento de dados será irregular somente quando deixar de observar a legislação ou quando não fornecer a segurança esperada pelo titular.

Ora, passando pelo conceito de responsabilidade civil proativa, proposto por Maria Cecília Bodin de Moraes<sup>167</sup>, e apresentado anteriormente, constata-se que os artigos apresentados são contrários a responsabilidade objetiva. Por isso, prevalece o entendimento, sustentado por doutrinadores como Gisela Sampaio e Rose Melo<sup>168</sup>, de que o sistema de responsabilidade civil na Lei Geral de Proteção de Dados intrinsecamente está vinculado ao elemento culpa, ou seja, trata-se de uma responsabilidade subjetiva.

Essas autoras argumentam que toda a estrutura da lei é pautada na criação de deveres e cuidado, dirigidos aos agentes de tratamento de dados, sob pena de responsabilização. Caso o intuito do legislador fosse responsabilizar os agentes, independente de culpa ou não, não teria motivo para criar esses deveres a serem seguidos. Diante disso, constata-se que a investigação a respeito do descumprimento de deveres e *standards* de conduta se aproxima de um modelo de responsabilização baseado na culpa.

Outros autores <sup>169</sup>que também compartilham dessa corrente são Gisela Sampaio Guedes, Aline Terra e Gustavo Tepedino, que dizem:

[...] as críticas à noção clássica conduziram à elaboração de conceito objetivado de culpa, designado culpa normativa, que se revela na ideia de desvio de conduta, e cuja apreciação desconsidera a análise do perfil subjetivo do agente que se pretende responsabilizar, mas leva em conta o comportamento exigível diante das especiais circunstâncias do caso concreto. Não se investiga o direcionamento da vontade do agente para o descumprimento da ordem jurídica in abstracto, e sim, ao revés, a adequação (ou não) de sua conduta ao padrão de comportamento esperado in concreto. Esse standard de comportamento desejado para o caso concreto serve a normatizar objetivamente a investigação da culpa, dando-lhe contornos consentâneos com a especificidade fática e circunstancial da hipótese em exame.

<sup>166</sup> TASSO, op. cit., p. 108.

<sup>167</sup> MORAES, op. cit.

<sup>168</sup> GUEDES: MEIRELES, op. cit., p. 231.

<sup>169</sup> GUEDES, Gisela Sampaio da Cruz; TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde. Fundamentos do Direito Civil. V.4. Rio de Janeiro: Forense, 2020, p. 4.



Segundo esses autores<sup>170</sup>, o conceito de culpa ganha uma nova roupagem, mais objetivada, trata-se do conceito de culpa normativa, que se revela quando o comportamento do agente destoia do padrão de comportamento esperado na situação concreta. Nesse caso, para aferição da conduta culposa, basta comparar a conduta do ofensor com o padrão de comportamento (*standards*) que dele era esperado. Essa conduta têm relevância na Lei Geral de Proteção de Dados, que estipula aos agentes de tratamento regras de comportamento que devem ser seguidas durante suas atividades.

Fernando Antônio Tasso<sup>171</sup> também defende o regime da responsabilidade civil subjetiva, afirmando que, pelo fato da Lei exigir dos agentes de tratamento de dados de um padrão de conduta, também confere aos agentes a possibilidade de autoregulação, ou seja, estabelece regras para a atividade que desempenham.

Além desses fatores, Gisela Sampaio e Rose Melo<sup>172</sup> ressaltam outros pontos que demonstram a adoção do regime subjetivo de responsabilidade pela LGPD, como o histórico de tramitação do projeto de lei que originou a LGPD, que se demonstra uma preferência pelo regime subjetivo ao se excluir a menção expressa à responsabilidade civil.

Ademais, o inciso II, do art. 43, remete à ideia de culpa como fundamento da responsabilidade civil, ao contrário dos incisos I e III, que afastam o nexo de causalidade e reconhecem a culpa exclusiva do titular de dados, respectivamente. No mesmo intuito, há a regra do inciso II que exclui a responsabilidade do agente de tratamento ainda que haja nexo de causalidade entre a conduta e o dano.

Porém, no caso de incidentes envolvendo dados sensíveis, Gisela Sampaio e Rose Melo admitem a aplicação da responsabilidade civil objetiva, tendo por base a atividade dos agentes, e com fundamento na cláusula geral de responsabilidade civil objetiva do Código Civil, artigo 927.

Diogo Ramos Ferreira<sup>173</sup>, é outro pesquisador da área que defende a responsabilidade subjetiva da LGPD, contudo, admitindo-se a aplicação da responsabilidade objetiva quando a atividade de tratamento, em razão de sua natureza ou elementos, apresentar graves riscos aos titulares, em razão da teoria do risco criado.

---

<sup>170</sup> Ibid.

<sup>171</sup> TASSO, op. cit.

<sup>172</sup> GUEDES, Gisela Sampaio da Cruz; VENCELAU MEIRELES, Rose Melo. Término do Tratamento de Dados. In: TEPEDINO, Gustavo et al. *Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 219-241.

<sup>173</sup> FERREIRA, Diogo Ramos. *Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva?* 2019. Disponível em: < <https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019>>. Acesso em: 3 jun. 2022.

Portanto, o argumento de maior relevo para a adoção do regime subjetivo é o fato da lei estabelecer deveres aos agentes de tratamento. Mas o simples estabelecimento de deveres não é elemento apto a definir o regime de responsabilização previsto na LGPD como subjetivo. Pois, a teoria subjetiva é calcada na ideia moderna de culpa normativa, deste modo, não é a única a estabelecer um padrão de comportamento a ser seguido.

Como no caso de responsabilização civil por dano ambiental, aplica-se a teoria do risco integral, segundo a qual o causador do dano responde objetivamente ainda que tenha cumprido todos os deveres impostos para o desempenho normal de sua atividade. Nesses casos, ocorrendo o dano, o causador não poderá alegar que o fato de ter cumprido com as exigências legais e regulamentares o isentará de responsabilidade.

Sendo assim, ocorrendo o dano, a demonstração de observância de tais deveres não pode ensejar a exoneração da responsabilidade do causador, pois os princípios de segurança, prevenção e mitigação do risco foram instituídos como contraposto ao risco intrínseco da atividade de tratamento de dados. Por isso, não trata de um efeito liberatório de responsabilização civil, porém, funciona como elementos balizadores da atividade, de observância obrigatória, podendo atenuar, quando efetivamente observados pelo agente de tratamento causador do dano, eventual multa administrativa que possa ser aplicada por parte da Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

### **3.4 Casos de vazamento de dados e a atuação dos Tribunais Brasileiros frente à Responsabilidade Civil na Lei Geral de Proteção de Dados**

Uma realidade cada vez mais frequente hoje em dia é o risco de lesão a direitos no tráfego de dados pessoais, como pôde ser visto nas corriqueiras notícias de vazamento de informações pessoais, inclusive dados sensíveis. Diante desse cenário, a sociedade tem se preocupado cada vez mais com a questão, sobretudo com a ampliação do uso de algoritmos e outras ferramentas de inteligência artificial para coleta e tratamento de dados obtidos no ciberespaço.

Por esta razão, partindo da premissa de que a legislação existente não seria suficiente para resolver os desafios emergentes deste novo cenário, a LGPD (Lei nº 13.709/18) instituiu um regime de responsabilidade civil próprio para situações envolvendo lesões ocorridas no tratamento de dados pessoais, como apresentado anteriormente. Evidentemente, que esse busca ser apto para propiciar a efetiva tutela da vítima e a reparação integral do dano, porém, como visto, é preciso analisar a coerência interna do sistema de responsabilidade civil no direito

brasileiro.

Destaca-se inicialmente, que a tendência legislativa consolidada desde o final do Século XX, trás como inconveniente uma erosão de sistematicidade e unidade do sistema jurídico de direito privado, como exposto por Gustavo Tepedino e Rodrigo da Guia Silva<sup>174</sup>:

Tais linhas teóricas compartilham o esforço de definição das soluções mais adequadas aos novos problemas. Identificam-se, nesse sentido, variadas formulações que enunciam princípios éticos próprios para a regulação dos robôs e demais sistemas autônomos. As célebres Leis de Asimov servem como boa representação do quanto exposto: o temor (ou encanto) das novidades tecnológicas parece instigar a formulação de novas regras e novas soluções. Empreende-se, assim, grande esforço para a concepção de respostas que se possam reputar adequadas aos novos desafios suscitados pela inteligência artificial.

Como pode ser visto, a análise da disciplina da LGPD não pode dispensar toda a evolução do sistema de responsabilidade civil legado pelo direito privado, principalmente das normas do Código Civil e do CDC. Esses, por conta da sua grande carga principiológica, valorativa e posição topológica no ordenamento, viabilizam a contínua construção e reconstrução da interpretação dos institutos de direito privado, funcionalizando-os para atender às necessidades empíricas de uma sociedade em constante mutação e de alta complexidade, assegurando o prestígio ao caráter ético que deve permear a conduta humana e as relações sociais, como visto nos capítulos anteriores<sup>175</sup>.

