INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA
MESTRADO ACADÊMICO EM DIREITO

Laryssa Ribeiro Avelino

# RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO EM CASOS DE VIOLAÇÃO À PROTEÇÃO DE DADOS PESSOAIS:

Uma Análise dos Sistemas Brasileiro e Europeu

BRASÍLIA, DF
2024

Laryssa Ribeiro Avelino

# RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO EM CASOS DE VIOLAÇÃO À PROTEÇÃO DE DADOS PESSOAIS:

Uma Análise dos Sistemas Brasileiro e Europeu

Dissertação apresentada como requisito parcial para obtenção do título de Mestre (a) em Direito Constitucional, pelo Programa de Pós-Graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP.

Orientadora: Profa. Dra. Laila Maia Galvão
Coorientador: Prof. Dr. Guilherme Pereira Pinheiro

BRASÍLIA, DF
2024

Código de catalogação na publicação – CIP

A949 Avelino, Laryssa Ribeiro
Responsabilidade civil dos agentes de tratamento em casos de violação à proteção de dados pessoais: uma análise dos sistemas brasileiro e europeu / Laryssa Ribeiro Avelino. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2024.

107 f. : il. color.

Orientadora: Profª. Drª. Laila Maia Galvão
Coorientador: Prof. Dr. Guilherme Pereira Pinheiro

Dissertação (Mestrado Acadêmico em Direito Constitucional) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2024.

1. Responsabilidade civil. 2. Proteção de dados - legislação - Brasil - Europa. 3. Tratamento de dados - aspectos jurídicos. I.Título

CDDir 342.151

Elaborada por Natália Bianca Mascarenhas Puricelli – CRB 1/3439

LARYSSA RIBEIRO AVELINO

**RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO EM CASOS DE VIOLAÇÃO À PROTEÇÃO DE DADOS PESSOAIS:**
Uma Análise dos Sistemas Brasileiro e Europeu

Dissertação de Mestrado apresentada como requisito parcial para obtenção do título de Mestre em Direito Constitucional, pelo Programa de Pós-Graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP).

Orientadora: Profa. Dra. Laila Maia Galvão

Brasília, 30 de julho de 2024.

**BANCA EXAMINADORA**

---

**Profª. Dra. Laila Maia Galvão**
Orientador(a)
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

---

**Prof. Dr. Guilherme Pereira Pinheiro**
Coorientador(a)
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

---

**Prof. Dr. Vinicius Gomes de Vasconcellos**
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa
Membro Interno

---

**Prof. Dr. Antonio Alex Pinheiro**
Centro de Ensino Unificado de Brasília
Membro Externo

## AGRADECIMENTOS

A Deus, pelo milagre da vida, pela graça que se renova a cada nova manhã, pelo amor incondicional.

Ao meu esposo, amigo, companheiro de jornada e o maior apoiador dos meus projetos e sonhos.

Aos meus pais, pelos anos de dedicação incansável à minha educação e desenvolvimento como ser humano e à minha família, os de sangue e os por escolha, por todo o apoio.

Aos meus amigos, que diariamente carregam os fardos e alegrias da vida comigo. Suas amizades são tesouros inestimáveis que enriquecem minha vida.

Ao IDP, que tem sido minha segunda casa desde 2015 (período de graduação e mestrado), por todas as oportunidades de crescimento e confiança depositada na minha trajetória acadêmica, seja por intermédio da concessão de bolsas de estudos, do apoio ao intercâmbio na Università Degli Studi Roma Tre ou pela oportunidade de ter aulas com as maiores autoridades no Direito no país.

Ao meu coorientador, prof. Guilherme Pereira Pinheiro, por suas excelentes contribuições à minha pesquisa.

Por fim, e não menos importante, à minha orientadora, profª Laila Maia Galvão, pelas incontáveis reuniões e conversas durante o desenvolvimento desta pesquisa, por sua dedicação, empenho e suporte em cada etapa.

## RESUMO

A presente dissertação tem como objetivo analisar a responsabilidade civil dos agentes de tratamento de dados pessoais em casos de violação à proteção de dados, analisando os sistemas normativos e jurisprudenciais do Brasil e do sistema regional de jurisprudência da Europa. A hipótese inicial levantada na pesquisa aponta que a legislação brasileira apresenta algumas lacunas a respeito de qual é o regime de responsabilidade efetivamente adotado e a quem este regime pode ser aplicado. Uma vez que a legislação brasileira de proteção de dados foi inspirada na experiência europeia, a pesquisa parte do pressuposto de que o sistema jurisprudencial regional da Europa pode servir de referência para a busca por interpretação dessas questões omissas. Utilizando uma metodologia jurídico-dogmática, dedutiva, qualitativa e funcionalista, foram analisadas as disposições do GDPR e da LGPD, além das decisões dos Tribunais de Justiça brasileiros, do STJ e do Tribunal de Justiça da União Europeia. A pesquisa apresenta um panorama do desenvolvimento da proteção de dados no Brasil e na Europa, destacando os princípios que regem essas normas e sua relação com a reparação de danos. Ademais, concluiu que a LGPD não adota expressamente um regime de responsabilidade objetiva, devido à complexidade e variabilidade das atividades de tratamento de dados, mas que também não adotou um regime de responsabilidade civil subjetivo nos moldes tradicionais. Identificou-se que os Tribunais tendem a analisar casos de violação à proteção de dados sob a ótica tradicional da responsabilidade civil, não considerando as especificidades do tratamento de dados. Além disso, que a fundamentação jurídica para responsabilidade e indenização por danos materiais, mesmo quando a LGPD é citada, ainda depende fortemente de outros regimes legais, evidenciando a dificuldade dos julgadores em manusear as disposições da LGPD no que tange à responsabilidade civil. Além de que há uma tendência de não reconhecer a violação de dados pessoais e o direito à indenização na ausência de um dano efetivo a outros direitos de personalidade, como imagem, privacidade e honra, tanto na jurisprudência brasileira quanto europeia.



**Palavras-chave:** Proteção de Dados. Responsabilidade Civil. GDPR. LGPD. União Europeia.

## ABSTRACT

This master's thesis investigates the civil liability of personal data processing agents in cases of data protection violations, analyzing the normative and jurisprudential systems of and the regional jurisprudence system in Europe. The initial hypothesis raised in the research suggests that Brazilian legislation presents some gaps regarding the actual liability regime adopted and to whom this regime can be applied. Since Brazilian data protection legislation was inspired by the European experience, this research assumes that the regional jurisprudence system in Europe can serve as a reference for seeking interpretations of these unresolved issues. Using a juridical-dogmatic, deductive, qualitative, and functionalist methodology, the provisions of the GDPR and LGPD, along with decisions from Brazilian courts, the STJ, and the Court of Justice of the European Union, were analyzed. The research presents an overview of data protection development in Brazil and Europe, highlighting the principles governing these norms and their relation to damage compensation. It concludes that the LGPD does not explicitly adopt an objective liability regime but also does not follow a traditional subjective civil liability model. Courts tend to analyze data protection violations through traditional civil liability, overlooking data processing specifics. Furthermore, legal bases for liability and compensation, even under the LGPD, still heavily rely on other legal regimes, highlighting judges' challenges in applying LGPD provisions. There is also a tendency not to recognize data protection violations and the right to compensation in the absence of effective damage to other personality rights, such as image, privacy, and honor, in both Brazilian and European jurisprudence.



**Keywords:** Data Protection. Civil Liability. GDPR. LGPD. European Union.

## LISTA DE GRÁFICOS

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ANPD | Autoridade Nacional de Proteção de Dados |
| ADI | Ação Direta de Inconstitucionalidade |
| CDC | Código de Defesa do Consumidor |
| CEDIS | Centro de Direito, Internet e Sociedade |
| CF | Constituição Federal |
| GDPR | General Data Protection Regulation |
| INSS | Instituto Nacional de Seguridade Social - INSS |
| LGPD | Lei Geral de Proteção de Dados |
| STJ | Superior Tribunal de Justiça |
| TAC | Termo de Ajustamento de Conduta |
| TJAM | Tribunal de Justiça do Amazonas |
| TJBA | Tribunal de Justiça da Bahia |
| TJMG | Tribunal de Justiça de Minas Gerais |
| TJPR | Tribunal de Justiça do Paraná |
| TJRS | Tribunal de Justiça do Rio Grande do Sul |
| TJSP | Tribunal de Justiça de São Paulo |

**SUMÁRIO**

## INTRODUÇÃO

A transformação mais importante ocorrida na sociedade no último século certamente está associada ao desenvolvimento tecnológico. Este, por sua vez, revolucionou o modo com que as informações pessoais são tratadas, bem como trouxe novos desafios aos conceitos de privacidade e intimidade. O surgimento desse grande volume de informações disponíveis online, decorrente do desenvolvimento e ampliação do acesso às tecnologias, resultou na crescente necessidade de lidar com uma grande quantidade de dados pessoais gerados diariamente na rede mundial de computadores.

O mercado percebeu rapidamente o potencial de extrair vantagens econômicas desses conjuntos massivos de dados, não apenas para melhorar a sua eficiência operacional e ganhar vantagem competitiva, mas também para personalizar serviços, otimizar processos e embasar decisões estratégicas.

Uma vez que o desenvolvimento tecnológico está intimamente ligado ao desenvolvimento econômico, os países da Europa podem ser considerados pioneiros nas discussões acerca da proteção de dados pessoais, sobretudo pelo seu histórico em debates sobre regulamentações e busca pela preservação dos direitos individuais[1].

Entretanto, a efetividade dos sistemas normativos que visam proteger direitos não depende apenas da abrangência extensiva de direitos e garantias, mas de um sistema de responsabilidade bem delineado, capaz de coibir as condutas indesejadas e responsabilizar os agentes causadores de danos, mas que, em contrapartida, preserve o desenvolvimento econômico e tecnológico.

Embora exista há alguns anos normas que em alguma medida garantem direitos aos titulares de dados no Brasil, somente com a vigência da Lei Geral de Proteção de Dados - LGPD um sistema de responsabilização sobre a violação à proteção de dados foi criado. No entanto, as leis sobre responsabilidade deixaram lacunas significativas acerca do regime de responsabilização adotado e outras questões.

O Código de Defesa do Consumidor - CDC foi claro ao estabelecer que o regime de responsabilidade adotado para reger as relações de consumo é o da responsabilidade civil objetiva ao afirmar que a reparação do dano independe de verificação de culpa, o que não se verifica na redação da LGPD.

---

[1] BIONI, Bruno; MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz. Tratado de Proteção de Dados Pessoais: Fundamentos, Direitos e a Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2021. ISBN 9786559642089. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 10 set. 2023.

Desse modo, considerando que o sistema jurídico europeu se encontra vários anos mais desenvolvido nas discussões relacionadas à proteção de dados pessoais e responsabilidade civil, a presente pesquisa pretende, a partir de uma análise das legislações e jurisprudências brasileira e europeia, responder aos seguintes questionamentos: (i) Qual é o regime de responsabilidade civil adotado pela LGPD e a quem ele se aplica? e; (ii) Em que medida as normas brasileiras que regem a responsabilização civil para a proteção do titular de dados foram delineadas de modo a permitir a reparação efetiva de danos a estes e de que modo estas normas têm sido aplicadas pelos Tribunais?

A hipótese inicial levantada na pesquisa aponta que a legislação brasileira apresenta algumas lacunas a respeito de qual é o regime de responsabilidade efetivamente adotado e a quem este regime pode ser aplicado, bem como que a Europa, pode servir de referência para a busca por interpretação dessas questões omissas.

O presente trabalho tem como objetivo identificar como está estruturada a responsabilidade civil dos agentes de tratamento em casos de violação à proteção de dados pessoais dos titulares na legislação brasileira, buscando também compreender como esse tema está estruturado na legislação e jurisprudência europeias, a fim de enfrentar possíveis e concretos problemas no sistema de responsabilidade civil implementado pela LGPD.

Além disso, analisar os tipos de violação à proteção de dados pessoais que podem resultar em responsabilidade civil dos agentes de tratamento de dados, bem como quais os critérios utilizados pela jurisprudência para determinar a responsabilidade civil dos agentes de tratamento em casos de violação à proteção de dados pessoais do titular.

A maior parte da legislação aplicável aos casos de violação à proteção de dados são da União Europeia, assim como boa parte da jurisprudência consolidada acerca de temas omissos ou controversos no GPDR. Contudo, o GPDR estabelece que algumas questões de ordem prática relacionadas à responsabilidade civil dos agentes de tratamento devem ser legisladas pelos Estados-Membros, o que justifica a escolha de um país específico para uma compreensão mais aprofundada da aplicação prática do regime de responsabilidade civil adotado em determinados momentos da pesquisa, razão pela qual a legislação e jurisprudência italiana serão utilizadas quando necessário para o fim acima explicitado.

Para a análise dos objetivos desta pesquisa, serão consideradas a legislação brasileira, em especial a LGPD, a legislação europeia, sobretudo o GDPR, além da jurisprudência dos Tribunais de Justiça e do Superior Tribunal de Justiça brasileiros, assim como do Tribunal de Justiça da União Europeia.

Um dos principais pontos a serem explorados na pesquisa é a natureza das obrigações atribuídas aos agentes de tratamento de dados. Será analisado o regime de responsabilidade adotado tanto no sistema brasileiro quanto europeu. O objetivo é compreender as diferenças e semelhanças existentes em relação à responsabilidade civil dos agentes de tratamento, levando em consideração fatores como os tipos e a extensão dos danos indenizáveis, os critérios de fixação do valor indenizatório, possibilidade de responsabilização objetiva, a possibilidade de aplicação da cláusula geral do art. 927 do CC (atividade de risco), dentre outros.

Todos esses questionamentos serão estudados a partir de uma abordagem metodológica jurídico-dogmática, dedutiva, qualitativa e funcionalista para analisar a responsabilidade civil dos agentes de tratamento em casos de violação à proteção de dados pessoais, analisando os sistemas brasileiro e europeu.

A pesquisa jurídico-dogmática consistirá em uma análise aprofundada das leis, regulamentos e jurisprudências relacionados ao tema, bem como a interpretação doutrinária desses instrumentos legais.

A abordagem dedutiva será utilizada para derivar conclusões lógicas a partir das premissas legais e teóricas estabelecidas. Além disso, a pesquisa será qualitativa, focando em análise de conteúdo e interpretação de dados qualitativos, como legislações e decisões judiciais.

Quanto ao direito comparado, a abordagem funcionalista permitirá a identificação de semelhanças funcionais entre os ordenamentos jurídicos e possibilitará o estudo analítico das leis e jurisprudência de cada um e em conjunto[2].

Apesar de o Brasil e os Estados-Membros da União Europeia terem economias, sistemas políticos e culturas distintas, os seus sistemas jurídicos, sobretudo no que diz respeito à proteção de dados, possuem semelhanças relevantes e suficientes para a análise comparada que se propõe no presente estudo.

Ambos os sistemas possuem suas bases no sistema romano-germânico, caracterizado pela existência das leis codificadas e pela interpretação sistemática do direito, além da separação do direito público e privado e o princípio da legalidade como uma das bases do Estado e do Direito.

---

[2] CURY, Paula Maria Nasser. Métodos de Direito Comparado: desenvolvimento ao longo do século XX e perspectivas contemporâneas/Methods of Comparative Law: Developments in the 20th century and contemporary perspectives. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD), ISSN-e 2175-2168, Vol. 6, Nº. 2, 2014 (Ejemplar dedicado a: Julho/Setembro), p. 178.

É importante destacar que a Lei brasileira de proteção de dados foi inspirada e é bastante semelhante em diversos pontos ao mais importante Regulamento sobre proteção de dados na Europa, de modo que alguns artigos da LGPD parecem cópias literais traduzidas do GDPR.

Ademais, os sistemas de responsabilidade civil brasileiro e europeu possuem muitas semelhanças funcionais, como a existência de uma base legal codificada, são regidas pelo princípio da reparação integral, a adoção das ideias de causalidade e culpabilidade, etc.

Pelas razões anteriormente elencadas, a metodologia escolhida permitirá uma compreensão aprofundada dos fundamentos jurídicos, das divergências e convergências entre os sistemas e das nuances da responsabilidade civil dos agentes de tratamento em relação à proteção de dados pessoais do titular de dados.

Acerca das decisões judiciais brasileiras a serem analisadas na presente pesquisa, é importante esclarecer que será utilizado o levantamento de decisões feito pelo Centro de Direito, Internet e Sociedade - CEDIS, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP, e pelo Jusbrasil, no projeto Painel LGPD nos Tribunais, cujo objetivo é o levantamento qualitativo e quantitativo de decisões envolvendo a LGPD nos seus primeiros anos de vigência[3].

Além do mais, serão analisados os acórdãos do Superior Tribunal de Justiça que mencionam a LGPD como referência legislativa. Quanto às decisões europeias, como os temas se encontram mais consolidados, serão utilizadas decisões colegiadas específicas e emblemáticas do Tribunal de Justiça da União Europeia.

No capítulo 1, serão apresentadas as principais normas e princípios que regem a proteção de dados pessoais no Brasil e na Europa, o desenvolvimento da proteção de dados em cada um deles e os respectivos regimes de responsabilidade adotados. Compreender os fundamentos de ambos os sistemas possibilitará uma análise adequada entre os regimes de responsabilidade adotados, bem como viabiliza a análise das decisões proferidas em seus respectivos ordenamentos.

No capítulo 2, será abordada a responsabilidade civil dos agentes de tratamento e outros sujeitos da relação de tratamento de dados no sistema brasileiro de proteção de dados, a partir da análise das leis e jurisprudência europeia, destacando elementos como o regime de

[3] Centro de Direito, Internet e Sociedade (CEDIS-IDP); Jusbrasil. Painel LGPD nos Tribunais: Jurisprudência do 2º ano de vigência da Lei Geral de Proteção de Dados. Última atualização: Abril de 2023 (com dados de setembro de 2022). Disponível em: <https://painel.jusbrasil.com.br/>. Acesso em: 11 set. 2023.

responsabilidade adotado, a responsabilidade em caso de controladoria conjunta, dos encarregados de dados e dos sub-operadores.

Por fim, no capítulo 3, será realizada uma análise qualitativa das decisões judiciais condenatórias em matéria de responsabilidade civil nos referidos sistemas, considerando eventuais desafios e oportunidades de aprimoramento do sistema brasileiro de responsabilidade civil em proteção de dados.

Por fim, em suma, esta dissertação tem como objetivo analisar a responsabilidade civil dos agentes de tratamento em casos de violação à proteção de dados pessoais, comparando as abordagens adotadas pelo sistema brasileiro e europeu, com base na literatura especializada, na legislação e na jurisprudência.

# 1 OS SISTEMAS BRASILEIRO E EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS

## 1.1 Evolução da Proteção de Dados no Brasil

Apesar de o Brasil ter adotado uma legislação específica e sistêmica acerca da proteção de dados pessoais há pouco tempo, é um engano pensar que apenas recentemente o tema ingressou no ordenamento jurídico brasileiro. Isso porque o direito à privacidade, amplamente resguardado na Constituição de 1988, é o pilar mais importante do direito à proteção de dados e deu fundamento a uma série de instrumentos de proteção desse direito antes mesmo da entrada em vigor da LGPD.

O Marco Civil da Internet - Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, também aborda a privacidade dos usuários e trata da coleta e tratamento de dados na rede[4], demonstrando a sua precursão no reconhecimento da proteção de dados pessoais como um direito autônomo.

Já a Lei do Cadastro Positivo - Lei nº 12.414/2011 regula a formação e consulta a bancos de dados com informações de adimplemento, com regras específicas para garantir a privacidade dos dados dos consumidores[5].

A Lei de Acesso à Informação - Lei nº 12.527/2011 regula o direito dos cidadãos de receberem acesso a informações do seu interesse particular dos órgãos públicos, incluindo o acesso aos seus dados pessoais[6].

O Código de Defesa do Consumidor também possui disposições relacionadas à proteção dos dados pessoais, como os artigos 43 e seguintes, que tratam acerca do direito de acesso do consumidor aos bancos de dados dos fornecedores em que sejam processadas informações pessoais suas[7].

---

[4] Idem.

[5] BRASIL. Lei nº 12.414, de 9 de junho de 2011. Dispõe sobre a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União, Brasília, DF, 10 jun. 2011. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/06/2011&jornal=1&pagina=2&totalArquivos=204>. Acesso em: out. 2023.

[6] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/11/2011&jornal=1000&pagina=1&totalArquivos=12>. Acesso em: out. 2023.

[7] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em:

É importante mencionar ainda o *Habeas Data*, previsto no artigo 5º, inciso LXXII, da Constituição, que é o remédio constitucional destinado a assegurar o conhecimento, retificação e exclusão de informações relativas à pessoa, constantes em registros ou bancos de dados de entidades governamentais ou de caráter público[8].

O direito à proteção de dados também encontra fundamento no direito de imagem, de inviolabilidade da intimidade e da honra, todos previstos no art. 5º, X, da Constituição Federal[9].

Com a entrada em vigor da Lei nº 13.709/2018[10], a Lei Geral de Proteção de Dados, o marco mais importante para a proteção de dados pessoais no Brasil, o tratamento de dados pessoais finalmente recebeu unidade sistêmica, uma vez que foram estabelecidos os princípios fundamentais para o tratamento de dados, os direitos do titular de dados, a criação e atribuições da Autoridade Nacional de Proteção de Dados - ANPD, as responsabilidades e sanções aplicáveis pelo tratamento inadequado, bem como outras importantes diretrizes sobre o tratamento de dados no país e no exterior.

Chama a atenção como países que começam a se dedicar à proteção dos dados pessoais seguem uma trajetória semelhante. Inicialmente, é necessário vencer a batalha crucial do reconhecimento da proteção de dados como um direito autônomo. A mudança de mentalidade se encontra em compreender que o tratamento de dados pessoais representa, por si só, independentemente de ofensas à privacidade ou outros direitos, um risco para o indivíduo[11].

Posteriormente, é imperativo reconhecer que o verdadeiro detentor desses dados é o titular, independentemente de quem esteja realizando o tratamento. O fenômeno do tratamento de dados massivo e globalizado criou no imaginário social a equivocada concepção de que o "dono" dos dados é quem os detém e não os indivíduos a quem eles se referem.

Nesse sentido, vale mencionar os tipos de modelos de proteção aos dados pessoais identificados por Adolfo di Majo, que serão tratados mais adiante, o qual identificou que,

---

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=12/09/1990&jornal=1&pagina=1&totalArquivos=144>. Acesso em: 10 out. 2023.

[8] BRASIL. Constituição da República Federativa do Brasil de 1988. Art. 5º, inciso LXXII. Promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 out. 2023.

[9] Ibidem, art. 5º, X.

[10] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014.. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 out. 2023.

[11] BIONI, Bruno. Tratado de Proteção de Dados Pessoais . Rio de Janeiro: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 8 dez. 2023.

dentre outras possibilidades, os direitos de proteção de dados podem ser protegidos como um direito de personalidade ou como um direito de propriedade. Quando compreendidos sob a perspectiva de um direito de propriedade, as informações pessoais tornam-se direitos disponíveis, mas sob a perspectiva de que os dados pessoais representam uma extensão da personalidade dos seus titulares são tratados como direitos fundamentais e, portanto, indisponíveis[12].

Os dados pessoais, no mundo digitalizado, representam um forte reflexo da própria personalidade dos seus titulares, uma vez que podem fornecer informações acerca de suas preferências, inclinações e até mesmo estado de saúde ou genético, de modo que permitir o uso indiscriminado destes por terceiros pode representar uma violação do livre desenvolvimento da personalidade, da dignidade humana, da honra, dentre outros direitos de natureza íntima[13]. A respeito dos riscos decorrentes do tratamento inadequado de dados pessoais, Danilo Doneda afirma:

> A esta problemática "clássica" da privacidade podemos acrescentar atualmente um outro elemento: o fato de sermos, perante diversas instâncias, representados - e julgados - através destes dados. Tal fato abre uma outra possibilidade de enfocar a questão, pela qual a privacidade faz ressoar uma série de outras questões referentes à nossa personalidade. Isso por significar a perda de uma parte da nossa autonomia, de nossa individualidade e, por fim, de nossa liberdade. Nossos dados, estruturados de forma a significarem para determinado sujeito uma nossa representação virtual - ou um avatar -, podem ser examinados no julgamento de uma concessão de uma linha de crédito, de um plano de saúde, a obtenção de um emprego, a passagem livre pela alfândega de um país, além de tantas outras hipóteses[14].

Desse modo, atribuir-lhes a condição de direito fundamental emerge como uma etapa essencial desse percurso, uma vez que reconhece a importância que os dados pessoais têm no cotidiano dos indivíduos no mundo digitalizado e os riscos decorrentes do tratamento inadequado desses dados.

---

[12] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2020, p. 287.

[13] BORRILLO, Barbara. La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR. Dirittifondamentali.it, p. 326.

[14]DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. 1. ed. Rio de Janeiro: Renovar, 2006. p. 2.

Nesse sentido, as Ações Diretas de Inconstitucionalidade - ADIs nº 6.387, 6.388, 6.389, 6.390 e 6.393 tiveram uma atuação fundamental no reconhecimento pelo Supremo Tribunal Federal - STF de um direito fundamental à proteção de dados pessoais[15].

Mais recentemente o direito à proteção de dados pessoais foi reconhecido como um direito fundamental e inserido no art. 5º, inciso LXXIX, da Constituição Federal, bem como foi incluído no rol de competências privativas para legislar da União (art. 22, XXX, CF), ambos por intermédio da Emenda Constitucional 115 de 2022, o que reforçou o empenho empreendido nos últimos anos para que o tema amadureça e obtenha a atenção devida.

Desse modo, conclui-se que o Brasil tem avançado em direção a um sistema de proteção de dados robusto e alinhado aos padrões globais, assegurando que os direitos dos titulares sejam efetivamente protegidos e permitindo a delineação de um sistema de responsabilidade civil extracontratual capaz de efetivamente reparar os titulares e coibir condutas danosas pelos agentes de tratamento.

## 1.2 Evolução da Proteção de Dados na Europa

O sistema europeu de proteção de dados possui uma normativa própria para a regulação do tratamento de dados pessoais desde 1995, por intermédio da Diretiva 95/46/CE do Parlamento Europeu[16]. Além do mais, a Lei sobre proteção de dados pessoais mais antiga identificável foi promulgada em 1970 e advém da Alemanha[17], demonstrando que a Europa vinha apresentando preocupação com o tema antes que o mundo começasse a considerá-lo um fenômeno juridicamente relevante.

Mais recentemente, em 25 de maio de 2018, entrou em vigor o Regulamento Geral de Proteção de Dados - GDPR, a legislação da União Europeia destinada a fortalecer e unificar a proteção de dados nos países da Europa. Um regulamento foi escolhido como forma jurídica para o GPPR devido à sua força normativa direta e possibilidade de aplicação uniforme em todos os estados membros da União Europeia, considerando que a antiga

---

[15] BIONI, Bruno. Tratado de Proteção de Dados Pessoais . Rio de Janeiro: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 8 dez. 2023.

[16] UNIÃO EUROPEIA. Parlamento Europeu. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia, L 281, p. 31-50, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046. Acesso em: 15 jul. 2024.

[17] BIONI, Bruno. Tratado de Proteção de Dados Pessoais . Rio de Janeiro: Grupo GEN, 2020. E-book. ISBN 9788530992200, p. 22. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: dez. 2023.

Diretiva não era autoaplicável, dependendo da regulamentação do tema pelos países-membros[18].

Ademais, fazia-se imperativa uma resposta ágil aos desafios tecnológicos emergentes, que, como é característico da economia digital, não se sujeitam aos limites territoriais das nações e levantam desafios envolvendo privacidade, segurança cibernética, discriminações no âmbito digital e proteção de dados pessoais.

Desse modo, a entrada em vigor do GDPR marcou o início de um novo tempo para a proteção de dados pessoais na União Europeia, com o fortalecimento dos direitos dos titulares de dados, restrições à transferência internacional de dados e a responsabilização e dever de prestação de contas dos agentes de tratamento, com a possibilidade de aplicação de sanções e penalidades por não conformidade ao regulamento[19].

É importante destacar que o início da vigência do GDPR não tornou inócua ou desnecessária a elaboração de legislações sobre proteção de dados pelos países-membros, uma vez que as legislações internas exercem a importante função de abranger questões legislativas de natureza prática ou lacunas intencionalmente deixadas pelo GDPR[20]. Nesse sentido, o art. 84 do Regulamento estabelece que compete aos Estados-Membros estabelecerem as regras relativas à aplicação das sanções em caso de violação à proteção de dados pessoais previstas no Regulamento e determina que essas sanções devem ser efetivas, proporcionais e dissuasivas, isto é, com força para coibir as condutas desejadas[21].

A entrada em vigor do GDPR também trouxe uma série de mudanças para as empresas no âmbito da União Europeia, que tiveram que revisar suas práticas de tratamento de dados para assegurar a conformidade com os novos requisitos legais trazidos pelo Regulamento. Desse modo, a vigência do GDPR incentivou o desenvolvimento de uma cultura de proteção de dados mais consciente, não somente na Europa, mas também globalmente, tendo em vista que empresas de fora da União Europeia, que tratam dados de cidadãos europeus, também precisaram começar a se adequar às normas.