Exatamente por isso, no intuito de melhor analisar a construção da responsabilização dos envolvidos em caso de vazamento de dados, buscar-se-á analisar as decisões dos Tribunais brasileiros sobre o tema que vêm sendo tomadas nos últimos anos, bem como alguns casos recentes de vazamento de dados que estão sendo apurados.

Em 2017, ocorreu o vazamento de dados da Netshoes, empresa de venda digital de artigos esportivos. Duas listas de dados pessoais de quase 2 milhões de consumidores da empresa foram vazadas, expondo o nome, data de nascimento, endereço, CPF e informações de pedidos de 1.999.704 contas de clientes.

Além disso, o incidente vazou informações de servidores públicos que estavam cadastrados no banco de informações da empresa. Entre os emails de órgãos públicos cadastrados havia contas, do Tribunal de Contas da União (TCU), da Câmara dos Deputados, do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT), da Polícia Federal, do Superior

<sup>174</sup> TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Desafios da inteligência artificial em matéria de responsabilidade civil. *Revista Brasileira de Direito Civil – RBDCivil*, v. 21, Belo Horizonte, jul./set. 2019, p. 79.

<sup>175</sup> NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. *Responsabilidade Civil na LGPD: Problemas e soluções*. Disponível em: < <https://indexlaw.org/index.php/conpedireview/article/view/7024>>. Acesso em: 04 jun. 2022.

Tribunal de Justiça (STJ), do Supremo Tribunal Federal (STF), do Ministério da Justiça e da Advocacia-Geral da União e Presidência da República.

Diante do caso, a Comissão de Proteção dos Dados Pessoais do MPDFT instaurou, em janeiro de 2018, um inquérito civil público e realizou recomendações para a empresa entrar em contato com todos os clientes que tiveram informações vazadas.

Após análise do caso, a Netshoes, firmou um Termo de Ajustamento de Conduta (TAC) com o Ministério Público do Distrito Federal e Territórios (MPDFT), em janeiro de 2019. A empresa ré aceitou pagar R\$ 500 mil a título de indenização por danos morais coletivos de caráter nacional, devido ao vazamento da base de dados interna, em troca da não propositura de uma ação coletiva pelo Parquet e da suspensão do Inquérito Civil Público até a quitação integral da transação. O valor da indenização será revertido ao Fundo de Defesa de Direitos Difusos.

Segundo o TAC, a Netshoes cumpriu com as recomendações do MPDFT, entre elas a empresa entrou em contato com os clientes por email, emitiu notas à imprensa, bem como também comunicou-se por telefonemas e publicações em seu próprio portal. A empresa também terá que promover campanhas de conscientização para a proteção de dados no ambiente eletrônico.

O TAC, assinado pelo promotor de Justiça Frederico Ceroy e pelo CEO da empresa, Marcio Kumruian, também estabeleceu que a Netshoes teria que implantar medidas de segurança como o gerenciamento de riscos e vulnerabilidades no portal Netshoes, ações de adequação à Lei Geral de Proteção dos Dados Pessoais (LGPD), atualização da política de segurança cibernética, orientação de consumidores sobre medidas de proteção de dados pessoais e a participação em fóruns e eventos sobre o tema<sup>176</sup>.

Segundo o MPDFT, o descumprimento das obrigações implicará em uma ação cível de reparação pelos danos morais coletivos no valor de R\$10 milhões (dez milhões de reais). E caso a Netshoes não siga as obrigações, será ajuizada uma ação cível de reparação pelos danos patrimoniais no valor de R\$85 milhões (oitenta e cinco milhões de reais), esse valor representa R\$5,00 (cinco reais) por cada titular que teve os dados pessoais comprometidos<sup>177</sup>.

O termo de negociação de ajustamento tem como base jurídica a LGPD, aprovada em agosto de 2018, e o Marco Civil da Internet. Passando a análise do respectivo de Termo de

---

<sup>176</sup> DANTAS, Thaile. *Netshoes terá de pagar R\$500 mil por vazamento de dados de milhões de clientes*. Disponível em: < <https://thaile.jusbrasil.com.br/noticias/685006882/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-milhoes-de-clientes>>. Acesso em: 07 jun. 2022.

<sup>177</sup> Ibid.

Conduta, deve-se começar pelo dano moral coletivo nos casos de proteção de dados, inicialmente, prevaleceu na jurisprudência brasileira<sup>178</sup>, que o dano moral não poderia ser titularizado por uma coletividade, pois atinge a intimidade, a honra e a imagem de uma pessoa, individualmente considerada. O Superior Tribunal de Justiça<sup>179</sup> mudou esse entendimento e reconheceu o dano moral coletivo, considerando uma espécie autônoma de dano que está relacionada à integridade psico-física da coletividade, e a um bem de natureza estritamente transindividual.

Do caso Netshoes pode ser indagado como conciliar a lógica privatista das negociações com a atuação da Administração na tutela de direitos de expressão coletiva, tradicionalmente considerados indisponíveis. Como visto no início do capítulo, a Lei Geral de Proteção de Dados coloca em análise a possibilidade de existirem transações sobre incidentes de segurança coletivos. Expressamente a Lei não dispõe sobre a celebração de conciliação em casos de reparação de danos coletivos. Contudo, no caso Netshoes foi realizado o acordo antes da vigência da Lei, não sendo esse abarcado por ela.

Doutrinadores como Fredie Didier Jr. e Hermes Zanetti Jr<sup>180</sup>. alertam para a necessidade de um controle judicial das negociações coletivas, sobretudo quando essas fujam do mero ajustamento de condutas e passem a tratar efetivamente sobre o direito lesado, por isso é passível do Juiz realizar um exame de mérito do acordo, quando da oportunidade de homologação judicial da autocomposição. No caso do TAC em questão, está sim prevista a submissão do acordo à homologação judicial, na Cláusula 5ª. Isso também viabiliza o contraditório e a ampla defesa, por isso é importante a adequada representação dos interesses das partes envolvidas, cabendo ao magistrado identificar qualquer falha na representação dos interesses individuais<sup>181</sup>.

Além de amparar a tutela reparatória, o acordo já inclui também o cumprimento do art. 48 da LGPD, ou seja, o controlador dos dados deve comunicar aos titulares atingidos a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante, devendo essa

---

<sup>178</sup> BRASIL. Superior Tribunal de Justiça. *REsp nº 971844 RS 2007/0177337-9*. Relator: Ministro Teori Albino Zavascki. Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/8591223/recurso-especial-resp-971844-rs-2007-0177337-9/inteiro-teor-13674826>>. Acesso em: 03 jun. 2022.

<sup>179</sup> BRASIL. Superior Tribunal de Justiça. *REsp nº 1.473.846/SP 2014/0184129-1*. Relator: Ministro Ricardo Villas Bôas Cueva. Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/443282925/recurso-especial-resp-1473846-sp-2014-0184129-1/inteiro-teor-443282935>>. Acesso em: 03 jun. 2022.

<sup>180</sup> DIDIER JR., Fredie; ZANETTI JR., Hermes. Justiça multiportas e tutela constitucional adequada: autocomposição em direitos coletivos. In: \_\_\_\_\_; \_\_\_\_\_; CABRAL, Trícia Navarro Xavier. *Justiça multiportas: mediação, conciliação, arbitragem e outros meios de solução adequada para conflitos*. V. 9. Salvador: JusPodivm, 2017, p. 54.

<sup>181</sup> FACHINELLO, João Antônio Tschá. Acordos e tutela coletiva: algumas reflexões a partir do TAC no caso do vazamento de dados da Netshoes. *Revista Iberoamericana de Derecho Procesal*, v. 10, p. 85-112, jul./ dez. 2019.

comunicação ser feita em prazo razoável.

De acordo com João Antonio Tschá Fachinello<sup>182</sup>, constata-se a impossibilidade de divisão dos direitos coletivos, uma vez que não se trata de mera somatória dos direitos individuais envolvidos. Existindo uma constante busca para ajuste do processo tradicional às necessidades e peculiaridades da litigância de interesse público, de modo a romper com as regras do processo individual. Sendo assim, caso reconhecido o dano, a busca por soluções alternativas à via jurisdicional pode ser uma alternativa para os problemas que surgirem, garantindo a tutela dos consumidores individualmente considerados, sem comprometer a continuidade da atividade empresarial.

Outro caso anterior a vigência da LGPD foi o do Facebook. Em meados de 2018, foi noticiado que usuários do Facebook teriam sofrido com o uso indevido de dados pela empresa Cambridge Analytica<sup>183</sup>. Essa empresa de consultoria política envolvida na campanha presidencial de Donald Trump nas eleições norte-americanas obteve acesso a dados pessoais sobre milhões de usuários do Facebook.

Diante dessa informação, o MP do Distrito Federal e Territórios (MPDFT) determinou a instauração de Inquérito Civil Público (ICP)<sup>184</sup>, nos termos da Portaria nº 02/2018158<sup>185</sup>. De acordo com a referida portaria, consta que compete à Comissão Nacional de Proteção de Dados Pessoais (CNPDP) do MPDFT receber comunicações sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo aos titulares dos dados pessoais (*data breach notification*), bem como sugerir ao responsável pelo tratamento dos dados, diante da gravidade do incidente de segurança, a adoção de outras providências, tais como: pronta comunicação aos titulares; ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

Além disso, foi aberto um processo perante à Secretaria Nacional do Consumidor (SENACON) para investigação sobre os fatos em território brasileiro, uma vez que foram divulgadas diversas notícias veiculadas pela mídia sobre informação de que usuários do

---

<sup>182</sup> Ibid.