---

[18] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados. 2. ed. revista e atualizada [Recurso eletrônico]. São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia LTDA, 2020, p. 190. Disponível em: N/A. Acesso em: set. 2023.

[19] GDPR. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://gdpr.eu/tag/gdpr/>. Acesso em: 15 out. 2023.

[20] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados. 2. ed. revista e atualizada [Recurso eletrônico]. São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia LTDA, 2020, p. 190. Disponível em: N/A. Acesso em: set. 2023.

[21] GDPR. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Art. 84. Disponível em: <https://gdpr.eu/tag/gdpr/>. Acesso em: 15 out. 2023.

Além disso, o GDPR introduziu o conceito de "privacy by design" que exige que a proteção de dados seja considerada desde o início do desenvolvimento de novos produtos e serviços, visando assegurar que os dados pessoais sejam protegidos de forma eficaz ao longo de todo o ciclo de vida do tratamento. Este conceito está contido no art. 25 do GDPR que estabelece que os controladores devem implementar medidas apropriadas para efetivar os princípios de proteção de dados desde a fase inicial do desenvolvimento de produtos e serviços[22]. No mesmo sentido, o Considerando 78 do GDPR dispõe:

> (78) A defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, **os princípios da proteção de dados desde a conceção** e da proteção de dados por defeito[23].

A criação da Autoridade Europeia para a Proteção de Dados e do Comitê Europeu para a Proteção de Dados fortaleceu ainda mais o sistema de proteção de dados na Europa, proporcionando uma aplicação mais uniforme das normas de proteção de dados em toda a União Europeia. Esses órgãos desempenham um papel crucial na resolução de disputas, na emissão de orientações e na promoção da cooperação entre as autoridades nacionais de proteção de dados.

Por fim, a evolução da proteção de dados na Europa reflete o desenvolvimento de um compromisso com a proteção dos direitos fundamentais à privacidade e à proteção de dados pessoais, adaptando-se constantemente às mudanças tecnológicas e sociais para garantir que esses direitos sejam efetivamente resguardados no ambiente digital.

## 1.3 Os princípios na LGPD e no GDPR: Diretrizes éticas para o tratamento de dados

### 1.3.1 Os princípios norteadores da proteção de dados na LGPD

Os sistemas brasileiro e europeu de proteção de dados compartilham algumas semelhanças no que diz respeito aos princípios aplicáveis tanto à proteção de dados genericamente quanto à responsabilidade civil em proteção de dados. Destacar essas semelhanças e diferenças é importante para compreender a função das normas contidas em

[22] Ibidem, art. 25, 1.
[23] Ibidem, Considerando 78.

cada ordenamento e delimitar o alcance e as características da responsabilidade civil pelo tratamento inadequado de dados pessoais.

Os princípios são importantes porque conferem unidade sistêmica a uma determinada matéria, bem como colaboram para a interpretação das normas, aplicação aos casos concretos e resolução de desafios práticos[24]. Segundo Robert Alexy, os "princípios são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes". Para o autor, os princípios exercem a importante missão de não apenas suprir as lacunas deixadas pela lei, mas de solucionar conflitos entre regras dentro de um ordenamento jurídico[25].

A adequada regulação da proteção de dados pessoais no país dependia da estruturação de um sistema de regras e princípios coerentes, que não apenas descrevesse uma lista de proibições e sanções para o tratamento inadequado de dados, mas que trouxesse unidade sistêmica e segurança jurídica para o tema no país.

A proteção de dados pessoais no Brasil é regida pelos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, prestação de contas e responsabilização - que garante a efetiva reparação dos titulares pelo tratamento inadequado de dados, bem como a penalização dos agentes causadores de tais danos.

Além desses princípios expressamente previstos, descritos no art. 6º da LGPD[26], estabelece alguns fundamentos e princípios implícitos sobre os quais a proteção de dados pessoais no Brasil é regido, como o princípio da autodeterminação informativa, do respeito à privacidade, consentimento esclarecido, etc.

Os fundamentos da disciplina de proteção de dados pessoais, previstos no art. 2º da LGPD, são: o respeito à privacidade; à autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[27].

---

[24] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados . Revista de Direito do Consumidor. vol. 120. ano 27. p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018. p. 474

[25] ALEXY, Robert. Teoria dos Direitos Fundamentais. 5. ed. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2015. ISBN 978-85-392-0073-3. p. 90.

[26] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Art. 6º. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l137. Acesso em: 23 dez. 2023.

[27] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 2º. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 dez. 2024.

O princípio do respeito à privacidade, previsto na Constituição Federal, apesar de intimamente atrelado ao direito à proteção de dados pessoais, dele se difere, como será posteriormente estudado. O princípio da autodeterminação informativa, tendo em vista a sua relevância e a mudança de perspectiva que representa para o tratamento de dados pessoais no Brasil, também será tratado em um subitem específico posterior.

Os princípios da liberdade de expressão, informação, comunicação e opinião estão previstos no art. 5º, incisos IV, IX e XIV, da Constituição Federal, e asseguram a liberdade de manifestação do pensamento, da expressão da atividade intelectual[28] etc., e, no contexto da proteção de dados, garante que o tratamento inadequado desses dados não ponha em risco a violação de tais direitos.

Ademais, o art. 5º, inciso X, da Constituição Federal, trata da inviolabilidade da intimidade, vida privada, honra e imagem, assegurando indenização pelo dano material ou moral decorrente de sua violação, incluindo os abusos relacionados ao uso de dados pessoais.

Já o princípio do desenvolvimento econômico e tecnológico e a inovação reconhece que a proteção de dados pessoais não deve impedir o progresso tecnológico e econômico, mas sim coexistir com ele de maneira equilibrada, atuando como um contraponto aos direitos individuais previstos na Lei.

Os princípios da livre iniciativa, livre concorrência e defesa do consumidor asseguram que a proteção de dados pessoais não prejudique a livre iniciativa e a concorrência, ao mesmo tempo em que protege os direitos dos consumidores no mercado digital.

Os últimos princípios fundamentais da disciplina de proteção de dados são dos direitos humanos, do livre desenvolvimento da personalidade, da dignidade e exercício da cidadania, que enfatizam a importância dos dados pessoais na definição da identidade e dignidade dos indivíduos, assegurando que a proteção de dados pessoais é um componente essencial dos direitos humanos.

O princípio da finalidade está descrito no art. 6º, inciso I, da Lei nº 13.709/2018[29] e garante que o tratamento seja realizado com propósitos legítimos e específicos e que esta

---

[28] BRASIL. Constituição da República Federativa do Brasil de 1988. Promulgada em 5 de outubro de 1988. Art. 5º, incisos IV, IX e XIV. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 15 out. 2023.

[29] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Art. 6º, inciso I. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 15 out. 2023.

finalidade seja devidamente informada ao titular de dados e está intimamente relacionado aos princípios da adequação, necessidade e transparência[30].

Segundo Danilo Doneda, o princípio da finalidade cria uma vinculação entre o objetivo para o qual o dado foi coletado e o consentimento do titular com a efetiva utilização desses dados[31]. Desse modo, o controlador que coleta os dados pessoais de um titular com o fim de realizar seu cadastro para a elaboração de um contrato, por exemplo, não pode utilizar essas informações para propagandas de marketing ou outra finalidade que não tenha sido previamente informada ou consentida pelo titular.

Observa-se do texto do inciso I do art. 6º da LGPD que a finalidade do tratamento não pode ser genérica ou indeterminada, antes, deve ser específica, explícita e informada ao titular[32]. Nesse sentido, é importante lembrar que o consentimento do titular para o tratamento de dados deve ocorrer de forma clara e inequívoca, sendo o dever do agente de tratamento demonstrar que o titular compreende todas as razões e extensão do tratamento de dados pessoais a ser realizado a partir da coleta dos dados pessoais.

O princípio da finalidade ressalta a ideia de que os dados pessoais são "propriedade" do seu titular e, ainda que seja autorizado o seu tratamento, deve haver o seu consentimento e o seu controle sobre a utilização e destinação dessas informações, resguardado inclusive o seu direito de revogação do consentimento previamente dado. O princípio da finalidade também pode ser observado sob a ótica da proteção da atividade de tratamento pelos agentes de tratamento, isto é, uma vez existente o fato específico autorizador do tratamento e/ou o consentimento do titular, surge ao agente não apenas o dever proteger os dados pessoais, mas também o direito de tratá-lo, na medida da finalidade para a qual os dados foram coletados e de acordo com os limites estabelecidos na lei.

Por fim, o princípio da finalidade também pode ser compreendido a partir da ideia de que as ações humanas devem ter um propósito ou objetivo, o que é de grande valor para o campo da responsabilidade civil, pois permite uma análise objetiva da intenção do agente de tratamento quando da coleta dos dados pessoais e vincula todas as suas ações posteriores a este fim.

---

[30] LIMA, Cíntia Rosa Pereira de. Comentários à Lei Geral de Proteção de Dados. Portugal: Grupo Almedina, 2020. E-book. ISBN 9788584935796, p. 128. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 1 dez. 2023.

[31] DONEDA, Danilo; VIOLA, Mario. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. Revista Brasileira de Regulação e Estudos de Telecomunicações (RBR), 10ª Edição, págs 85-102, 2010. Disponível em: <https://www.rbrs.com.br/edicoes.php>. Acesso em: dez. 2023.

[32] LIMA, Cíntia Rosa Pereira de. Comentários à Lei Geral de Proteção de Dados. São Paulo: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796, p. 129. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: dez. 2023.

Outro princípio elencado no art. 6º, no inciso II, da LGPD é o da adequação, segundo o qual deve haver "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". O princípio da adequação, como se percebe da leitura do texto, não apenas está relacionado ao princípio da finalidade como decorre diretamente dele. Trata-se, segundo Cíntia Rosa Pereira de Lima, de uma face mais objetiva do princípio da finalidade. Isso porque a Lei estabelece o dever de que o agente de tratamento não apenas se limite às finalidades para as quais os dados foram coletados, mas que informe ao titular quais são essas finalidades[33].

A adequação, portanto, diz respeito ao direito/dever do titular/agente de tratamento de informação acerca da finalidade do tratamento. Trata-se da garantia de que o tratamento será adequado à finalidade informada ao titular.

O princípio da necessidade, insculpido no inciso III do art. 6º da LGPD, está intimamente relacionado aos anteriormente elencados, e diz respeito à "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

Segundo Bioni, Rielli E Kitayama, o princípio da necessidade, juntamente com os princípios da finalidade e adequação, determina quando o legítimo interesse pode ser aplicado[34]. Isso porque, o art. 10, §1º, da LGPD, determina que: "Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados". É interessante notar como os princípios elencados para o tratamento de dados pessoais na LGPD exerce aqui uma função prática e não meramente teórica ou interpretativa das normas. Os autores acima elencados explicam a dinâmica de aplicação do princípio da necessidade no caso concreto nos seguintes termos:

> É importante ressaltar que o adjetivo "necessário" não se confunde com "indispensável", mas também não é sinônimo de "útil" ou "desejável". Dessa forma, a maneira mais fácil de se identificar a necessidade, para fins de aplicação do legítimo interesse, é questionar se existe outra forma de atingir a finalidade ou interesse identificado. Tal teste pode chegar a algumas respostas: se não houver outra forma de atingir a finalidade ou se a outra

[33] LIMA, Cíntia Rosa Pereira de. Comentários à Lei Geral de Proteção de Dados. Coimbra: Grupo Almedina, 2020. E-book. ISBN 9788584935796, p. 131 Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: dez. 2023.
[34] BIONI, Bruno Ricardo (Org.). Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021, p. 225.

> forma exigir esforço desproporcional, então o tratamento pode ser considerado necessário[35].

Desse modo, compreende-se que o princípio da necessidade busca limitar as atividades de tratamento aos métodos menos invasivos possíveis aos direitos dos titulares, o que não diz respeito apenas "à quantidade de dados coletados e tratados, mas ao impacto que o tratamento tem sobre os direitos e liberdades fundamentais do titular de dados." [36]

O princípio do livre acesso garante ao titular a "consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais"[37]. Este direito é consolidado no art. 18 da LGPD, que estabelece o direito do titular de obter do controlador informações claras e detalhadas sobre o tratamento dos seus dados pessoais, como a confirmação da existência de tratamento, o acesso aos seus dados no banco de dados do agente de tratamento, assim como a correção dos dados incompletos, inexatos ou desatualizados[38].

É importante notar a possibilidade de aplicação direta dos princípios do art. 6º, incluindo o princípio do livre acesso, uma vez que estão consolidados e respaldados na existência de normas específicas garantidoras dos direitos elencados e, portanto, são capazes de ensejar a responsabilidade dos agentes de tratamento.

Nesse sentido, a simples negativa do controlador em fornecer ao titular de dados acesso às suas informações pessoais constantes em seu banco de dados é suficiente para que este incorra em responsabilidade civil pela violação à legislação de proteção de dados pessoais e é obrigado a repará-lo, conforme preconiza o art. 42 da LGPD.

O princípio da qualidade dos dados dá aos titulares a garantia de exatidão, clareza, relevância e atualização dos seus dados, em conformidade com a necessidade dos dados coletados para cumprir a finalidade do tratamento.

Pode-se afirmar que o princípio da qualidade dos dados pessoais é a face do princípio da finalidade que se preocupa com a qualidades dos dados tratados para um determinado fim e não simplesmente com o objetivo do tratamento[39]. Ele se difere também do princípio da

---

[35] Ibidem, p. 226.
[36] BIONI, Bruno Ricardo (Org.). Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021, p. 227.
[37] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.in.gov.br/web/dou/-/lei-n-13-709-de-14-de-agosto-de-2018-36889940>. Acesso em: jan. 2024.
[38] Idem.
[39] DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 171.

necessidade, uma vez que a sua preocupação não é com a limitação dos dados, mas com a sua qualidade, isto é, com a exatidão e a clareza com que esses dados são tratados.

O princípio da qualidade dos dados é especialmente relevante quando o tratamento de dados realizado fornece informações qualificadas a respeito do titular, de modo que a inexatidão ou desatualização dos seus dados possa influenciar em decisões automatizadas ou baseadas em estatísticas, por exemplo.

A observância rigorosa da qualidade dos dados é crucial em situações específicas, como o tratamento destinado à análise/proteção de crédito, visto que a existência de dados inexatos ou desatualizados acerca do titular nesses casos têm o impacto de fornecer informações errôneas acerca do seu perfil de consumo ou de adimplência, gerando impactos negativos tanto sobre o perfil de credor (*score*) dos titulares - com a consequente restrição de acesso a bens e oportunidades - quanto sobre as políticas econômicas de crédito das instituições financeiras[40].

Isso porque, em sentido contrário à GDPR, em que a proteção ao crédito encontra sua base legal no legítimo interesse, o art. 7º, inciso X, da LGPD elenca a proteção ao crédito como base legal para o tratamento de dados, o que exclui a necessidade de consentimento do titular ou de demonstração do legítimo interesse pelo controlador para o tratamento de dados com essa finalidade[41].

O princípio da transparência, por sua vez, fornece aos titulares a garantia de "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento"[42].

Trata-se, segundo Laura Schertel Mendes, de sinônimo do princípio da publicidade, segundo o qual há a proibição da existência de banco de dados sigilosos e funciona como "condição essencial da *accountability* dos bancos de dados"[43].

A legislação brasileira, no entanto, não trouxe a publicidade do banco de dados como um princípio intrínseco ao princípio da transparência no tratamento, tendo atribuído à Autoridade Nacional de Proteção de Dados - ANPD o dever de dispor acerca da necessidade

---

[40] MARANHÃO, J. S. de A.; CAMPOS, R. R. Proteção De Dados De Crédito Na Lei Geral De Proteção De Dados. Direito Público, [S. l.], v. 16, n. 90, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3739. Acesso em: 2 jan. 2024.

[41] Ibidem, p. 147.

[42] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.in.gov.br/web/dou/-/lei-n-13-709-de-14-de-agosto-de-2018-36889940>. Acesso em: 2 jan. 2024.

[43] MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental, 1ª Edição. ISBN 9788502218987. Disponível em: https://integrada.minhabiblioteca.com .br/#/books/9788502218987/. Acesso em: 20 dez. 2023.E-book.. São Paulo: Editora Saraiva, 2014, p. 71.

de publicização do tratamento nos casos necessários[44], o que leva à compreensão de que não há obrigatoriedade de publicização e, portanto, não se trata de um princípio aplicável à atividade de tratamento de dados em geral.

O princípio da transparência, portanto, diz respeito ao direito do titular de obter informações claras acerca do tratamento dos dados pessoais, informações estas a serem fornecidas pelo agente de tratamento[45]. Não deve, por sua vez, ser confundido com o princípio do livre acesso, pois este dá ênfase ao direito do titular de acessar informações sobre seus dados, enquanto aquele enfatiza a responsabilidade do controlador em fornecer essas informações de maneira transparente e proativa.

O sétimo princípio elencado no art. 6º da LGPD é o da segurança, que diz que deve ser garantida a utilização de medidas técnicas e administrativas capazes de "proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"[46].

O princípio da segurança diz respeito a uma série de medidas a serem tomadas pelos agentes de tratamentos que garantem que o tratamento de dados pessoais seja realizado da forma mais segura possível, de modo a evitar situações acidentais ou incidentais que gerem prejuízo aos direitos garantidos por lei aos titulares de dados[47].

O art. 49 da LGPD dá um exemplo claro de efetivação do princípio da segurança ao determinar que "Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares".

Alguns casos de incidentes de segurança que poderiam ter sido evitados à luz da correta aplicação das normas sobre segurança de dados trazidos pela LGPD foram reportados no Brasil nos últimos anos, como o vazamento de dados da empresa Netshoes em 2017, que expôs dados de cadastro do e-commerce de mais de 2 milhões de clientes[48].

---

[44] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.in.gov.br/web/dou/-/lei-n-13-709-de-14-de-agosto-de-2018-36889940>. Acesso em: 2 jan. 2024.

[45] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.in.gov.br/web/dou/-/lei-n-13-709-de-14-de-agosto-de-2018-36889940>. Acesso em: jan. 2024.

[46] Idem.

[47] SIQUEIRA, D. P.; SANTOS DE MORAES, F. S. de M.; PLAZA TENA , L. Do reconhecimento da autodeterminação informativa como direito da personalidade e do princípio da segurança. Revista Direito em Debate, [S. l.], v. 31, n. 57, p. 4, 2022. DOI: 10.21527/2176-6622.2022.57.12476. Disponível em: https://revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/12476. Acesso em: dez. 2023.

[48] MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS (MPDFT). MPDFT e Netshoes firmam acordo para pagamento de danos morais coletivos após vazamento de dados. 2019. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-m

A empresa realizou um Termo de Ajustamento de Conduta - TAC, no âmbito do Inquérito Civil Pùblico de nº 08190.044813/18-44, para o pagamento de compensação os danos morais coletivos resultantes do incidente de segurança, bem como se comprometeu a:

> Cláusula 3ª - A empresa Netshoes (Ns2.Com Internet S.A.) compromete-se a: 1) implantar medidas adicionais ao seu Programa de Proteção de Dados, quais sejam: gerenciamento de riscos e vulnerabilidades no portal Netshoes; ações de adequação à Lei Geral de Proteção dos Dados Pessoais; e atualização contínua de sua Política de Segurança Cibernética; 2) realizar esforços de orientação de consumidores, a aumentar o nível de conhecimento sobre os riscos cibernéticos e medidas de proteção de seus dados pessoais, por meio de campanha de conscientização; e 3) disseminar ao mercado as melhores práticas para privacidade e proteção de dados pessoais, por meio da participação em fóruns e eventos especializados; e difusão de boas práticas de proteção dos dados[49].

O TAC firmado pela Netshoes ressalta alguns dos deveres de segurança e prevenção trazidos pela LGPD, como a adoção e atualização das suas políticas de boas práticas em relação à proteção de dados, transparência em relação aos consumidores titulares de dados e adoção de medidas técnicas de segurança.

De forma semelhante ao princípio da segurança, o princípio da prevenção busca proteger os dados pessoais de incidentes de segurança, no entanto, busca fazê-lo de modo preventivo, incidindo sobre o agente de tratamento o dever de adotar medidas prévias para evitar eventos geradores de danos em decorrência do tratamento (Art. 6º, VIII, da LGPD), como a elaboração de um relatório de impacto, definido na lei como:

> Art. 5º, VII. [...] documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A proteção de dados pessoais no Brasil também é regida pelo princípio da não discriminação, que proíbe o tratamento de dados com fins discriminatórios ilícitos ou abusivos (Art. 6º, IX, da LGPD), que garante o tratamento de dados de forma equitativa e protege o titular contra ofensas a diversos direitos fundamentais.

---

pdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados. Acesso em: dezembro de 2024.

[49] Termo de Ajustamento de Conduta - TAC n. 01/2019 - ESPEC, Inquérito Civil Público n º 08190.044813/18-44. Disponível em: https://www.mpdft.mp.br/portal/pdf/tacs/espec/TAC_Espec_2019_001.pdf.

Esse princípio possui especial relevância no contexto das decisões automatizadas. Nesse sentido, o artigo 20 da LGPD garante o direito à revisão de decisões tomadas unicamente com base em processamento automatizado.

O último princípio apontado no art. 6º da LGPD, o princípio da responsabilização e prestação de contas, reúne em si o dever de demonstração, pelo agente, da adoção de medidas que demonstrem a sua adequação a todos os princípios anteriores, bem como a eficácia dessas medidas.

### 1.3.2 Os princípios norteadores da proteção de dados no GDPR

Embora a legislação brasileira tenha sido inspirada na europeia, o GDPR listou alguns princípios que não fazem parte do escopo de princípios elencados na LGPD, como os princípios da licitude, lealdade, exatidão e limitação da conservação. Os demais princípios não serão abordados uma vez que possuem conteúdos muito semelhantes aos já anteriormente elencados.

O conceito de licitude expresso no GDPR é semelhante ao que convencionamos chamar de bases legais para o tratamento de dados no Brasil. O artigo 6º, 1, do Regulamento traz uma lista taxativa de situações em que, se não observadas ao menos uma delas, o tratamento de dados não será considerado lícito:

> 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
>
> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
>
> b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
>
> c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
> d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
> e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
> f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O princípio da licitude, portanto, se baseia na ideia de que o tratamento somente pode ocorrer quando encontrar correspondência em alguma das hipóteses legalmente previstas no GDPR, isto é, é preciso identificar motivos específicos para o tratamento[50]. Nesse sentido, o princípio da licitude, embora mais abrangente, se assemelha ao princípio da finalidade previsto na LGPD, uma vez que estabelece que o tratamento de dados pessoais deve ocorrer para propósitos específicos, isto é, deve estar amparado por bases legais específicas e determinadas na Lei.

É importante notar que, se antes a proibição ou a restrição ao tratamento era a exceção, agora é a regra. A ideia por trás do princípio da licitude é que dados pessoais em regra não podem ser tratados, exceto se cumprida ao menos uma das hipóteses trazidas no artigo 6º, 1, do Regulamento. O fato de o GDPR ter previsto as bases legais para o tratamento como um pressuposto do princípio da licitude demonstra isso com clareza. Isso porque, no GDPR, a licitude é um princípio norteador de toda a atividade de tratamento, enquanto na LGPD as bases legais são apresentadas como condições específicas nas quais o tratamento de dados é permitido. A mudança de enfoque representa uma abordagem mais restritiva em relação ao tratamento de dados pessoais.

Há uma diferença substancial no modo com que a LGPD e o GDPR optaram por abordar o tema. Como anteriormente mencionado, a LGPD optou por não inserir o princípio da licitude ou legalidade no seu rol de princípios, antes, preferiu trazer um artigo com as bases legais que justificam o tratamento de dados, quais sejam:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

[50] SPIECKER GENANNT DÖHMANN, I. A Proteção de Dados Pessoais sob o Regulamento de Proteção de Dados da União Europeia. Direito Público, [S. l.], v. 17, n. 93, 2020. DOI: 10.11117/rdp.v17i93.4235., p. 20. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4235. Acesso em: dez. 2023.

> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Muito embora seja difícil identificar as suas consequências práticas, essa escolha principiológica destaca o valor que o princípio da legalidade ou licitude possui em cada um dos sistemas. Ao optar por inserir a licitude no rol de princípios do GDPR, o legislador o definiu como um dos fundamentos da atividade de tratamento de dados.

É importante notar ainda que o rol de bases legais para o tratamento trazido pela LGPD é maior e mais amplo do que as hipóteses de tratamento legal apontadas no GDPR. Dentre as hipóteses apontadas na LGPD e não existentes no GDPR se encontra a do tratamento de dados para fins de proteção do crédito (art. 7º, inciso X).

Um rol mais amplo de hipóteses de tratamento representa, por um lado, mais possibilidades de utilização dos dados pessoais, o que naturalmente expõe os dados a mais riscos, mas, por outro, regula melhor o tratamento, de modo a garantir que as hipóteses de tratamento estejam devidamente delineadas na lei.

O princípio da lealdade está relacionado à criação de uma relação de confiança entre o titular de dados pessoais e o agente de tratamento[51], significa que os responsáveis pelo tratamento de dados possuem o dever de ir além das obrigações legais a eles impostas quando os interesses dos titulares assim exigirem[52]. Este princípio evidencia a opção pela integração de valores éticos pela GDPR, refletindo a preocupação do legislador em estabelecer um “ecossistema" de proteção de dados auto sustentável, fundamentado em seus próprios princípios e regras[53].

Além do mais, segundo o princípio da lealdade toda a atividade de tratamento deve ser documentada de forma transparente e não pode ter efeitos negativos imprevistos ao titular de

---

[51] UNIÃO EUROPEIA; CONSELHO DA EUROPA. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo: Serviço das Publicações da União Europeia, 2014. ISBN 978-92-871-9939-3 (Conselho da Europa). ISBN 978-92-9239-498-1 (FRA). doi:10.2811/73790, p. 78.
[52] Ibidem, p. 80.
[53] HIJMAN, Hielke; RAAB, Charles. Ethical Dimensions of the GDPR, AI Regulation, and Beyond. RDP, Brasília, Volume 18, n. 100, p. 63-90, out./dez. 2021, p. 65. DOI: https://doi.org/10.11117/rdp.v18i100.6197.

dados pessoais[54]. Neste aspecto, o princípio da lealdade assemelha-se ao princípio da transparência previsto na LGPD.

O princípio da exatidão também possui correspondência na legislação brasileira, pois diz respeito ao direito do titular de dados de "correção de dados incompletos, inexatos ou desatualizados" (art. 18, III, LGPD).

O princípio da exatidão possui duas faces: por um lado, assegura o direito do titular dos dados de manter suas informações sempre atualizadas; por outro lado, protege a necessidade social de zelar pela constante atualização dos bancos de dados, seja para fins de políticas de crédito mais justas, pesquisas na área da saúde ou para a realização de políticas públicas mais precisas[55].

É importante ressaltar que a responsabilidade de garantir a precisão dos dados deve ser compreendida considerando o propósito do processamento desses dados, isto é, de acordo com o princípio da finalidade[56]. Desse modo, não basta que os dados sejam corretos e atualizados, é necessário que esta correção se mantenha fiel aos interesses do titular de dados e à finalidade do tratamento. Nesse sentido:

> [...] Uma empresa de comercialização de mobiliário recolheu dados sobre a identidade e a morada de um cliente para fins de faturação. Seis meses depois, esta empresa pretende lançar uma campanha de marketing e deseja contactar antigos clientes. Para tal, a empresa pretende ter acesso ao registo de residentes nacionais, que conterá provavelmente moradas atualizadas, dado que os residentes estão obrigados por lei a comunicar a sua atual morada ao registo. Apenas têm acesso aos dados deste registo as pessoas e entidades que apresentem uma justificação válida para tal. Nesta situação, a empresa não pode utilizar o argumento de que está obrigada a manter a exatidão e atualidade dos dados para fundamentar o seu direito a consultar o registo de residentes a fim de recolher novos dados sobre a morada de todos os seus antigos clientes. Os dados foram recolhidos para fins de faturação; neste caso, é relevante a morada à data da venda. Não existe qualquer base legal para recolher novos dados sobre a morada, uma vez que o marketing não é um interesse que prevaleça sobre o direito à proteção de dados e, como tal, não pode justificar o acesso aos dados constantes do registo[57].

---

[54] UNIÃO EUROPEIA; CONSELHO DA EUROPA. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo: Serviço das Publicações da União Europeia, 2014. ISBN 978-92-871-9939-3 (Conselho da Europa). ISBN 978-92-9239-498-1 (FRA). doi:10.2811/73790, p. 80.

[55] HIJMAN, Hielke; RAAB, Charles. Ethical Dimensions of the GDPR, AI Regulation, and Beyond. RDP, Brasília, Volume 18, n. 100, p. 63-90, out./dez. 2021, p. 74. DOI: https://doi.org/10.11117/rdp.v18i100.6197.

[56] UNIÃO EUROPEIA; CONSELHO DA EUROPA. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo: Serviço das Publicações da União Europeia, 2014. ISBN 978-92-871-9939-3 (Conselho da Europa). ISBN 978-92-9239-498-1 (FRA). doi:10.2811/73790, p. 76.