<sup>183</sup> FOLHA DE SÃO PAULO. *Como a Cambridge Analytica recolheu dados do Facebook*: Entenda a estratégia usada por aliados de Trump durante a campanha eleitoral, 21 mar. 2018. Disponível em: <<https://www1.folha.uol.com.br/mercado/2018/03/como-a-cambridge-analytica-recolheu-dados-dofacebook.shtml>> Acesso em: 20 mai. 2022.

<sup>184</sup> CONJUR. *MP-DF investiga se Facebook repassou dados de brasileiros para publicidade*. Disponível em: <<https://www.conjur.com.br/2018-mar-22/mp-df-investiga-facebook-repassou-dados-brasileiros>> Acesso em: 20 mai. 2022.

<sup>185</sup> BRASIL. Ministério Público do Distrito Federal e Territórios. *Comissão de Proteção dos Dados Pessoais*. 1ª Promotoria de Justiça de Defesa do Consumidor. Portaria n. 2 / 2018 - Inquérito Civil Público - ICP - Cambridge Analytica / Facebook. Disponível em: <https://www.conjur.com.br/dl/mp-dftinvestiga-cambridge-analytica.pdf> Acesso em: 20 abr. 2021.

Facebook, no país, podem ter sofrido com o uso indevido de dados pela Cambridge Analytica. Com isso, foi instaurado o processo nº 08012.000723/2018-19, tendo figurado como representante o DPDC e, como representados, Facebook Inc. e Facebook Serviços Online do Brasil Ltda.

Após o referido processo administrativo da SENACON, foi proferida a Nota Técnica n.º 32/2019/CGCTSA/DPDC/SENACON/MJ<sup>186</sup>, que determinou a aplicação de multa aos representados, no valor de R\$ 6.600.000,00 (seis milhões e seiscentos mil reais), uma vez que teriam incorrido em prática abusiva por terem exposto indevidamente dados de usuários ao aplicativo *thisisyourdigitallife*, e que, por terem adotado modelo de negócio com padrão de configuração de compartilhamento automático de dados pessoais de usuários com aplicativos, deveriam ter adotado maiores cuidados na gestão desses dados.

Em 2021, já durante a vigência da LGPD, a Eletrobras e a Copel foram alvo de ataques de *ransomware*, os golpes não chegaram a interferir no fornecimento de energia nas localidades atendidas, mas obrigaram as companhias a retirarem sistemas do ar ou interromperem atendimentos a clientes por conta das intrusões. O ataque aconteceu na rede da Eletronuclear, subsidiária responsável pelo controle das usinas Angra 1 e 2, no estado do Rio de Janeiro<sup>187</sup>.

Apesar do ataque, não foram detectadas falhas ou interrupções no fornecimento de energia ou no funcionamento das usinas nucleares. Por outro lado, a Eletrobras informou ter interrompido o funcionamento dos sistemas administrativos para conter e erradicar os efeitos do ataque, de modo que a integridade dos dados disponíveis fosse mantida. Agora, a companhia trabalha para verificar os reflexos do ataque ao lado de órgãos do governo federal e da Presidência da República<sup>188</sup>.

Ouro caso recente foi o do integrador de marketplaces *HariExpress*<sup>189</sup>, que atua em diversas plataformas de grandes varejistas, teve 1,75 bilhão de dados (610 GB) expostos, segundo um relatório do *SafetyDetectives*, um grupo de pesquisadores que investigam vazamentos na internet. A empresa presta serviços para vendedores que anunciam produtos em plataformas como Magazine Luiza, Mercado Livre, Shopee, Amazon, as do grupo Americanas

<sup>186</sup> BRASIL. Ministério da Justiça e Segurança Pública. *Nota Técnica n.º 32/2019/CGCTSA/DPDC/SENACON/MJ*. Prática abusiva. Violação aos princípios da boa-fé, ao direito à privacidade e à informação clara e adequada sobre bens e serviços. Disponível em: <[https://brunobioni.com.br/wp-content/uploads/2020/01/SEI\\_08012.000723\\_2018\\_19-1-1.pdf](https://brunobioni.com.br/wp-content/uploads/2020/01/SEI_08012.000723_2018_19-1-1.pdf)> . Acesso em: 29 mai. 2022.

<sup>187</sup> DEMARTINI, Felipe. *Eletrobras e Copel são vítimas de ataques de ransomware*. Site Canal Tech. Disponível em: <<https://canaltech.com.br/seguranca/eletrobras-e-copel-sao-vitimas-de-ataques-de-ransomware-178557/>>. Acesso em 30 mai. 2022.

<sup>188</sup> Ibid.

<sup>189</sup> BRANDÃO, Raquel. *Plataforma vaza 1,75 bilhão de dados de clientes de marketplaces e Correios*. Disponível em: < <https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2021/10/13/plataforma-vaza-175-bilhao-de-dados-de-clientes-de-marketplaces-e-correios.ghtml>>. Acesso em: 31 mai. 2022.

e os Correios.

De acordo com o relatório da empresa, o vazamento deixou expostos dados de pedidos de clientes que compraram on-line, como nome, endereço de e-mail, endereço de entrega da encomenda e telefone. Também foram expostos dados dos vendedores, porém, não se pode afirmar que os dados tenham sido capturados por hackers.

Os Correios manifestaram que não há indícios de violação de informações – de pessoas físicas ou jurídicas – oriundas da base de dados da estatal e seguirá apurando o caso para tomar as medidas necessárias.

Analisando o tema, na segunda metade da década de 2010, observa-se que houve uma inversão da jurisprudência brasileira em relação ao tema, para permitir a concessão de indenização por danos morais *in re ipsa* nessa matéria. A mudança de paradigma se deve a conscientização sobre o problema, não eram mais vistos só como uma questão relacionada ao direito do consumidor, decorrente da regra do art. 43 do Código de Defesa do Consumidor sobre bancos de dados, mas uma questão relacionada aos direitos da personalidade, que exigiria uma nova abordagem por um ramo novo, que consiste no direito à proteção de dados pessoais<sup>190</sup>.

Além da promulgação do Marco Civil da Internet, em 2014 e, em 2018, entrou em vigor o GDPR, bastante divulgado no Brasil, bem como a própria LGPD, fazendo com que se tornassem mais evidentes as percepções sobre os danos causados às pessoas em termos de tratamento automatizado de dados pessoais.

Acerca dessa mudança de entendimento jurisprudencial, merece destaque que o mesmo Superior Tribunal de Justiça, no REsp. nº 1758799/MG<sup>191</sup>, já mencionado anteriormente, julgou ação proposta por uma pessoa contra empresa que presta serviços de análise e concessão de crédito, pela qual se pediu a condenação por abertura de cadastro sobre a pessoa sem que fosse notificado.

O caso foi concluído com o entendimento de que o consumidor fornece dados na medida necessária à contratação, não com a finalidade de repasse a terceiros com fins lucrativos, razão pela qual se considerou ter ocorrido dano moral *in re ipsa*. Porém, faz-se distinção em relação ao REsp. nº 1.419.697/RS, no qual se fixou entendimento da desnecessidade de consentimento do consumidor sobre a abertura do cadastro por não se fazer restrição ao crédito,

---

<sup>190</sup> VIGLIANISI FERRARO, Angelo; TOMASEVICIUS FILHO, Eduardo. Indenização pelo tratamento ilegítimo de dados pessoais: comparação entre os direitos italiano e brasileiro. Revista dos Tribunais [Recurso Eletrônico]. São Paulo, n.1031, set. 2021. Disponível em: <https://dspace.almg.gov.br/handle/11037/41773>. Acesso em: 26 mai. 2022.

<sup>191</sup> BRASIL. Superior Tribunal de Justiça. (3ª Turma). REsp. nº 1758799/MG. Relatora: Min. Nancy Andrighi. Brasília, 12.11.2019. Publicado no DJe em 19.11.2019.



mas apenas a análise do crédito<sup>192</sup>.

Outro caso de mesmo sentido foi o do Tribunal Superior do Trabalho<sup>193</sup>, em que uma companhia produtora de café deixou vaziar documento em rede social com informações de salário e funcionais de trabalhadores, incluindo o rol de quem seria dispensado pelo empregador. No caso, mesmo alegando que o documento era sigiloso, a empresa foi condenada ao pagamento de indenização por danos morais.

O dano moral em decorrência de caso de vazamento de dados segue sendo pleiteado pelo Ministério Público. Como no caso da ação civil pública, proposta pelo Parquet, por vazamento de dados pessoais e transações de clientes de um banco brasileiro 100% digital, pleiteou-se indenização equivalente a R\$ 10 milhões. Porém, fez-se acordo para encerramento da questão, mediante pagamento de indenização de R\$ 1,5 milhão<sup>194</sup>.