[57] Idem.

Por fim, segundo o princípio da limitação da conservação, descrito no art. 5º, 1, e, do GDPR, os dados pessoais devem ser "Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados".

O GDPR ainda estabelece o dever de o responsável pelo tratamento informar ao titular dos dados o prazo de conservação dos dados ou, se não for possível, ao menos quais foram os critérios utilizados para definir esse prazo[58].

É importante notar que o art. 5º, XI, da LGPD, trouxe um conceito parecido, ao afirmar que considera-se anonimização, para os fins da Lei, a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

A LGPD, no entanto, não traz a anonimização como um princípio basilar do tratamento de dados pessoais. O art. 16, IV, da LGPD, autoriza a conservação dos dados após o término do tratamento para finalidades específicas, dentre as quais se encontra o tratamento para uso exclusivo do controlador e desde que anonimizados. Além disso, o art. 40 da Lei atribuiu à ANPD o poder de dispor sobre o tempo de guarda de registros de dados pessoais.

Em suma, percebe-se que, apesar da clara inspiração na legislação europeia, há algumas diferenças na escolha dos princípios importados para a legislação brasileira, escolhas estas que revelam o modo com o que a LGPD optou por delinear o sistema brasileiro de proteção de dados, revelando quais são as suas prioridades em relação ao tratamento de dados no Brasil.

### 1.3.3 O princípio da autodeterminação informativa

A autodeterminação informativa é um conceito relevante em ambas as legislações e que merece aprofundamento. Tanto a LGPD quanto o GDPR são fortemente influenciadas pela ideia de que o titular de dados pessoais tem o direito de deter o controle sobre como os seus dados são tratados.

Merece aprofundamento, no entanto, a compreensão acerca da natureza e do conceito de autodeterminação informativa, tendo em vista que na LGPD ela não está mencionada no rol de princípios que norteiam a proteção de dados. Na LGPD, a autodeterminação

[58] GDPR. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://gdpr.eu/tag/gdpr/>. Acesso em: 13 out. 2023.

informativa foi mencionada como um dos fundamentos da disciplina de proteção de dados pessoais, o que significa que este conceito é fundamental para a compreensão e aplicação das normas de proteção de dados no Brasil.

Conforme observado por Laura Trenado, a autodeterminação informativa é um direito de construção jurisprudencial[59]. O surgimento do reconhecimento do conceito como um direito legal remonta ao caso *Volkszählungsurteil*, julgado na Alemanha em 1983, também conhecido como "Caso do Censo"[60].

O caso deliberou sobre um projeto do governo alemão de realizar uma pesquisa nacional que exigiria a coleta de uma enorme quantidade de dados pessoais dos cidadãos. A iniciativa rapidamente levantou uma série de questionamentos e preocupações com a possibilidade de uso abusivo das informações e invasão de privacidade dos indivíduos[61].

Na decisão, o Tribunal Constitucional Alemão afirma que o tratamento de dados pessoais pelo governo deve ser ponderado com os direitos fundamentais dos cidadãos, introduzindo no ordenamento jurídico o conceito de autodeterminação informativa ao defender que os titulares possuem o direito de escolha sobre quem e como seus dados pessoais serão tratados[62].

No âmbito da jurisprudência da União Europeia o direito à autodeterminação afirmativa remete ao caso Google Spain, S.L. e Google Inc. *versus* a Agência Espanhola de Proteção de Dados em que o Tribunal de Justiça da União Europeia, após o remetimento de questões prejudiciais pelo Tribunal Espanhol, reconheceu pela primeira vez a existência do direito ao esquecimento[63].

O conceito de direito ao esquecimento está profundamente atrelado ao de autodeterminação informativa, tendo em vista que o reconhecimento de que o indivíduo possua o direito de desatrelar de sistemas de busca, por exemplo, informações pessoais suas

---

[59] CABALLERO TRENADO, Laura. Cartografía legal de la autodeterminación informativa digital: un derecho de construcción jurisprudencial. Universitas, 2021, n. 35, p. 2-27. ISSN 1698-7950. DOI: https://doi.org/10.20318/universitas.2021.6189. Acesso em: 28 jun. 2024.

[60] CUNHA, Anita Spies da; SCHIOCCHET, Taysa. A constitucionalidade do DNA na persecução penal: o direito à autodeterminação informativa e o critério de proporcionalidade no Brasil e na Alemanha. The constitutionality of DNA in criminal prosecution: the right to informative self-determination and the proportionality criterion in Brazil and Germany. Revista de Investigação Constitucional, Curitiba, v. 8, n. 2, p. 529-554, maio/ago. 2021. DOI: https://revistas.ufpr.br/rinc/article/view/74420. Acesso em: 27 jun. 2024.

[61] ALEMANHA. Tribunal Constitucional Federal. Volkszählungsurteil - BVerfGE 65, 1. 15 de dezembro de 1983. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 28 jun. 2024.

[62] Idem.

[63] CABALLERO TRENADO, Laura. Cartografía legal de la autodeterminación informativa digital: un derecho de construcción jurisprudencial. Universitas, 2021, n. 35, p. 2-27. ISSN 1698-7950. DOI: https://doi.org/10.20318/universitas.2021.6189. Acesso em: 28 jun. 2024.

decorre do reconhecimento de que o titular de dados possui o direito de tomar decisões acerca do tratamento dos seus dados pessoais.

Apesar de relacionados, o direito ao esquecimento e a autodeterminação informativa possuem alcances e significados distintos, valendo ressaltar que o STF não reconheceu a existência ao direito ao esquecimento no ordenamento jurídico brasileiro, em ocasião do julgamento do RE nº 1.010.606, Tema 786[64], apesar de serem amplamente reconhecidos e defendidos os direitos à privacidade e à autodeterminação informativa.

O caso Google Spain, S.L. e Google Inc. *versus* Agência Espanhola de Proteção de Dados (*Agencia Española de Protección de Datos - AEPD*) tratava inicialmente dos pedidos de um cidadão espanhol que encontrou informações desatualizadas e prejudiciais sobre ele em uma busca no Google. Essas informações diziam respeito a um leilão de propriedade devido a dívidas sociais, publicado em um jornal em 1998. Mario Costeja González pediu ao Google e ao jornal que removessem ou alterassem as páginas para que seus dados pessoais não aparecessem mais nos resultados de busca[65].

A decisão trouxe uma série de esclarecimentos importantes, dentre eles, o de que os operadores de busca na internet (como o Google) são responsáveis pelo tratamento de dados pessoais que aparecem em páginas web publicadas por terceiros e consequentemente que estes motores de busca podem ser obrigados a remover *links* para informações pessoais de seus resultados[66], reconhecendo assim a existência do direito ao esquecimento e à autodeterminação informativa.

Segundo Epping, citado por Cunha e Schiocchet, a autodeterminação informativa está diretamente relacionada às liberdades e ao livre desenvolvimento da personalidade do indivíduo[67], *in verbis*:

> É por conta disso que o direito à autodeterminação informativa decorre do direito geral de personalidade, que, por sua vez, é um desdobramento da dignidade humana. Ora, o indivíduo intimidado, que não sabe quais informações o Estado detém sobre si, irá evitar certas atitudes, o que

---

[64] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº 1.010.606, Relator: Min. Alexandre de Moraes. Brasília, DF. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15346473757&ext=.pdf>. Acesso em: 14 jul. 2024.

[65] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf. Acesso em: 27 jun. 2024.

[66] Idem.

[67] CUNHA, Anita Spies da; SCHIOCCHET, Taysa. A constitucionalidade do DNA na persecução penal: o direito à autodeterminação informativa e o critério de proporcionalidade no Brasil e na Alemanha. The constitutionality of DNA in criminal prosecution: the right to informative self-determination and the proportionality criterion in Brazil and Germany. Revista de Investigação Constitucional, Curitiba, v. 8, n. 2, p. 529-554, maio/ago. 2021. DOI: https://revistas.ufpr.br/rinc/article/view/74420. Acesso em: 27 jun. 2024.

> implicará diretamente no livre desenvolvimento e a livre expressão de sua personalidade, parte essencial da dignidade humana[68].

A autodeterminação informativa do indivíduo se reflete tanto na percepção deste sobre si mesmo quanto no modo que ele enxerga a percepção da sociedade sobre ele, e, como será posteriormente abordado, o livre desenvolvimento da personalidade humana está profundamente atrelado a essas duas faces de percepção de um indivíduo sobre si. Na mesma medida em que o direito à privacidade é importante para a preservação desse aspecto interno do livre desenvolvimento da personalidade humana a autodeterminação informativa exerce um papel fundamental no aspecto externo.

Como menciona a decisão no "Caso do Censo" anteriormente abordado, se as pessoas sentirem que estão sob vigilância do governo ao participar de uma manifestação ou atividade da sociedade civil, elas podem acabar sendo desencorajadas de exercer seus direitos fundamentais de associação e manifestação, por exemplo, o que demonstra a importância da autodeterminação para a manutenção de uma sociedade democrática livre[69].

Naturalmente, o reconhecimento da autodeterminação informativa deve ser ponderado com outros direitos e princípios, sobretudo os de ordem pública. Nesse sentido, Cunha e Schiocchet afirmam que para a análise da proporcionalidade na aplicação do direito à autodeterminação informativa devem ser ponderadas, além do tipo de informação, as possibilidades de utilização e a utilidade dos dados[70]. Nesse sentido:

> O direito à autodeterminação informativa, assim como os demais direitos fundamentais, não tem um cerne previamente definido, razão pela qual a violação ao núcleo essencial também deverá ser analisada considerando as características e peculiaridades do direito em conflito e do caso concreto. Ademais, para verificação do núcleo deste direito, não basta considerar o dado em si, mas também o seu tratamento e os possíveis usos. De todo modo, considera-se abstratamente que há uma violação ao núcleo essencial do direito à autodeterminação informativa quando se retira completamente do sujeito o seu espaço privado necessário para desenvolver sua personalidade livremente[71].

---

[68] Idem.

[69] ALEMANHA. Tribunal Constitucional Federal. Volkszählungsurteil - BVerfGE 65, 1. 15 de dezembro de 1983. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 27 jun. 2024.

[70] CUNHA, Anita Spies da; SCHIOCCHET, Taysa. A constitucionalidade do DNA na persecução penal: o direito à autodeterminação informativa e o critério de proporcionalidade no Brasil e na Alemanha. The constitutionality of DNA in criminal prosecution: the right to informative self-determination and the proportionality criterion in Brazil and Germany. Revista de Investigação Constitucional, Curitiba, v. 8, n. 2, p. 529-554, maio/ago. 2021. DOI: https://revistas.ufpr.br/rinc/article/view/74420. Acesso em: 27 jun. 2024.

[71] Idem.

Desse modo, nota-se que a análise da proporcionalidade e a proteção ao direito à autodeterminação informativa requerem uma avaliação detalhada e contextualizada de cada caso. É fundamental considerar não apenas o tipo de informação, mas também o modo pelo qual esses dados podem ser utilizados e sua utilidade para fins específicos.

Como mencionado, a autodeterminação informativa se encontra refletida em uma série de princípios e direitos estabelecidos na Lei. O princípio da transparência, previsto no art. 6º, inciso VI, da LGPD[72], permite que os indivíduos saibam quem está processando seus dados, para que fins e como esses dados serão utilizados, capacitando-os a tomarem decisões informadas.

O direito de retificação e de exclusão dos dados, previstos no art. 18, incisos III e IV, da LGPD[73], garante aos titulares o poder de retificar dados incompletos, inexatos ou desatualizados ou de anonimizar, bloquear ou eliminar dados desnecessários, excessivos ou tratados em desconformidade com a Lei, fortalecendo o seu poder de decisão sobre o modo com que seus dados são mantidos no banco de dados dos agentes de tratamento. A LGPD ainda concede ao titular o direito de consentir e revogar seu consentimento para o tratamento dos seus dados pessoais a qualquer momento e quantas vezes o titular desejar[74].

Em suma, embora a LGPD não tenha previsto autodeterminação informativa como princípio (mas sim como um fundamento), efetivamente define o conceito por meio de inúmeros direitos e princípios que visam garantir o controle dos titulares sobre seus dados pessoais.

Por fim, a análise comparativa entre os princípios elencados no GDPR e na LGPD demonstra que ambos os sistemas compartilham a ideia central de estabelecer princípios éticos para a proteção dos direitos dos titulares, princípios estes que desempenham um papel fundamental no desenvolvimento de sistemas jurídicos coerentes de proteção de dados.

---

[72] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 27 jun. 2024.
[73] Idem.
[74] Idem.

# 2 A RESPONSABILIDADE CIVIL NOS SISTEMAS BRASILEIRO E EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS

O tema da responsabilidade civil, tanto nos sistema brasileiro quanto europeu de proteção de dados pessoais, está intrinsecamente ligado ao direito à privacidade. Embora, na atualidade, o direito à privacidade dos titulares não abranja completamente o escopo da proteção de dados pessoais, é notório que a privacidade desempenhou um papel importante como um dos principais fundamentos na estruturação do direito à proteção de dados.

Em ambos os ordenamentos, o direito à privacidade teve forte influência do direito americano, que exportou para o mundo a ideia de *privacy* como um direito legal e ético, notabilizada com a publicação do artigo *The Right to Privacy*, por Samuel D. Warren e Louis D. Brandeis na *Harvard Law Review* em 1890 [75].

O direito à privacidade diz respeito à reivindicação do indivíduo de não ser objeto de observação por parte de terceiros, evitando a exposição de seus assuntos, informações pessoais e características particulares ao escrutínio de terceiros, do público em geral ou do Poder Público[76].

O reconhecimento da privacidade como um direito traz como consequência lógica implicações no campo da responsabilidade civil. Nesse sentido, no caso *Pavesich versus New England Life Ins. Co*., frequentemente apontado como um dos primeiros casos nos Estados Unidos a reconhecer o direito à privacidade, foi reconhecido pela Suprema Corte do Estado da Geórgia que o uso pela empresa *New England Life Insurance Company* da imagem da autora em seus anúncios publicitários sem a sua permissão configurou violação a seu direito de privacidade[77]. Consequentemente, a empresa foi proibida de continuar a utilizar a imagem de *Pavesish* sem consentimento. Além disso, a decisão judicial no caso estabeleceu um precedente importante no direito norte-americano, demonstrando a importância de se proteger a privacidade dos indivíduos contra usos comerciais não autorizados de suas imagens.

---

[75] COLOMBO, C.; BERNI, D. L. M. Privacy no direito italiano: tríade de decisões judiciais rumo a insights sobre limites conceituais, deslocamento geográfico e transparência do corpo eletrônico . Revista IBERC, Belo Horizonte, v. 5, n. 1, p. 112–131, 2022. DOI: 10.37963/iberc.v5i1.205. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/205. Acesso em: 15 fev. 2024.

[76] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 4. ed. rev. e atual. São Paulo: Saraiva, 2009. 590 p. ISBN 978-85-02-07819-2, p. 465.

[77] ZANINI, L. E. de A. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. Revista Brasileira de Direito Civil, [S. l.], v. 3, n. 01, 2017. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/107. Acesso em: fev. 2024, p. 14.

Desde então a ideia de *privacy* como um direito evoluiu gradualmente para os ordenamentos jurídicos de todo o mundo, principalmente os de *common law.* No Brasil, o direito à privacidade foi mencionado expressamente na Constituição Federal de 1988, ao afirmar que "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (art. 5º, inciso X, CF)"[78], bem como nas disposições sobre a inviolabilidade do sigilo da correspondência e das comunicações telegráficas (art. 5º, inciso XII, CF)[79].

No contexto europeu, uma importante decisão envolvendo a ideia de privacidade como um direito foi o caso *Von Hannover versus Germany,* julgado pelo Tribunal Europeu dos Direitos Humanos. Neste caso, a princesa Caroline de Mônaco processou a República Federal da Alemanha por permitir a publicação de fotos suas em atividades da vida privada sem sua permissão.

O Tribunal decidiu que a Alemanha não havia protegido suficientemente o direito à privacidade da princesa, conforme garantido pelo Artigo 8 da Convenção Europeia dos Direitos Humanos. Este caso estabeleceu um precedente importante ao equilibrar a liberdade de imprensa com o direito à privacidade, afirmando que figuras públicas também têm direito à proteção de sua vida privada quando não estão em atividades públicas[80].

Na Itália, a doutrina aponta que a partir do ano de 1950 os tribunais passaram a reconhecer a existência de um *diritto alla riservatezza,* sobretudo a partir do caso envolvendo Clara Petacci, uma italiana de família nobre que teve um relacionamento amoroso com o ditador Benito Mussolini e teve seu caso relatado em uma novela[81]. A sentença que julgou o pedido da família de retirada de circulação da novela, reconheceu a ofensa ao *diritto alla riservatezza* ainda que sem ofensa direta à honra ou à reputação[82].

É importante mencionar que o fenômeno do *big data* modificou substancialmente tanto a essência quanto o destinatário do direito à privacidade, em comparação ao inicialmente concebido por Samuel D. Warren e Louis D. Brandeis. Isso porque, até a década de 60, conforme observado por Danilo Doneda, o direito à privacidade estava predominantemente associado a figuras públicas de destaque. No entanto, com a

---

[78] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Art. 5º, inciso X. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 fev. 2024.
[79] Ibidem, art. 5º, inciso XII.
[80] EUROPEAN COURT OF HUMAN RIGHTS. Case of Von Hannover v. Germany. Application no. 59320/00, Judgment of 24 June 2004. Disponível em: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Von%20Hannover%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}. Acesso em: 03 jul. 2024.
[81] CORTE D'APPELLO DI MILANO. Sezione I. Sentença de 21 jan. 1995. Rivista di Diritto Civile, p. 170.
[82] Idem.

popularização da internet e o aumento da cultura de exposição da vida privada digitalmente, o direito à privacidade expandiu significativamente seu alcance e a proteção de dados pessoais conquistou uma posição de destaque no escopo de abrangência do conceito de privacidade[83].

Desse modo, não poucas vezes os termos "proteção de dados pessoais" e "privacidade" são tidos como sinônimos ou mencionados em contextos semelhantes. Essa confusão semântica-conceitual, no entanto, merece atenção e aprofundamento, sob o risco de esvaziamento do conceito de direito à proteção de dados pessoais, que enfrentou tantos desafios para conquistar autonomia e relevância no ordenamento jurídico brasileiro.

A grande mudança de paradigma trazida pela LGPD ao ordenamento jurídico não foi simplesmente a possibilidade de responsabilização dos agentes de tratamento em casos de violação à privacidade ou aos dados pessoais dos titulares - muitos destes já abarcados em alguma medida pelas legislações anteriores à LGPD, mas o reconhecimento da proteção de dados pessoais como um direito autônomo.

O tratamento inadequado de dados, nesse sentido, é amparado pelo direito não mais porque outros direitos de personalidade, como a privacidade, foram violados, mas porque a lei passou a considerar os dados pessoais em si um bem jurídico relevante o suficiente para receber tutela jurídica própria (fato jurídico), além de dar protagonismo ao titular sobre as decisões a respeito dos seus dados pessoais.

A tutela jurídica da proteção de dados pessoais traz consigo a necessidade de um regime de responsabilidade capaz de coibir e reparar as condutas danosas dos agentes de tratamento. Nota-se que se dá cada vez menos ênfase às definições de privacidade como "direito de ser deixado em paz", em favor de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito (princípio da autodeterminação informativa)[84].

Antes de adentrar a discussão do regime de responsabilidade civil adotado pela LGPD, é importante mencionar que a responsabilidade civil representa apenas um dos modelos de tutela da proteção dos dados pessoais, pois como identificado pelo jurista Adolfo Di Majo as

---

[83] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados. 2. ed. revista e atualizada [Recurso eletrônico]. São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia LTDA, 2020, p. 33. Disponível em: https://www.amazon.com.br/privacidade-prote%C3%A7%C3%A3o-dados-pessoais-elementos-ebook/dp/B089QV2MZ9. Acesso em: fev. 2024.

[84] RODOTÀ, Stefeano. Tecnologie e Diritti (Capítulo 1) [eBook]. Editora Il Mulino. Disponível em: vbk://YPrZGkvqzGQ9IvvWK88v7QpG61rGm0eThywySx24dUs. Acesso em 12 jun. 2024.

modalidades de tutela para os dados pessoais podem ser: “a tutela proprietária, a tutela dos direitos da pessoa, a tutela aquiliana e a tutela das leis de proteção de molde germânico”[85].

Sob a perspectiva da tutela proprietária, os dados são compreendidos como propriedade do titular, cabendo a ele, inclusive, o direito de acessar, modificar, excluir e transferir esses dados, enfatizando o controle que o indivíduo tem sobre suas informações pessoais de modo semelhante ao controle que se tem sobre a propriedade física[86]. Como bem observado por Danilo Doneda, “Nessa abordagem está presente a discussão sobre a natureza dos dados pessoais – se devem ser considerados bens jurídicos de livre disposição pelos seus titulares ou não".

A tutela dos direitos da pessoa está relacionada à proteção dos dados pessoais como uma extensão dos direitos fundamentais, dignidade humana e um direito de personalidade, uma vez que reconhece que os dados pessoais estão intrinsecamente ligados à identidade e à privacidade do indivíduo, e sua proteção é essencial para garantir outros direitos humanos, como a honra, a imagem e a vida privada[87].

Por fim, a tutela aquiliana refere-se à proteção baseada na responsabilidade civil por danos causados pelo tratamento inadequado de dados pessoais. Esta abordagem se baseia na responsabilidade extracontratual, em que qualquer dano causado pela violação das normas de proteção de dados pode levar à obrigação de reparação por parte do responsável pelo tratamento dos dados.  Danilo Doneda afirma, a respeito desse modelo:

> Outra crítica recai sobre sua possibilidade meramente relativa e, por vezes, especulativa de incentivar o estabelecimento de um padrão de comportamento, justamente em uma área na qual o recurso à responsabilidade civil não é um caminho encorajador em grande parte dos casos. Um papel auxiliar da responsabilidade civil, no entanto, pode se integrar na disciplina de proteção de dados, principalmente se vier acompanhada da definição de casos específicos de responsabilidade objetiva – vide que a imensa dificuldade na demonstração do dano é um dos maiores problemas enfrentados pela consolidação da tutela da proteção de dados. Assim, uma disciplina de responsabilidade objetiva específica para o setor de tratamento de dados pessoais pode ser um instrumento tanto para a satisfação de interesses lesados como para fomentar uma determinada cultura no tratamento desses dados[88].

---

[85] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2020, p. 287.
[86] Idem.
[87] Idem.
[88] Ibidem, p. 289.

Nesse sentido, é importante ressaltar que os modelos de tutela não são necessariamente excludentes entre si, uma vez que um mesmo ordenamento jurídico pode adotar diferentes modelos de tutela para a proteção dos dados pessoais.

No Brasil, a LGPD introduziu uma mudança significativa na forma como os dados pessoais são compreendidos e tratados. Historicamente, dados pessoais eram frequentemente vistos sob a ótica do direito de propriedade, onde o controle sobre os dados poderia ser comparado à posse de um bem material. Esse entendimento, contudo, limita a proteção dos dados ao contexto patrimonial e econômico, negligenciando aspectos fundamentais da dignidade e autonomia individual. A LGPD, ao ser promulgada, trouxe uma nova perspectiva, alinhando-se ao GDPR e passando a reconhecer os dados pessoais não apenas como um ativo econômico, mas como uma extensão da personalidade e dignidade humana, como um direito de personalidade.

A responsabilidade civil trata  do dever de reparar o dano causado a outra pessoa ou ao seu patrimônio em decorrência de uma conduta que viola uma norma jurídica. Em outras palavras, é a obrigação de compensar o prejuízo causado a alguém em virtude de uma ação ou omissão que cause danos, seja por negligência, imprudência, ou intencionalmente. O dano causado precisa ser necessariamente a um bem jurídico, enquanto a conduta do agente pode ser legal ou ilegal. Acerca deste conceito, aplicado às relações de tratamento de dados pessoais, afirma Stefano Rodotà:

> Não que esse último aspecto estivesse ausente das definições tradicionais: mas, nelas, ele servia para sublinhar e exaltar a componente individualista, apresentando-se como um mero instrumento para realizar o objetivo de ser deixado em paz; enquanto hoje chama especialmente a atenção para a possibilidade de indivíduos e grupos controlarem o exercício dos poderes fundados na disponibilidade de informações, contribuindo assim para o estabelecimento de equilíbrios sociopolíticos mais adequados[89].

O regime de responsabilidade civil extracontratual estabelecido pela LGPD está baseado principalmente nos artigos 42 e seguintes da Lei, mas outras normas do ordenamento jurídico, como as disposições do Código Civil e do Código de Defesa do Consumidor complementam e subsidiam o regime previsto na LGPD.  Segundo o artigo 42 da LGPD:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

[89] RODOTÀ, Stefano. Tecnologie e Diritti (Capítulo 1) [eBook]. Editora Il Mulino. Disponível em: vbk://YPrZGkvqzGQ9IvvWK88v7QpG61rGm0eThywySx24dUs. Acesso em 12 jun. 2024.

O artigo 43 da mesma Lei complementa dispondo que:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

As disposições trazidas sobre a responsabilização dos agentes de tratamento logo levantaram questionamentos acerca do tipo de responsabilidade adotado pela LGPD, tendo em vista que, embora a descrição do texto legal seja semelhante ao adotado pelo CDC, a LGPD não menciona a expressão "independentemente da existência de culpa" presente no CDC.

Segundo a Lei de Introdução às Normas do Direito Brasileiro[90], "A lei nova, que estabeleça disposições gerais ou especiais a par das já existentes, não revoga nem modifica a lei anterior". Nesse sentido, o Código Civil estabeleceu o regime de responsabilidade civil subjetiva como regra geral, ressalvando os casos especificados em lei ou quando a atividade desenvolvida pelo agente trouxer riscos, casos em que a responsabilidade será objetiva. *In verbis*:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos **casos especificados em lei**, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, **por sua natureza**, **risco** para os direitos de outrem.

Pela interpretação do art. 927 e parágrafo único a análise da responsabilidade civil no presente caso pode ser compreendida da seguinte forma. A regra de responsabilidade civil no ordenamento jurídico brasileiro é a da responsabilidade subjetiva. A responsabilidade não será subjetiva, isto é, será objetiva: (i) nos casos especificados em lei, e, aqui cabe uma interpretação literal, no sentido de que a lei dirá expressamente quando a responsabilidade for objetiva ou (ii) quando se tratar de atividade de risco.

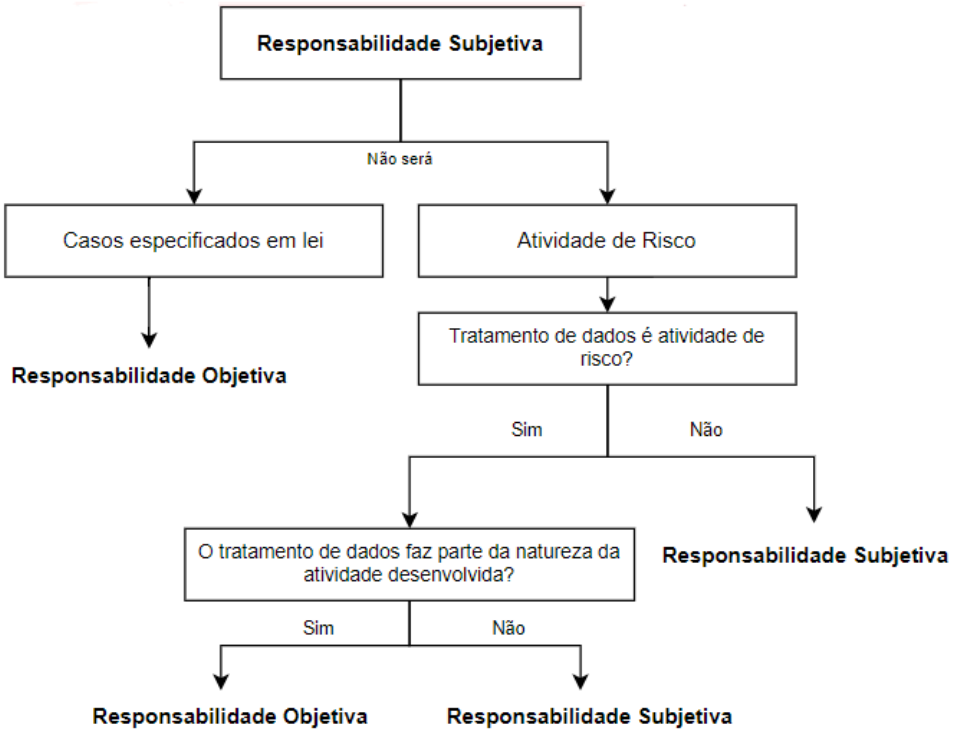
Tendo em vista que a LGPD não afirma com clareza que o regime de responsabilidade aplicável às atividades de tratamento de dados é de natureza objetiva, não é possível a

[90] BRASIL. Lei n. 4.657, de 4 de setembro de 1942. Lei de Introdução às Normas do Direito Brasileiro. Art. 2º, §2º. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4657.htm. Acesso em: 29 fev. 2024.

aplicação do artigo supra pelo primeiro critério, presente na expressão "nos casos especificados em lei".