Partindo da análise do Painel LGPD nos Tribunais<sup>195</sup>, realizado pelo Centro de Direito, Internet e Sociedade (CEDIS-IDP) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) e o Jusbrasil, que trata-se de uma seleção das mais importantes decisões judiciais que envolvem a Lei Geral de Proteção de Dados no seu primeiro ano de vigência, destaca-se quais principais decisões envolvendo a nova Lei.

De acordo com esse Painel, foram encontradas 584 (quinhentas e oitenta e quatro) decisões, publicadas entre setembro de 2020 e agosto de 2021. Em seguida, essas decisões foram analisadas qualitativamente pelos pesquisadores do IDP *PrivacyLab* e, desse montante, os pesquisadores encontraram 274 decisões que efetivamente aplicam a LGPD, nos seus mais diversos aspectos. Os Tribunais de onde saíram mais decisões envolvendo a nova Lei nesse primeiro ano de vigência pode ser visto no gráfico do anexo 1.

Constata-se que a nova Lei está também muito pleiteada na Justiça do Trabalho, reafirmando o quanto o tema é amplo e vai muito além da esfera consumerista, como chegou a ser dito anteriormente. Em todas as áreas é preciso adequar-se sobre a nova Lei e seus reflexos.

Conforme analisado, antes da entrada em vigor da Lei, já eram investigados e apurados os casos de vazamento de dados no país. E após a LGPD, o tema segue em voga, inclusive o pleito da indenização pelo dano moral sofrido nos casos de vazamento, mantendo-se recorrente

<sup>192</sup> VIGLIANISI FERRARO; TOMASEVICIUS FILHO, op. cit.

<sup>193</sup> BRASIL. Tribunal Superior do Trabalho (6ª Turma). *RR nº 118-55.2013.5.09.01273*. Relatora: Min. Katia Magalhães Arruda. Brasília, 06.12.2017.

<sup>194</sup> BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios (15ª Vara Cível da Circunscrição Especial Judiciária de Brasília). *Ação Civil Pública 0721831-64.2018.8.07.0001*. Disponível em: <https://www.jusbrasil.com.br/processos/203231447/processo-n-072XXXX-6420188070001-do-tjdf>. Acesso em: 20 mai. 2022.

<sup>195</sup> JUSBRASIL. *Painel LGPD nos tribunais*. Disponível em: < <https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html>>. Acesso em: 03 jun. 2022.

e cada vez mais debatido.

### **3.5 A Responsabilidade Civil na prática de acordo com as Lei de Dados Pessoais Internacionais**

Primeiramente, inicia-se a análise pelo regulamento Europeu sobre Proteção de Dados, que entrou em vigor em 2018 e, partindo deste, passa-se a análise da eficácia da LGPD no Brasil, que entrou em vigor no ano de 2020. A Europa promulgou o seu Regulamento Geral de Proteção de Dados – GDPR<sup>196</sup>, em 2016, e depois disso surgiu a necessidade de reforma ou criação da legislação sobre proteção de dados em diversos países do mundo inteiro.

A GDPR criou um regime de sanções particularmente complexo e multifacetado, tanto do ponto de vista do direito público, quanto no aspecto do direito privado. Já do ponto de vista do direito administrativo, o art. 83 da GDPR<sup>197</sup> identifica dois tipos de sanções que devem ser aplicadas pela autoridade nacional de controle, em conformidade com uma série de circunstâncias nos casos concretos, tanto de natureza econômica, podendo chegar a 20 milhões de Euros, ou até 4% do faturamento anual mundial do ano anterior, assim como medidas corretivas, mediante adequação dos tratamentos às disposições atuais ou em comunicar ao interessado a violação de dados pessoais, bem como a imposição de uma limitação temporária ou definitiva ao processamento, incluindo a proibição de processamento, retificação ou cancelamento de dados pessoais e suspensão dos fluxos de dados para um destinatário em um país terceiro ou organização internacional.

No tocante à responsabilidade civil, destaca-se o artigo 82<sup>198</sup> da GDPR, composto por seis parágrafos. No primeiro parágrafo, estabeleceu-se que qualquer pessoa que sofra danos patrimoniais e extrapatrimoniais causados por uma violação deste regulamento, tem o direito de obter uma compensação pelos danos causados pelo agente encarregado do tratamento. No parágrafo 3º do mesmo artigo, tanto nos danos patrimoniais quanto nos extrapatrimoniais causados aos lesados, o responsável pelo tratamento ou o subcontratante só se exime de responsabilidade se tiver demonstrado que o evento danoso não decorreu por atitude deliberada ou falha dele<sup>199</sup>.

Como pode ser visto, na GDPR há referência explícita à indenização por danos

<sup>196</sup> UNIÃO EUROÉIA. *Regulamento 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation)*. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679#:~:text=O%20presente%20regulamento%20respeita%20todos,pensamento%2C%20de%20consci%C3%Aancia%20e%20de>>. Acesso em: 03 jun. 2022.

<sup>197</sup> Ibid.

<sup>198</sup> Ibid.

<sup>199</sup> VIGLIANISI FERRARO; TOMASEVICIUS FILHO, op. cit.

extrapatrimoniais, que parece ser o principal tipo de prejuízo que pode resultar da violação das regras relativas ao direito fundamental ao uso correto de dados pessoais.

A Itália, por meio do Decreto Legislativo nº 101<sup>200</sup>, de 10 de agosto de 2018, regulamentou o utilização dos dados pessoais em seu território. Semelhante a legislação européia, se introduziu um modelo de responsabilidade agravada, gerando uma inversão do ônus da prova, em favor da pessoa lesada, remetendo-se às regras que exemplificam como os dados pessoais de outras pessoas devem ser tratados para que seu uso seja considerado legítimo.

Analisando a responsabilidade civil na GDPR, quanto a ocorrência de dano *in re ipsa* a ser indenizado, sem a necessidade de demonstrar a existência de prejuízo concreto causado pelo ofensor, não foi acolhido pela maioria da doutrina europeia. De qualquer modo, ainda que somente os danos-consequências sejam dignos de reparo, foi questionado que os interesses específicos precisavam ser identificados, ou uma espécie de regra de compensação por danos não pecuniários por uso ilegítimo de dados pessoais.

Com a entrada em vigor da LGPD, notadamente inspirada no GDPR, poder-se-á observar no futuro de que modo a mesma norma jurídica relativa à indenização será aplicada em casos similares a serem julgados no Brasil. Como já visto, mesmo sem estar em vigor, a LGPD já era invocada como se estivesse em vigor para a defesa das pessoas em termos de tratamento ilegítimo de dados.

Os principais problemas relacionados a tratamento ilegítimo de dados que constata-se da análise das decisões dos tribunais do Brasil e da Itália, referem-se a dois tipos de problemas: a falta de consentimento para o tratamento de dados e o vazamento de dados, que é um defeito de armazenamento de dados, ou, nos termos da LGPD, um incidente de dados, conforme o art. 48 da LGPD<sup>201</sup>.

A questão do consentimento é ponto central ao se discutir acerca de tratamento de dados, tanto para a legislação quanto para a jurisprudência, de modo a possibilitar à pessoa a autodeterminação informativa como forma de defender-se de violações aos seus direitos fundamentais, especialmente quanto à privacidade e honra. Contudo, esses conceitos e entendimentos podem alterar-se com o passar do tempo.

Em termos de vazamento de dados, a jurisprudência brasileira é variante quanto ao dano *in re ipsa*. Atualmente, o entendimento predominante é do dano quando houver abuso do

---

<sup>200</sup> ITÁLIA. *Decreto Legislativo nº 101*, de 10.08.2018 (Disposições para a adequação da legislação nacional às disposições do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27.04.2016, relativo à Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como ao acesso gratuito circulação desses dados, e que revoga a Diretiva 95/46/CE).

<sup>201</sup> VIGLIANISI FERRARO; TOMASEVICIUS FILHO, op. cit.

direito ou contrariedade às regras protetivas aos direitos fundamentais, independente de critérios e condições mais restritivas à condenação, como se verifica pela expressa alteração da jurisprudência pelo Superior Tribunal de Justiça.

Quanto ao tratamento na Itália, tem-se, notadamente, a interpretação contrária ao disposto no GDPR que prevê a indenização ampla nesses casos. A jurisprudência italiana adotou critérios em termos de análise dos casos para posterior indenização. Diante disso, há o risco de desestimular cidadãos sem meios econômicos a buscarem proteção de seus direitos fundamentais e merecedores de proteção particularmente incisiva, o que pode contribuir com as condutas ilegais por parte de empresas<sup>202</sup>.

Desde a entrada em vigor do GDPR, em 25 de maio de 2018, na União Europeia, já foram aplicadas mais de 700 sanções, com valor que ultrapassa 293 milhões de euros o somatório das multas aplicadas, como pode ser visto no gráfico no anexo 2, que mostra o número de multas aplicadas, entre julho de 2018 e julho de 2021, com base no GDPR<sup>203</sup>.

Da análise da pesquisa constata-se que a aplicação das sanções foi baixa nos primeiros meses da entrada em vigor do GDPR, isso é uma reflexo da postura adotada pelas Autoridades locais de Proteção de Dados que priorizaram inicialmente a orientação<sup>204</sup>. Inclusive, essa era a expectativa da ANPD. No gráfico do Anexo 3 da presente pesquisa, pode-se observar os motivos que mais levaram à aplicação de multas pelas autoridades europeias.