Desse modo, parte da doutrina tem voltado seus esforços a demonstrar que a atividade de tratamento de dados é atividade de risco. Contudo, além de identificar se a atividade de tratamento é atividade de risco, é preciso verificar se a atividade de tratamento faz parte da natureza da atividade comumente desenvolvida pelo autor do dano, conforme demonstrado diagrama a seguir:

**Diagrama 1: Modelos de responsabilidade civil no ordenamento jurídico brasileiro**




Fonte: Elaborado pela autora.

Essa interpretação aparenta ser um tanto quanto improvável quando analisado o entendimento doutrinário tradicional acerca do risco e do que seria uma atividade que apresenta risco por sua natureza. O risco, para fins de responsabilização objetiva, precisa estar atrelado à natureza da atividade desenvolvida. Desse modo, o questionamento a ser respondido é não apenas se o tratamento de dados é uma atividade de risco, mas se o

tratamento de dados está intrinsecamente atrelado à atividade desenvolvida pelo agente de tratamento[91].

Para o desenvolvimento do raciocínio acerca da atividade de tratamento ser ou não uma atividade de risco por natureza, é importante rememorar o contexto de surgimento da teoria do risco. A teoria do risco surgiu como uma justificativa para a adoção do regime de responsabilidade objetiva.

Até então, a responsabilidade civil era pautada exclusivamente em critérios subjetivos, isto é, a partir da análise da culpa do sujeito causador do dano. Até os dias atuais a responsabilidade baseada na culpa representa, na maioria dos casos, a medida de direito mais justa, uma vez que possibilita a averiguação concreta da responsabilidade do agente causador do dano.

Contudo, com o crescimento das empresas decorrente da industrialização dos meios de produção, as relações de trabalho e de consumo foram se tornando cada vez mais complexas, tornando difícil a reparação de danos às vítimas com base em critério de culpa, considerando a assimetria de informações entre as grandes empresas e os consumidores/trabalhadores.

A inversão do ônus probatório, portanto, se dá principalmente pela superioridade de conhecimento técnico das empresas em relação à atividade desenvolvida. É natural esperar-se, por exemplo, que uma empresa atuante no ramo de seguros tenha conhecimento técnico aprofundado acerca da sua atividade em comparação com o consumidor.

No entanto, não parece razoável admitir que qualquer empresa que atue realizando tratamento de dados pessoais como atividade secundária possua o mesmo nível de conhecimento técnico acerca da atividade de tratamento realizada. Muitas dessas empresas, inclusive, terceirizam completamente a atividade de tratamento dos dados dos seus clientes, no entanto, pela legislação vigente, são responsáveis pelo tratamento inadequado que venha a ser realizado.

Outro questionamento a ser levantado é se o tratamento de dados é uma atividade de risco, tendo em vista a amplitude do termo “risco”. Em sentido genérico, dirigir pode ser considerado uma atividade de risco, criar filhos é uma atividade de risco e até mesmo

---

[91] SANTOS, Rômulo Marcel Souto dos; LEITÃO, André Studart; WOLKART, Erik Navarro. A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais e a regra de Hand. Civil responsibility in the General Personal Data Protection Law and the Hand Rule. Responsabilidad civil en la Ley General de Protección de Datos Personales y la regla de Hand. Revista de Direito, v. 20, n. 34, p. 60-84, 2022. Editora responsável: Profa. Dra. Fayga Bedê. Submetido em: 24 nov. 2021. Aprovado em: 21 dez. 2021. DOI: 10.12662/2447-6641oj.v20i34.p60-84.2022. Disponível em: https://orcid.org/0000-0001-6444-2631. Acesso em: jun. 2024.

atividades cotidianas, como cozinhar ou praticar esportes, podem ser consideradas atividade de risco.

No entanto, quando se fala em risco no contexto de responsabilidade objetiva, é necessário adotar uma interpretação mais restrita e técnica. O risco relevante é aquele que, pela natureza intrínseca da atividade, apresenta um potencial significativo de causar danos a terceiros, independentemente de culpa ou negligência por parte do agente.

Portanto, para afirmar que o tratamento de dados é uma atividade de risco, é preciso demonstrar que a própria essência dessa atividade envolve um perigo inerente e constante de causar prejuízos. Isso implica em considerar fatores como a sensibilidade dos dados tratados, a extensão e a gravidade dos possíveis danos decorrentes de um tratamento inadequado, e a capacidade técnica da empresa para gerenciar e mitigar esses riscos[92].

Nesse sentido, como será demonstrado no último capítulo, os Tribunais brasileiros têm entendido haver uma diferença valorativa entre os tipos de dados, sendo que nem todos os dados pessoais, levando-se em conta também o contexto em que são tratados, são aptos a gerar prejuízos ao titular. Sendo assim, seria incoerente pensar que toda e qualquer atividade de tratamento de dados é uma atividade de risco. Esse raciocínio não implica na conclusão de que nem todos os dados pessoais são importantes, apenas que, no sentido de risco aqui tratado é preciso analisar com cautela a sua existência.

Desse modo, a transferência das implicações da teoria do risco e da responsabilidade civil objetiva para o tratamento de dados, sem considerar as distinções significativas desse novo campo do direito, não parece se apresentar como a medida mais sensata de se compreender as implicações da responsabilidade civil no campo da proteção de dados.

Por essas e outras razões, segundo Bruno Bioni, a discussão binária acerca do regime de responsabilidade estabelecido na LGPD empobrece o debate, uma vez que "parte da falsa premissa de dualidade de regimes jurídicos de responsabilidade" (responsabilidade objetiva *versus* subjetiva)[93].

A visão de que o tratamento de dados é, por sua natureza, atividade de risco e que, portanto, está sujeito ao regime de responsabilidade objetiva, mediante interpretação das

---

[92] SANTOS, Rômulo Marcel Souto dos; LEITÃO, André Studart; WOLKART, Erik Navarro. A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais e a regra de Hand. Revista Opinião Jurídica, [S.l.], v. 20, n. 34, p. 60-84, mar. 2022. DOI: 10.12662/2447-6641oj.v20i34.p60-84. Disponível em: https://periodicos.unichristus.edu.br/index.php/opiniajuridica/article/view/7895. Acesso em: 17 jun. 2024.

[93] BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. civilistica.com, ano 9, n. 3, 2020, p. 2. Disponível em: https://civilistica.com. Acesso em: 29 jun. 2024.

disposições do Código Civil, também apresenta alguns problemas do ponto de vista interpretativo e fático.

Há um elemento substancial na interpretação da teoria do risco quando trata-se de dados pessoais. Isso porque, as técnicas de proteção de dados pessoais, devido à rápida evolução das tecnologias, podem rapidamente tornar-se inócuas. Nesse sentido, o inciso III do art. 44 da LGPD dispõe que as técnicas de tratamento de dados pessoais disponíveis à época do tratamento serão consideradas para fins de reconhecimento da irregularidade do tratamento.

Segundo a teoria do risco, "quem exerce determinadas atividades deve ser responsável também pelos seus riscos, independentemente do seu comportamento pessoal." Trata-se do resultado de um processo histórico de superação da necessidade de se comprovar a culpa do agente[94].

Um importante questionamento que se coloca diante desta situação é a razoabilidade de se esperar que os agentes de tratamento estejam sempre atualizados no que tange às técnicas de tratamento de dados mais seguras. Uma comparação extrema, mas válida para fins de compreensão do argumento, seria supor que hospitais ou clínicas médicas devessem sempre manter-se atualizados com os medicamentos mais recentes do mercado, desde que estes apresentem um nível maior de efetividade no tratamento dos pacientes.

Mesmo no caso anterior, em que o bem da vida resguardado é dos mais importantes, o direito à saúde, é comum que se faça uma análise da razoabilidade dos meios empregados para o tratamento, levando-se em consideração o valor de mercado das técnicas e medicamentos empregados.

O inciso III do art. 44 da LGPD, dispõe:

> O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: [...] III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado[95].

A leitura do referido dispositivo leva à interpretação mais imediata de que é dever do controlador manter-se atualizado em relação às técnicas de tratamento de dados pessoais mais recentes que proporcionem maior segurança à proteção destes dados. O dispositivo, no

---

[94] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. Fundamentos do direito civil: responsabilidade civil. 2. ed. Rio de Janeiro: Forense, 2021. p. 216.

[95] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 44, inciso III. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 jul. 2024.

entanto, não faz menção à aplicação de princípios como o da razoabilidade ou proporcionalidade para a análise da regularidade do tratamento.

Portanto, a aplicação da teoria do risco na esfera do tratamento de dados pessoais demanda uma reflexão sobre a viabilidade e a medida de justiça dessa abordagem. Embora seja imperativo que os agentes de tratamento estejam atualizados nas melhores práticas de segurança de dados, é igualmente necessário considerar a razoabilidade e a proporcionalidade dessas exigências, especialmente em um contexto em constante evolução tecnológica.

A responsabilidade civil em proteção de dados também apresenta características substancialmente relevantes no que diz respeito aos conceitos de conduta humana, nexo causal e dano. O conceito de dano, como tradicionalmente concebido, diz respeito a qualquer prejuízo ou lesão causada a uma pessoa, seus bens ou seus direitos. Trata-se de elemento essencial da responsabilidade civil.

Como bem observado por Anderson Schreiber, nem todo dano é, por direito, ressarcível. Segundo o autor, "o dano não consiste, em definitivo, na lesão a um interesse tutelado em abstrato, mas na lesão a um interesse concretamente merecedor de tutela"[96]. A título exemplificativo da afirmação anterior, o autor apresenta as seguintes situações hipotéticas:

> Tomem-se duas hipotéticas ações de indenização promovidas, com fundamento na responsabilidade objetiva, por pessoa que foi submetida a procedimento de revista. Na primeira ação, a revista foi praticada na saída de estabelecimento comercial, por suspeita de furto, e o tribunal, analisando o caso, entende configurado o dano moral (dano à intimidade), a cuja reparação condena o réu. Na segunda ação, a revista foi praticada em aeroporto com a finalidade de assegurar que o passageiro não ingressaria com nenhum objeto metálico no interior da aeronave. Aqui, o tribunal entende não ser devida a indenização. Parece claro que o nexo causal encontra-se presente em ambas as hipóteses: o comportamento do réu causa o alegado dano do autor. Nem se trata de discutir a culpa, em sede de responsabilidade objetiva. É o alegado dano que não se configura na segunda hipótese, pois, embora o interesse à intimidade seja abstratamente tutelado, não o é concretamente; cede, nas circunstâncias fáticas aludidas, ao interesse na segurança e integridade física dos demais passageiros. Vale dizer: não há dano reparável, dano injusto, ou, simplesmente, dano em sentido técnico para fins de responsabilização[97].

No contexto da LGPD, é frequentemente um desafio identificar os danos ressarcíveis causados aos titulares de dados pessoais. Isso porque os dados pessoais são bens imateriais e a

---

[96] SCHREIBER, Anderson. Novos paradigmas da responsabilidade civil: da erosão dos filtros à diluição dos danos, 2ª Ed.: São Paulo: Atlas, 2009, p. 189.
[97] Idem.

sua violação nos termos da Lei nem sempre gera lesões concretas de fácil ou imediata identificação.

Nesse sentido, o acórdão no processo C-300/21 do Tribunal de Justiça da União Europeia, trouxe à tona uma importante discussão, acerca de como implementar o art. 82 do GPDR, que estabelece regras para a aplicação de indenização em casos de tratamento irregular dos dados[98]. Segundo entendimento do Tribunal, ao não trazer uma diretriz clara de como avaliar o dano, aponta que os Estados-Membros possuem a discricionariedade de definir critérios normativos de como compensar na prática os danos causados pelo tratamento irregular de dados[99].

Guardadas as devidas proporções, percebe-se uma lógica contrária ao que normalmente ocorre no ordenamento jurídico brasileiro, onde, independentemente de como os tribunais inferiores estejam decidindo, esse tipo de questão costuma ser levada aos tribunais superiores para definição e uniformização da jurisprudência acerca do tema.

Outro elemento importante para a identificação da ocorrência do dano é a ilicitude ou a antijuridicidade da conduta. Não há que se falar em dano injusto e, portanto, ressarcível quando não verificada a ilicitude ou, ao menos, a antijuridicidade. A ilicitude refere-se à violação de uma norma jurídica específica, enquanto a antijuridicidade refere-se à contrariedade de uma conduta em relação ao ordenamento jurídico como um todo. A antijuridicidade é um conceito mais amplo, pois engloba não apenas a violação de normas específicas, mas também a incompatibilidade de uma conduta com os princípios e valores do sistema jurídico[100].

Mesmo no caso do dano extrapatrimonial, é possível a averiguação, a partir da experiência social de como os indivíduos geralmente reagem e sofrem com as situações, do possível dano psicológico sofrido. Isso é o que permite, por exemplo, o reconhecimento do dano *in re ipsa* em situações em que o prejuízo de ordem moral é presumido.

Além do mais, a conduta do agente é justificada no risco assumido pela atividade desenvolvida. Nas relações de consumo, a conduta do agente em prol de evitar o dano ao

---

[98] UNIÃO EUROPEIA. Tribunal de Justiça. Acórdão no Processo C-300/21, UI v. Österreichische Post AG. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=3020662. Acesso em: 27 jun. 2024.

[99] LI, Shu. Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. Maastricht Journal of European and Comparative Law, v. 30, n. 3, p. 335-345, 2023. Disponível em: https://doi.org/10.1177/1023263X231208835. Acesso em: 27 jun. 2024.

[100] DA SILVA, Rafael Peteffi. Antijuridicidade como requisito da responsabilidade civil extracontratual: amplitude conceitual e mecanismos de aferição. Revista de Direito Civil Contemporâneo, São Paulo, v. 18, p. 169-214, 2024. Disponível em: https://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/568f. Acesso em: 17 jul. 2024.

consumidor não é um critério relevante para fins de condenação do fornecedor em reparar os danos causados (exceto no caso extremo de culpa exclusiva do consumidor).

Neste ponto o CDC diferencia-se substancialmente da LGPD, uma vez que não há na primeira Lei normas que condicionem a responsabilidade do agente ao fato de estes não terem adotado medidas de natureza subjetiva para evitar o dano ao consumidor[101].