Constata-se que os motivos mais comuns são “Base legal insuficiente para tratamento de dados” e “medidas técnicas e organizacionais insuficientes para garantir a segurança da informação” que são temas recorrentes também nas decisões sobre a LGPD. E entre os países que mais aplicaram multa na Europa estão: Itália com 83 multas (equivalente a 81,8 milhões de euros decorrentes delas); França com 15 multas (equivalente a 55,1 milhões de euros); Alemanha com 30 multas (equivalente a 49,2 milhões de euros); Reino Unido com 5 multas (equivalente a 44,3 milhões de euros); Espanha com 240 multas (equivalente a 29,7 milhões de euros).

Além disso, já é possível encontrar decisões de tribunais de todo o país que se baseiam

<sup>202</sup> VIGLIANISI FERRARO; TOMASEVICIUS FILHO, op. cit.

<sup>203</sup> VAINZOP, Bruno. *Sanções da LGPD, de competência exclusiva da ANPD, entram em vigor no dia 1º de agosto*. Infógrafo OPICE BLUM. Disponível em: <[<sup>204</sup> Ibid.](https://opiceblum.com.br/sancoes-da-lgpd-de-competencia-exclusiva-da-anpd-entram-em-vigor-no-dia-1o-de-agosto/#:~:text=1%C2%BA%20de%20agosto-,San%C3%A7%C3%B5es%20da%20LGPD%2C%20de%20compet%C3%A2ncia%20exclusiva%20da%20ANPD%2C%20entram%20em,no%20dia%201%C2%BA%20de%20agosto&text=INFOGR%C3%81FICO%207C%20As%20san%C3%A7%C3%B5es%20administrativas%20da,domingo%2C%20dia%201%C2%BA%20de%20agosto.>. Acesso em: 08 mai. 2022.</a></p>
</div>
<div data-bbox=)

na LGPD. De acordo com a pesquisa feita pela Opice Blum<sup>205</sup>, entre setembro de 2020 e 25 de junho de 2021, foram expedidas 598 sentenças que tiveram como objeto o uso indevido de dados pessoais por empresas.

No caso dos Estados Unidos, o entendimento é de que o simples vazamento de dados pessoais muitas vezes pode causar aflição ao sujeito, juntamente com o risco de que informações pessoais, sensíveis e de caráter confidencial, possam estar sendo observadas e utilizadas em detrimento de sua honra e dignidade. Mesmo assim, diante das dificuldades de identificação das vítimas e vazamentos, as indenizações no caso de vazamento de dados costumam dar-se somente pela via coletiva ou mesmo na forma sancionatória<sup>206</sup>.

O reconhecimento de um dano moral a cada indivíduo atingido pelo vazamento de dados representa um prejuízo pelas indenizações a serem suportadas pela empresa, devido ao número excessivo de ações individuais de valores baixos.

No direito norte-americano, existe a figura das *claim resolution facilities*, utilizada no âmbito da reparação de danos massificados. São entidades administradoras destinadas à distribuição equânime de indenizações entre as vítimas de danos reconhecidos em acordo ou judicialmente<sup>207</sup>.

Sendo assim, o Regulamento Europeu, assim como a LGPD, além de constituírem norma principiológica, observa-se que o texto e sua interpretação guardam consonância com as principais diretrizes de direitos humanos e, conseqüentemente, orienta o uso da Internet a luz dos direitos personalíssimos e fundamentais do indivíduo.

O GDPR manteve o princípio geral de que o controlador detém a responsabilidade principal sob qualquer atividade de seu controle, mas reconhece também, que os processadores devem ser diretamente responsáveis em relação aos titulares de dado.

Proteção dos dados pessoais e o respeito pela vida privada são direitos fundamentais, nesse sentido, o Parlamento Europeu propõe salvaguardar os dados pessoais na União Europeia, aumentando o controle dos utilizadores sobre os seus próprios dados e reduzindo os custos para as empresas. Atitude semelhante é o que se busca quanto à adequação das empresas brasileiras, inclusive pela própria Autoridade Nacional de Proteção de Dados, a ANPD.

---

<sup>205</sup> Ibid.

<sup>206</sup> GARCIA, Rafael S. *O papel da autoridade nacional de proteção de dados e os colegitimados na defesa dos titulares de dados pessoais*. Dissertação – Mestre em Direito Econômico e Desenvolvimento, Instituto brasileiro de ensino, pesquisa e desenvolvimento, Universidade de Brasília. Brasília, 2021, p. 28.

<sup>207</sup> Ibid.

## CONCLUSÃO

O presente trabalho dispôs-se a analisar como questão principal a identificação do regime de responsabilização civil adotado pela Lei Geral de Proteção de Dados. Embora seja um importante marco regulatório que sistematiza o tratamento de dados pessoais no Brasil, a lei não foi explícita quanto ao regime de responsabilização civil diante dos casos de vazamento de dados, se subjetivo, calcado na culpa, ou objetivo, calcado no risco da atividade.

Os dados pessoais estão entre os bens mais valiosos economicamente que qualquer indivíduo possui. Exercem influência sobre as liberdades civis e direitos fundamentais, em suma, os dados pessoais possuem uma importância transversal e impactam indivíduos e sociedade de maneiras diversas, do ponto de vista econômico e social.

Como visto ao longo da pesquisa, a Lei Geral de Proteção de Dados criou um sistema de responsabilidade civil compatível com o Código Civil e o Código de Defesa do Consumidor para regular as relações jurídicas de direito privado baseadas no tratamento de dados pessoais. Porém, conforme exposto, o tema é divergente nos embates doutrinários e jurisprudência.

A princípio, verifica-se que a Lei Geral de Proteção de Dados elegeu o sistema de responsabilidade civil subjetiva em perfeito alinhamento com o Código Civil, inserindo-se de forma harmoniosa no mosaico legislativo. Um aspecto que precisa ser acompanhado é a adoção da teoria da culpa para a responsabilização, para não dificultar o acesso da vítima à justiça e a afastar a reparação do dano.

Porém, a LGPD atrai também um sistema de responsabilidade objetiva, se aproximando ao Código de Defesa do Consumidor que, dado o tratamento Constitucional da defesa do consumidor, atrai para seu sistema de responsabilidade objetiva os fatos jurídicos dessa natureza. E do mesmo modo que os consumidores, os titulares são considerados também hipossuficientes.

Como visto, há muitas semelhanças entre ambas as legislações quanto a responsabilização dos agentes de tratamento ou fornecedores e vendedores de produtos. Como também no tocante a possibilidade de inversão do ônus da prova a favor do titular dos dados em uma eventual ação judicial, seguindo os mesmos requisitos previstos no CDC, a verossilhança das alegações e a hipossuficiência técnica do titular/consumidor.

Na presente pesquisa, adotou-se como hipóteses de pesquisa que a LGPD teria adotado a prevenção de danos como valor máximo a ser perseguido pelos agentes de tratamento, de modo que o regime de responsabilidade a ser adotado deve refletir esse posicionamento. Assim, para que houvesse a responsabilização diante de um caso de vazamento, necessitaria de uma

comprovação do dano sofrido diretamente pelo titular do dado.

Antes disso, precisou ser feita uma análise quanto ao dano patrimonial e extrapatrimonial decorrente dos incidentes de segurança, e depois de entender os diferentes papéis do controlador e do operador de dados, bem como suas respectivas responsabilidades dentro do processo de tratamento de dados. Em seguida, foi analisada a questão-problema exposta: a responsabilidade civil da LGPD é objetiva, dispensa a comprovação do dano, nessa o simples incidente de vazamento de dados já comprova o dever de indenizar, ou é subjetiva, sendo preciso que ocorra um dano direto ao titular do dado e que esse seja comprovado para ser indenizado, não bastando a mera exposição dos dados no vazamento?

Após o estudo aqui desenvolvido, juntamente com a análise jurisprudencial realizada, encontraram-se elementos que puderam confirmar que a LGPD se insere em um sistema de proteção de dados pessoais, para aperfeiçoar o arcabouço normativo e permitir maior robustez aos direitos dos titulares de dados. Inclusive, isso já pode ser observado desde o art. 1º da lei, ao dispor que o objetivo dela é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A concepção de privacidade adotada pelo legislador aponta para uma noção segundo a qual o desenvolvimento da personalidade é a essência desse conceito. Nesse sentido, a proteção de dados deixa de ser apenas uma forma de tutela de dados pessoais para se tornar uma forma de anteparo à autodeterminação do indivíduo.

Durante a pesquisa, verificou-se que a LGPD, com vistas a maior proteção dessa concepção de privacidade, adotou mecanismos de proteção dos titulares de dados que se compatibilizam com a preocupação de que o tratamento de dados pode representar riscos à individualidade, autonomia e liberdade.

No que diz respeito às regras relativas ao tratamento de dados, evidencia-se uma preocupação com a prevenção de danos, especialmente ao se analisar os princípios de “segurança”, “prevenção” e a “responsabilização e prestação de contas”. A lei previu mecanismos de mitigação do risco de dano a serem adotados pelos agentes de tratamento, a fim de garantir o cumprimento das normas de proteção de dados pessoais e salvaguardar os direitos dos titulares de dados.

A lei buscou estabelecer padrões de conduta a serem observados pelos agentes de tratamento com vistas a não ocorrência de danos. Nesse ponto, o regime de responsabilidade civil adotado pela lei parece se clarificar e ganhar maior visualização.

Quanto ao regime subjetivo, demonstrou-se que a concepção atual de culpa desconsidera a vontade do agente para o descumprimento da norma, levando-se em conta

apenas o padrão de conduta esperado na situação concreta. Sendo padrão de conduta apresentado ao longo da lei, baseando-se na criação de deveres aos agentes de tratamento, prezando pela conduta preventiva e visando sempre a não ocorrência de danos ou a mitigação do risco de dano.

Como exposto, o argumento de maior relevo para a adoção do regime subjetivo é justamente o fato da lei estabelecer deveres aos agentes de tratamento. Mas o simples estabelecimento de deveres aos agentes de tratamento não é elemento suficientemente apto a definir como subjetivo o regime de responsabilização previsto na LGPD.

Já o regime de responsabilidade civil objetivo, o risco da atividade é um dos fatores que fazem incidir sua característica objetiva. Contudo, na LGPD, o risco é inerente ao desenvolvimento da atividade de tratamento de dados, devendo-se analisá-lo para avaliar seu impacto de modo a preservar e proteger os direitos dos titulares de dados pessoais.

Por essa razão, a adoção de um regime objetivo parece ser o caminho mais adequado, na medida em que a LGPD disciplinou de maneira bastante vigorosa a adoção de um comportamento proativo dos agentes de tratamento.

Com o desenvolvimento da pesquisa, demonstrou-se que a estrutura da lei é voltada para uma análise preventiva, buscando a minimização da ocorrência de riscos e a mitigação de danos, explicitando a natureza intrínseca do risco na atividade de tratamento de dados.

Do mesmo modo, da análise do regulamento e das decisões internacionais sobre proteção de dados, constatou-se que é esse mesmo o intuito, as legislações de proteção de dados buscam minimizar os riscos e mitigar os danos aos dados pessoais. O Regulamento Europeu, por exemplo, assim como a LGPD, além de constituírem norma principiológica, observamos que o texto e sua interpretação guardam consonância com as principais diretrizes de direitos humanos e, conseqüentemente, orienta o uso da Internet a luz dos direitos personalíssimos e fundamentais do indivíduo.

No tocante a responsabilidade civil, a GDPR manteve o princípio geral de que o controlador detem a responsabilidade principal sob qualquer atividade de seu controle, mas reconhece também, que os processadores devem ser diretamente responsáveis em relação aos titulares de dados.

De acordo com a análise das decisões judiciais, notou-se que as mesmas já levavam em consideração a LGPD, antes mesmo de sua vigência, apontando importantes princípios relacionados à minimização de riscos no tratamento de dados, como adequação e necessidade. Sendo assim, o entendimento dominante hoje nos Tribunais Superiores é a prevalência do regime da responsabilidade objetiva para a proteção dos direitos dos titulares de dados,



porém, a discussão acerca do tema segue acirrada.

## REFERÊNCIAS

ALVES, Rodrigo da Costa. *Regimes de responsabilidade civil dos agentes de tratamento na lei geral de proteção de dados pessoais – lei nº 13.709/18*. Monografia curso de Direito, Faculdade de Direito – FD/UNB, Universidade de Brasília – UNB. Brasília, 2020.

AMORIM, Filipo Bruno Silva. *O sistema da responsabilidade no Código Civil de 2002: prevalência da responsabilidade subjetiva ou objetiva?*. Disponível em: <<https://jus.com.br/artigos/22841/o-sistema-da-responsabilidade-no-codigo-civil-de-2002-prevalencia-da-responsabilidade-subjetiva-ou-objetiva>>. Acesso em: 03 abr. 2022.

ARAÚJO, Adriana Baker Goveia.; WESTINEBAID, Ana Augusta R. *Uma análise jurídica sobre o marco civil da internet. Colloquium Socialis, Presidente Prudente*, v. 01, n. Especial, p.655-661 jan/abr 2017. Disponível em: <<http://www.unoeste.br/site/enepe/2016/suplementos/area/Socialis/Direito/UMA%20AN%C3%81LISE%20JURIDICA%20SOBRE%20O%20MARCO%20CIVIL%20DA%20INTERNET.pdf>> Acesso em: 26 mai. 2021.

BRASIL. *Código Civil*. 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: 23 mai. 2022.

\_\_\_\_\_. *Código de Defesa do Consumidor*. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/18078compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm)>. Acesso em: 05 jun. 2021.

\_\_\_\_\_. Decreto nº 7.962, de 15 de março de 2013. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/decreto/d7962.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm)>. Acesso em: 05 jun. 2021.

\_\_\_\_\_. *Lei nº 12.735*, de 30 de novembro de 2012. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112735.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112735.htm)>. Acesso em: 26 mai. 2021.

\_\_\_\_\_. *Lei nº 12.737*, de 30 de novembro de 2012. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm)>. Acesso em: 26 mai. 2021.

\_\_\_\_\_. *Lei nº 12.965*, de 23 de abril de 2014. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm)>. Acesso em: 26 mai. 2021.

\_\_\_\_\_. *Lei nº 13.709*, de 14 de agosto de 2018. 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: 05 jun. 2021.

\_\_\_\_\_. Ministério Público do Distrito Federal e Territórios. Comissão de Proteção dos Dados Pessoais. 1ª Promotoria de Justiça de Defesa do Consumidor. *Portaria n. 2 / 2018 - Inquérito Civil Público - ICP - Cambridge Analytica / Facebook*. Disponível em: <https://www.conjur.com.br/dl/mp-dftinvestiga-cambridge-analytica.pdf> Acesso em: 20 abr. 2021.

\_\_\_\_\_. Ministério da Justiça e Segurança Pública. *Nota Técnica n.º 32/2019/CGCTSA/DPDC/SENACON/MJ. Prática abusiva. Violação aos princípios da boa-fé, ao direito à privacidade e à informação clara e adequada sobre bens e serviços*. Disponível em: <[https://brunobioni.com.br/wp-content/uploads/2020/01/SEI\\_08012.000723\\_2018\\_19-1-1.pdf](https://brunobioni.com.br/wp-content/uploads/2020/01/SEI_08012.000723_2018_19-1-1.pdf)> . Acesso em: 29 mai. 2022.

\_\_\_\_\_. Senado Federal. *Proposta de emenda à Constituição Federal n.º 17 de 2019*. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1633717204657&disposition=inline>>. Acesso em: 04 jun. 2022.

\_\_\_\_\_. Superior Tribunal de Justiça. Compartilhamento de informações de banco de dados exige notificação prévia ao consumidor. Disponível em: <<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Compartilhamento-de-informacoes-de-banco-de-dados-exige-notificacao-previa-ao-consumidor.aspx>>. Acesso em: 08 jan. 2022.

\_\_\_\_\_. Superior Tribunal de Justiça. *REsp: 971844 RS 2007/0177337-9. Relator: Ministro Teori Albino Zavascki*. Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/8591223/recurso-especial-resp-971844-rs-2007-0177337-9/inteiro-teor-13674826>>. Acesso em: 03 jun. 2022.

\_\_\_\_\_. Superior Tribunal de Justiça. *Resp. n.º 1758799 MG 2017/0006521-9*, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 12/11/2019, T3 - TERCEIRA TURMA, Data de Publicação: DJe 19/11/2019). Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/859849413/recurso-especial-resp-1758799-mg-2017-0006521-9/inteiro-teor-859849423?ref=serp>>. Acesso em: 08 jun. 2022.

\_\_\_\_\_. Superior Tribunal de Justiça. *REsp 1.473.846/SP 2014/0184129-1*. Relator: Ministro Ricardo Villas Bôas Cueva. Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/443282925/recurso-especial-resp-1473846-sp-2014-0184129-1/inteiro-teor-443282935>>. Acesso em: 03 jun. 2022.

\_\_\_\_\_. Superior Tribunal de Justiça. (3ª Turma). *REsp. n.º 1758799/MG*. Relatora: Min. Nancy Andrighi. Brasília, 12.11.2019. Publicado no DJe em 19.11.2019.

\_\_\_\_\_. Tribunal Superior do Trabalho (6ª Turma). *RR n.º 118-55.2013.5.09.01273*. Relatora: Min. Katia Magalhães Arruda. Brasília, 06.12.2017.

\_\_\_\_\_. Tribunal de Justiça do Distrito Federal e dos Territórios (15ª Vara Cível da Circunscrição Especial Judiciária de Brasília). *Ação Civil Pública 0721831-64.2018.8.07.0001*. Disponível em: <https://www.jusbrasil.com.br/processos/203231447/processo-n-072XXXX-6420188070001-do-tjdf>. Acesso em: 20 de mai. de 2022.

\_\_\_\_\_. Tribunal de Justiça de São Paulo. *Apelação n.º 101139195.2015.8.26.0005*. Relator: Desembargador Francisco Eduardo Loureiro. Disponível em: < <https://tj-sp.jusbrasil.com.br/jurisprudencia/350317872/apelacao-apl-10113919520158260005-sp-1011391-9520158260005>>. Acesso em: 03 jun. 2022.

BRANDÃO, Raquel. *Plataforma vaza 1,75 bilhão de dados de clientes de marketplaces e Correios*. Disponível em: < <https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2021/10/13/plataforma-vaza-175-bilhao-de-dados-de-clientes-de-marketplaces-e-correios.ghtml>>. Acesso em: 31 mai. 2022.

CAPANEMA, Walter Aranha. *A responsabilidade civil na Internet: Uma Análise da Lei 12.965/2014*. Revista da EMERJ, Rio de Janeiro, v. 20, n. 78, p. 107 - 123, Janeiro/Abril. 2017.

\_\_\_\_\_. *A responsabilidade civil na Lei Geral de Proteção de Dados*. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

CARVALHO, Rhayra Melo Ribeiro de. *Responsabilidade civil no Direito do Consumidor*. Disponível em: <<https://jus.com.br/artigos/50652/responsabilidade-civil-no-direito-do-consumidor>>. Acesso em: 23 mai. 2021.

CAVALIERI FILHO, Sérgio. *Programa de responsabilidade civil*. 9. ed. São Paulo: Atlas, 2009, p. 16.

CONJUR. *MP-DF investiga se Facebook repassou dados de brasileiros para publicidade*. Disponível em: <<https://www.conjur.com.br/2018-mar-22/mp-df-investiga-facebook-repassou-dados-brasileiros>> Acesso em: 20 mai. 2022.

DANTAS, Thaile. *Netshoes terá de pagar R\$500 mil por vazamento de dados de milhões de clientes*. Disponível em: < <https://thaile.jusbrasil.com.br/noticias/685006882/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-milhoes-de-clientes>>. Acesso em: 07 jun. 2022.

DEMARTINI, Felipe. *Eletrobras e Copel são vítimas de ataques de ransomware*. Site Canal Tech. Disponível em: <<https://canaltech.com.br/seguranca/eletrobras-e-copel-sao-vitimas-de-ataques-de-ransomware-178557/>>. Acesso em 30 mai. 2022.

DIDIER JR., Fredie; ZANETI JR., Hermes. *Justiça multiportas e tutela constitucional adequada: autocomposição em direitos coletivos*. In: \_\_\_\_\_; \_\_\_\_\_; CABRAL, Trícia Navarro Xavier. *Justiça multiportas: mediação, conciliação, arbitragem e outros meios de solução adequada para conflitos*. V. 9. Salvador: JusPodivm, 2017, p. 54.

DINIZ, Maria Helena. *Curso de direito civil brasileiro*. 23. ed. refor. V. VII. São Paulo: Saraiva, 2009, p. 7 e 8.

DONEDA, Danilo. *Da privacidade à Proteção de Dados Pessoais*. 2. Ed. São Paulo: Revista dos Tribunais, 2020, p. 290.

FACHINELLO, João Antônio Tschá. *Acordos e tutela coletiva: algumas reflexões a partir do TAC no caso do vazamento de dados da Netshoes*. Revista Iberoamericana de Derecho Procesal, v. 10, p. 85-112, jul./ dez. 2019.

FERREIRA, Diogo Ramos. *Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva?* 2019. Disponível em: < <https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019>>. Acesso em: 3 jun. 2022.

FOLHA DE SÃO PAULO. *Como a Cambridge Analytica recolheu dados do Facebook: Entenda a estratégia usada por aliados de Trump durante a campanha eleitoral*, 21 mar. 2018. Disponível em: <<https://www1.folha.uol.com.br/mercado/2018/03/como-a-cambridge-analytica-recolheu-dados-dofacebook.shtml>> Acesso em: 20 mai. 2022.

FONSECA, Edson Pires da. *Lei Geral de Proteção de Dados Pessoais – LGPD*. Salvador: JusPodivm, 2021, p. 53.

FRANZOLIN, Cláudio José; VALENTE, Victor Augusto Estevam. *Alguns apontamentos sobre a responsabilidade ativa mediante a prestação de contas e a prevenção de danos por meio de conformidades*. *Revista de Direito do Consumidor*. V. 133. Ano 30. p. 75-106. São Paulo: RT, jan./fev. 2021. Disponível em: <<https://dspace.almg.gov.br/handle/11037/4015>>. Acesso em: 26 mai. 2021.

GARCIA, Rafael S. *O papel da autoridade nacional de proteção de dados e os colegitimados na defesa dos titulares de dados pessoais*. Dissertação – Mestre em Direito Econômico e Desenvolvimento, Instituto brasileiro de ensino, pesquisa e desenvolvimento, Universidade de Brasília. Brasília, 2021, p. 28.

GOMES, Maria Cecília Oliveira. *Entre o método e a complexidade: compreendendo a noção de risco na LGPD*. In: PALHARES, Felipe (coord.). *Temas Atuais de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2020, p. 245-273.

GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro: Responsabilidade Civil*. 7. ed. V.4. São Paulo: Saraiva, 2012. p. 18.

GUEDES, Gisela Sampaio da Cruz; TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde. *Fundamentos do Direito Civil*. V.4. Rio de Janeiro: Forense, 2020, p. 4.

GUEDES, Gisela Sampaio da Cruz; VENCELAU MEIRELES, Rose Melo. *Término do Tratamento de Dados*. In: TEPEDINO, Gustavo et al. *Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 219-241.

JUSBRASIL. Painel LGPD nos tribunais. Disponível em: <<https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html>>. Acesso em: 03 jun. 2022.

MARTINS, Guilherme Magalhães. *Vulnerabilidade e responsabilidade Civil na Internet: a inconstitucionalidade do artigo 19 do Marco Civil*. *Revista de Direito do Consumidor*. v. 137/2021, Set - Out / 2021. Rio de Janeiro, p. 33 a 59.

MENDES, Laura Schertel; DONEDA, D. *Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil*. *Revista de Direito do Consumidor*, São Paulo, v. 120, ano 27, p. 469- 483, nov.-dez. 2018.

MENDONÇA, Rafael Dantas Carvalho de. *A responsabilidade Civil no direito brasileiro*. Disponível em: <<https://conteudojuridico.com.br/consulta/Artigos/51542/a-responsabilidade-civil-no-direito-brasileiro>>. Acesso em 04 jun. 2022.

MORAES, Maria Celine Bodin de. *LGPD: um novo regime de responsabilização dito*

“proativo”, Civilistica.com, Rio de Janeiro, ano 8, n. 3, 2019. Disponível em: <<http://civilistica.com/lgpd-um-novo-regime/>>. Acesso em: 4 jun. 2022.

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.

MULHOLLAND, Caitlin. *A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?* Disponível em: <<https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco>>. Acesso em: 26 mai. 2021.

NEVES, Thiago Ferreira Cardoso. *O Comércio Eletrônico e o Direito do Consumidor*. Disponível em: <[https://www.emerj.tjrj.jus.br/revistaemerj\\_online/edicoes/revista64/revista64\\_154.pdf](https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista64/revista64_154.pdf)>. Acesso em: 02 jun. 2021.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. *Responsabilidade Civil na LGPD: Problemas e soluções*. Disponível em: <<https://indexlaw.org/index.php/conpedireview/article/view/7024>>. Acesso em: 04 jun. 2022.  
 RECUERO, Raquel. *Redes Sociais na Internet*. Porto Alegre: Sulina, 2009, p. 191.

RODRIGUES, Marcel André. *A responsabilidade civil e o Código de Defesa do Consumidor*. Disponível em: <<https://marcelandre.jusbrasil.com.br/artigos/126510917/a-responsabilidade-civil-e-o-codigo-de-defesa-doconsumidor>>. Acesso em: 23 mai. 2021.

SAFERNET. *Safernet Brasil*. 2005. Disponível em: <<https://new.safernet.org.br/content/institucional>>. Acesso em: 10 jun. 2021.

SCHREIBER, Anderson. *Marco Civil da Internet: Avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiros*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. *Direito & Internet III; Marco Civil da Internet*. T. II. São Paulo: Quartier Latin, 2015.

SCHREIBER, Anderson. *Responsabilidade Civil na Lei Geral de Proteção de Dados*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2020, p. 319 a 337.

SOARES, Jéssica. *O Direito do Consumidor e a sua relação com a Lei Geral de Proteção de Dados (LGPD) à Luz da Responsabilidade Civil*. In: PINHEIRO, Ana Cristina Augusto (Coord.). *Temas Contemporâneos para TCC*. V. 04. Rio de Janeiro: Processo, 2021, p. 17 a 32.  
 STOLZE, Pablo; PAMPOLHA FILHO, Rodolfo. *Novo Curso de Direito Civil: Responsabilidade Civil*. 10. ed. São Paulo: Saraiva, 2013, p. 97.

TARTUCE, Flávio; NEVES, Daniel Assumpção. *Manual de Direito do Consumidor*. 7. ed. São Paulo: Forense, 2018, p. 129 a 139.

TASSO, Fernando Antonio. *A responsabilidade civil na Lei Geral de Proteção de Dados e sua*

interface com o Código Civil e o Código de Defesa do Consumidor. *Cadernos Jurídicos*, São Paulo, ano 21, n. 53, p. 97-115, jan.-mar./2020. Disponível em: <[https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii\\_1\\_interface\\_entre\\_a\\_lgpd.pdf?d=637250344175953621](https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_a_lgpd.pdf?d=637250344175953621)>. Acesso em: 04 jun. 2022. p.105.

TEFFÉ, Chiara Spadaccini de. Direito à imagem na internet: estudo sobre o Tratamento do Marco Civil da internet para os casos de divulgação não autorizada de imagens íntimas. *Revista de Direito Civil Contemporâneo*. v. 15/2018, p. 93 a 127. Disponível em: <<http://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/413>>. Acesso em: 07 jun. 2022.

TEPEDINO, Gustavo; SILVA, *Rodrigo da Guia*. *Desafios da inteligência artificial em matéria de responsabilidade civil*. *Revista Brasileira de Direito Civil – RBDCivil*, v. 21, Belo Horizonte, jul./set. 2019, p. 79.

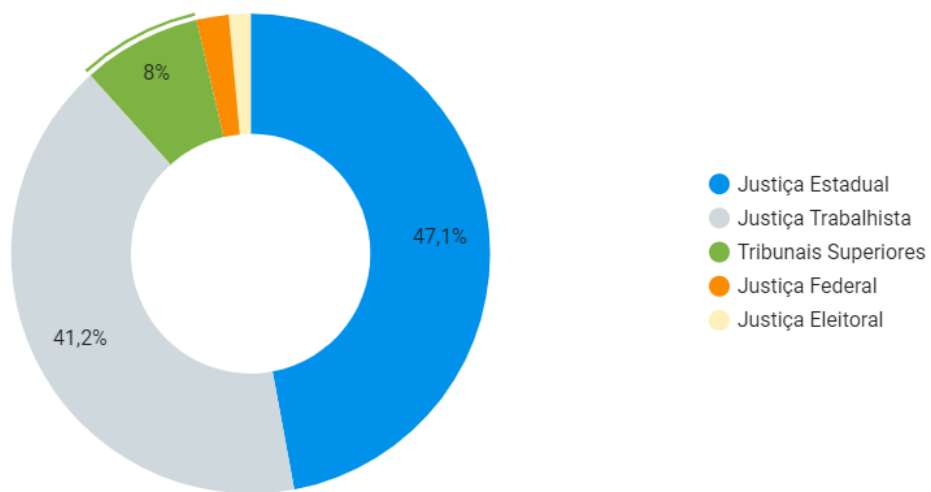
UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679#:~:text=O%20presente%20regulamento%20respeita%20todos,pensamento%2C%20de%20consci%C3%Aancia%20e%20de>>. Acesso em: 03 jun. 2022.

VAINZOF, Rony. *Da responsabilidade por danos decorrentes de conteúdo gerado por terceiros*. In: Del Masso, Fabiano; Abrusio, Juliana; Filho, Marco Aurélio Florêncio (coords.). *Marco Civil da internet lei 12.965/2014*. São Paulo: Editora Revista dos Tribunais. 2014.

VAINZOP, Bruno. *Sanções da LGPD, de competência exclusiva da ANPD, entram em vigor no dia 1º de agosto*. Infógrafa OPICE BLUM. Disponível em: <[https://dspace.almg.gov.br/handle/11037/41773](https://opiceblum.com.br/sancoes-da-lgpd-de-competencia-exclusiva-da-anpd-entram-em-vigor-no-dia-1o-de-agosto/#:~:text=1%C2%BA%20de%20agosto-,San%C3%A7%C3%B5es%20da%20LGPD%2C%20de%20compet%C3%Aancia%20exclusiva%20da%20ANPD%2C%20entram%20em,no%20dia%201%C2%BA%20de%20agosto&text=INFOGR%C3%81FICO%20%7C%20As%20san%C3%A7%C3%B5es%20administrativas%20da,domingo%2C%20dia%201%C2%BA%20de%20agosto.>. Acesso em: 08 mai. 2022.</p>
<p>VIGLIANISI FERRARO, Angelo; TOMASEVICIUS FILHO, Eduardo. Indenização pelo tratamento ilegítimo de dados pessoais: comparação entre os direitos italiano e brasileiro. <i>Revista dos Tribunais [Recurso Eletrônico]</i>. São Paulo, n.1031, set. 2021. Disponível em: <a href=). Acesso em: 26 mai. 2022.

VIVIAN, Wilson de Alcântara Buachi. *Princípio alterum non laedere (neminem laedere), dignidade humana e boa-fé*. 2016. Disponível em: <<https://ambitojuridico.com.br/cadernos/direito-civil/principio-alterum-non-laedere-neminem-laedere-dignidade-humana-e-boa-fe/>>. Acesso em: 03 jun. 2021.

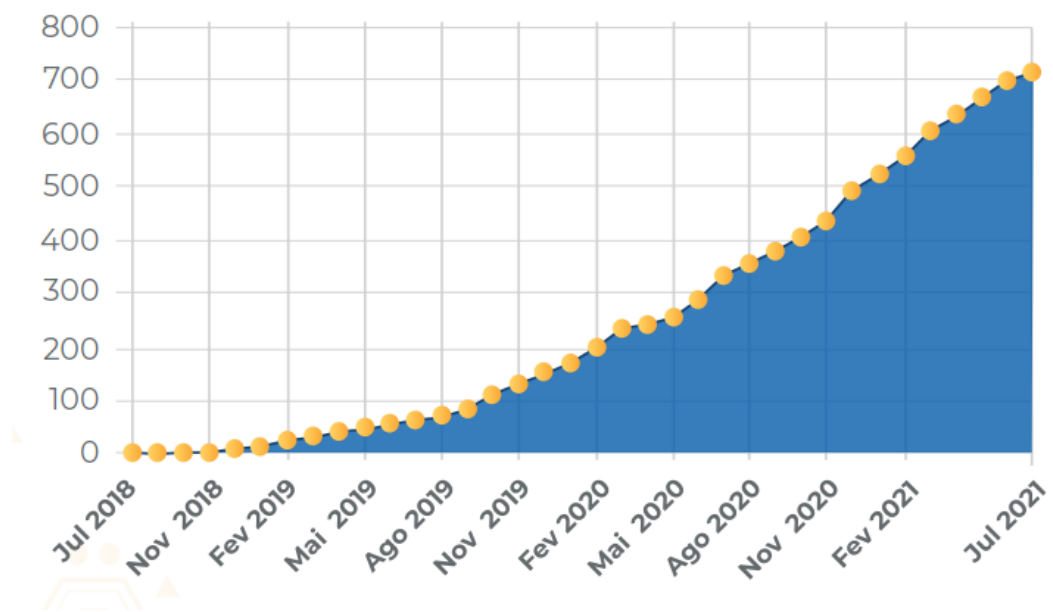
## ANEXO 1



Tribunais que emitiram mais decisões envolvendo a LGPD no primeiro ano de sua vigência.  
(JUSBRASIL, *Painel LGPD nos tribunais.*)



## ANEXO 2

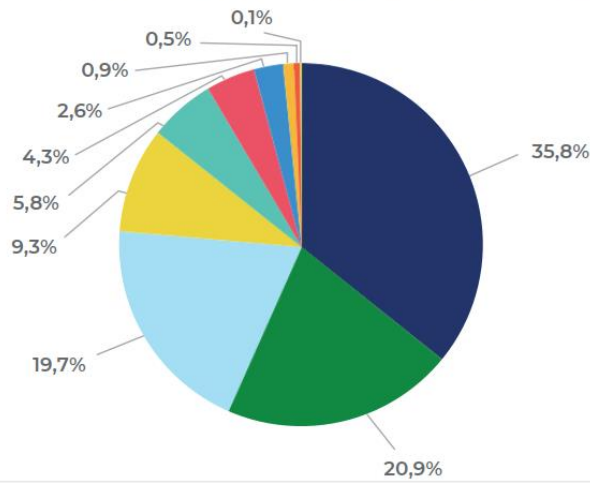


Número de multas aplicadas, entre julho de 2018 e julho de 2021, com base no GDPR.

(Infógrafa OPICE BLUM)

## ANEXO 3

## MOTIVOS DAS MULTAS APLICADAS PELAS AUTORIDADES EUROPEIAS



VIOLAÇÃO	NÚMERO DE MULTAS
■ Base legal insuficiente para tratamento de dados	265
■ Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação	155
■ Desacordo com os princípios gerais de processamento de dados	146
■ Atendimento insuficiente aos direitos dos titulares dos dados	69
■ Atendimento insuficiente às obrigações de informação	43
■ Cooperação insuficiente com a Autoridade supervisora	32
■ Cumprimento insuficiente das obrigações de notificação de violação de dados	19
■ Ausência de nomeação do DPO ( <i>Data Protection Officer</i> )	7
■ Acordo insuficiente de processamento de dados	4
■ Desconhecida	1

Motivos mais recorrentes na aplicação de multas pelas autoridades europeias. (Infógrafo OPICE BLUM)