A LGPD, por sua vez, condicionou a responsabilidade do agente à não adoção de uma série de medidas para a proteção dos dados do titular, medidas estas "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."[102] Por serem bastante abrangentes, tais medidas tornam a análise da conduta do agente subjetiva, isto é, a responsabilidade será baseada na possibilidade deste de evitar o dano (responsabilidade subjetiva) e não na presunção de responsabilidade em razão do desenvolvimento de atividade de risco (responsabilidade objetiva). Nesse sentido, afirma José Emiliano Paes Landim Neto que:

> Mostra-se imprescindível, pois, na concepção da teoria subjetiva aventada, que os agentes de tratamento (conduta dolosa ou culposa) para serem responsabilizados civilmente – reparação de dano ao titular – devem violar as normas jurídicas impostas pela LGPD. Da análise, portanto, da responsabilidade civil subjetiva, o agente de tratamento, ao demonstrar que não agiu de forma dolosa ou culposa, que realizou o tratamento de forma segura, com as técnicas e modo de realização disponíveis à época do tratamento, poderá invocar sua excludente de responsabilidade – ausência do dever de indenizar –art. 43, II, da LGPD[103].

A escolha do legislador por não delinear de forma clara um regime de responsabilidade de natureza objetiva não representa um erro ou um simples esquecimento. Pelo contrário, trata-se de uma decisão deliberada que considerou a multiplicidade e a diversidade das atividades relacionadas ao tratamento de dados pessoais, assim como os impactos que o tipo de responsabilidade pode acabar tendo sobre a atividade econômica[104].

---

[101] BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. civilistica.com |a. 9. n. 3. 2020. p. 7.

[102] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 46. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 jun. 2024.

[103] LANDIM NETO, José Emiliano Paes. Responsabilidade Civil dos Agentes de Tratamento à Luz da Lei Geral de Proteção de Dados: Análise Jurisprudencial dos Tribunais Estaduais. 2022. 74 f. Dissertação (Mestrado Profissional em Direito Econômico e Desenvolvimento) - Instituto Brasileiro de Ensino, Pesquisa e Desenvolvimento (IDP), Brasília, DF, 2022.

[104] SANTOS, Rômulo Marcel Souto dos; LEITÃO, André Studart; WOLKART, Erik Navarro. A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais e a regra de Hand. Revista de Direito, v. 20,

Nesse sentido, é importante lembrar que o anteprojeto da LGPD adotava expressamente um regime de responsabilidade objetiva, inclusive mencionando que a atividade tratamento seria atividade de risco[105].

A LGPD também não condiciona a reparação apenas ao dano patrimonial ou moral, inserindo no rol de danos indenizáveis o dano individual e coletivo (art. 42, caput). Como anteriormente mencionado, uma das grandes mudanças de paradigma trazido pela LGPD foi o reconhecimento da proteção de dados como um bem suficientemente relevante para receber tutela jurídica própria.

Com isso, pode-se dizer que o bem jurídico tutelado são os dados pessoais em si e a autodeterminação do titular sobre estes. A consequência prática dessa mudança de entendimento é que os dados pessoais são protegidos não apenas quando há violação ao direito de privacidade, ao direito de imagem etc., de modo que o próprio tratamento irregular, sobretudo considerando que o titular possui o direito de participação ativa nas decisões sobre o tratamento, deve ser considerada uma conduta danosa. O dano é a própria exposição ao tratamento irregular. Segundo Laura Schertel Mendes,

> A violação do direito à proteção de dados pode gerar tanto dano patrimonial quanto dano moral. O dano patrimonial pode ocorrer, por exemplo, se o armazenamento de dados pessoais incorretos ensejar a contratação de um crédito mais caro pelo consumidor. Já o dano moral configura-se com a simples violação do direito à personalidade, isto é, comprovada a violação dos dados pessoais do consumidor, sem o seu consentimento ou base legal, cabe a reparação dos danos morais. Não é o elemento subjetivo - dor, vexame ou humilhação - que configura o dano moral, mas o elemento objetivo - interesse lesado[106].

No entanto, segundo o entendimento de que os dados pessoais são, em si, bens juridicamente tutelados, é preciso reconhecer um terceiro tipo de dano, decorrente da própria exposição dos dados pessoais ao tratamento irregular. Se a violação aos dados pessoais se condicionar tão somente ao dano patrimonial ou moral sofrido, como exemplificado na citação supramencionada, não há sentido na adoção de uma legislação específica para a proteção dos dados pessoais no que tange à responsabilidade civil. Isso porque, os danos

---

n. 34, p. 60-84, 2022. DOI: 10.12662/2447-6641oj.v20i34.p60-84.2022. Disponível em: https://orcid.org/0000-0001-6444-2631. Acesso em: jun. 2024.

[105] BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. civilistica.com, v. 9, n. 3, p. 5, 2020.

[106] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. 1ª ed. São Paulo: Saraiva Jur - Sob Demanda, 2013. 248 p. ISBN 978-8502218963.

patrimoniais e morais, inclusive os decorrentes da violação de dados, já eram devidamente abarcados pela legislação pátria.

O tratamento inadequado de dados pessoais por instituições financeiras que ocasionasse a exposição dos dados de um titular a fraudes financeiras, como a clonagem de cartões ou obtenção de um empréstimo por terceiro, por exemplo, já eram devidamente abrangidos pela lei.

Segundo a Súmula 479 do Superior Tribunal de Justiça "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". O entendimento sumulado supramencionado abarca qualquer tipo de dano sofrido, inclusive os danos decorrentes da exposição indevida dos dados do titular e o dano extrapatrimonial.

Outro dano frequentemente causado pelo tratamento irregular de dados diz respeito aos danos morais decorrentes da exposição de informações pessoais indevidamente, sobretudo aquelas consideradas sensíveis ou que afetem a honra do titular diante da sociedade, danos estes também já abarcados pelos direitos de personalidade.

Um terceiro tipo de dano possível é o dano decorrente da exposição dos dados pessoais em si, independentemente da ocorrência de danos patrimoniais ou morais. Este dano decorre do entendimento de que o titular possui autodeterminação sobre os seus próprios dados e a violação deste direito em si é um bem juridicamente tutelado. As consequências legais e práticas desse tipo de violação, no campo da responsabilidade civil extracontratual, não resultaram tão claras da redação da LGPD.

Essa lacuna na redação da LGPD em relação ao reconhecimento explícito do dano decorrente da mera exposição irregular dos dados pessoais reflete uma complexidade inerente à proteção de dados na era digital. Historicamente, o foco da responsabilidade civil foi nos danos patrimoniais ou morais, mais facilmente identificáveis e mensuráveis. No entanto, com a evolução tecnológica e o aumento das ameaças à privacidade e segurança dos dados, tornou-se evidente a necessidade de uma proteção mais abrangente, que considere o próprio ato de tratamento irregular como prejudicial.

Essa perspectiva reconhece não apenas os danos tangíveis, como fraudes financeiras ou constrangimentos sociais, mas também os danos imateriais decorrentes da perda de controle sobre os próprios dados. A LGPD, ao reconhecer o direito à autodeterminação informativa, estabelece uma base para esse entendimento mais abrangente do dano.

Nesse sentido, uma análise da doutrina europeia pode oferecer diferentes perspectivas e abordagens para lidar com os desafios emergentes no campo da proteção de dados,

especialmente em relação ao reconhecimento e reparação dos danos decorrentes da exposição irregular dos dados pessoais e à identificação de uma regime de responsabilidade que seja adequado à realidade da proteção de dados.

Ao explorar as contribuições da doutrina da União Europeia, é possível enriquecer o debate sobre responsabilidade civil nos sistemas brasileiro de proteção de dados pessoais, buscando soluções mais abrangentes e eficazes para os desafios da era digital.

A jurisprudência da União Europeia tem se deparado com a mesma dificuldade acima mencionada, em distinguir o dano do risco gerado aos dados pelo tratamento irregular, tendo em vista que o GPDR não definiu de modo claro o conceito de dano em proteção de dados e nem estabeleceu regras claras para a indenizar os danos imateriais decorrentes de violação do Regulamento. Nesse sentido, a jurisprudência tem se debruçado em analisar se o risco por si só pode ser reconhecido como um dano indenizável, in verbis:

> When applying the above conceptual framework to the context of data processing, the direct consequence of violating any GDPR violation is that the control of data subjects over their personal information becomes weaker. The loss of control, however, is in nature more of a risk rather than a kind of actual harm, let alone tort damage. It creates ‘a risk of future injury’, which is only a speculation of harm rather than actual harm.34 In order to successfully claim compensation, a data subject must further prove that the loss of control has caused material or non-material harm that posed actual disadvantage to them and further from a legal perspective, that harm is recoverable tort damage defined by law. Therefore, as the judgment confirmed and literature elaborated, a cumulative requirement for compensation is de facto established by Article 82 GDPR. Three cumulative conditions must be established for the sake of compensation: the existence of infringement of any provision of the GDPR, the existence of material or non-material damage and a causal link between infringement and damage.35 Regarding the nature of the loss of control, it is noted that the wording of Recital (85) GDPR is confusing.36 In this recital, loss of control is equivalent to damage. This equivalence is wrong and misleading[107] [108].

---

[107] LI, Shu. Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. Maastricht Journal of European and Comparative Law, v. 30, n. 3, p. 335-345, 2023. Disponível em: https://doi.org/10.1177/1023263X231208835.

[108] Tradução livre: Ao aplicar o quadro conceitual acima ao contexto do processamento de dados, a consequência direta de violar qualquer disposição do GDPR é que o controle dos titulares dos dados sobre suas informações pessoais torna-se mais fraco. A perda de controle, no entanto, é mais um risco do que um tipo de dano real, quanto mais dano por responsabilidade civil. Cria um "risco de lesão futura", que é apenas uma especulação de dano em vez de dano real. Para reivindicar com sucesso a compensação, um titular de dados deve provar que a perda de controle causou dano material ou não material que lhe trouxe desvantagem real e, ainda, do ponto de vista legal, que esse dano é recuperável por responsabilidade civil definida por lei. Portanto, como o julgamento confirmou e a literatura elaborou, um requisito cumulativo para compensação é de fato estabelecido pelo Artigo 82 do GDPR. Três condições cumulativas devem ser estabelecidas para fins de compensação: a existência de violação de qualquer disposição do GDPR, a existência de dano material ou não material e um vínculo causal entre a violação e o dano. Quanto à natureza da perda de controle, nota-se que a redação do Considerando (85) do GDPR é confusa. Neste considerando, a perda de controle é equivalente a dano. Esta equivalência é errada e enganosa.

O Recital 85 do GDPR sugere que a perda de controle é equivalente a dano, mas essa equivalência não tem sido reconhecida para fins de fixação de indenização. Assim, tem-se compreendido que para reivindicar a indenização, o titular dos dados deve provar que a perda de controle sobre os dados causou um dano material ou imaterial que resultou em uma desvantagem real. Esta abordagem visa evitar indenizações baseadas apenas em riscos especulativos, exigindo provas concretas de que a violação resultou em danos concretos[109].

## 2.1 A responsabilidade civil dos agentes de tratamento em casos de controladoria conjunta

Um aspecto da responsabilidade civil dos agentes de tratamento não mencionado na LGPD, mas cuja discussão é presente e já se encontra bastante desenvolvida na União Europeia diz respeito à responsabilidade civil em casos de controladoria conjunta de dados pessoais.

Segundo o art. 5º, inciso IX, da LGPD são agentes de tratamento o controlador e o operador. O controlador é definido como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (inciso VI) e o operador é definido como a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (inciso VII). A diferença básica entres esses agentes de tratamento é o poder decisório a respeito do modo com que os dados serão tratados[110].

Tendo em vista a sua maior responsabilidade sobre o tratamento, a LGPD atribui uma série de deveres ao controlador, como o dever de elaborar relatório de impacto, fornecer instruções sobre o tratamento ao operador, o suporte do ônus da prova quanto ao consentimento do titular, dentre outros[111].

A LGPD, contudo, não prevê, mas também não exclui, a possibilidade de mais de um controlador ser responsável pelo tratamento de dados. Desse modo, não há previsão legal

---

[109] LI, Shu. Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. Maastricht Journal of European and Comparative Law, v. 30, n. 3, p. 335-345, 2023. Disponível em: https://doi.org/10.1177/1023263X231208835.

[110] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 jun. 2024.

[111] Idem.

de como se deve dar o compartilhamento da responsabilidade nesses casos. Não se sabe, por exemplo, se caso constatada a controladoria conjunta, se cada agente responde na medida da sua responsabilidade pelas decisões tomadas ou se ambos respondem de forma integral pelo tratamento irregular realizado.

Nesse sentido, vale mencionar a decisão no caso C-210/16 (*Wirtschaftsakademie Schleswig-Holstein GmbH*), em que o Tribunal de Justiça da União Europeia decidiu que um administrador de uma *fan page* no *Facebook* pode ser considerado um controlador conjunto com o *Facebook* no que diz respeito ao processamento de dados dos visitantes da página. O tribunal enfatizou que ambos têm influência sobre o processamento de dados e, portanto, compartilham a responsabilidade de garantir a conformidade com o GDPR[112]. *In verbis:*

> 29 Além disso, uma vez que, como está expressamente previsto no artigo 2.o, alínea d), da Diretiva 95/46, o conceito de «responsável pelo tratamento» visa o organismo que, «individualmente ou em conjunto com outrem», determine as finalidades e os meios de tratamento dos dados pessoais, este conceito não se refere necessariamente a um único organismo e pode dizer respeito a vários atores que participam nesse tratamento, estando assim cada um deles sujeito às disposições aplicáveis em matéria de proteção dos dados. 30 No caso em apreço, deve considerar-se que a Facebook Inc. e, tratando-se da União, a Facebook Ireland determinam, a título principal, as finalidades e os meios de tratamento dos dados pessoais dos utilizadores do Facebook, bem como das pessoas que já visitaram as páginas de fãs alojadas no Facebook, e são por isso abrangidas pelo conceito de «responsável pelo tratamento», na aceção do artigo 2.o, alínea d), da Diretiva 95/46, o que não é posto em causa no presente processo. 31 Posto isto, e para responder às questões colocadas, importa examinar se e em que medida o administrador de uma página de fãs alojada no Facebook, como a Wirtschaftsakademie, contribui, no âmbito desta página de fãs, para determinar, conjuntamente com a Facebook Ireland e com a Facebook Inc., as finalidades e os meios de tratamento dos dados pessoais dos visitantes da referida página de fãs e pode, por conseguinte, também ele ser considerado «responsável pelo tratamento», na aceção do artigo 2.o, alínea d), da Diretiva 95/46[113].

O Tribunal interpretou que um controlador é qualquer entidade que, sozinha ou em conjunto com outras, determina as finalidades e os meios do tratamento de dados pessoais. A *fan page* da *Wirtschaftsakademie* permitia à empresa obter dados estatísticos anônimos sobre os visitantes da página por meio de uma ferramenta fornecida pelo *Facebook* chamada "Facebook Insights".

---

[112]TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-210/16, Wirtschaftsakademie Schleswig-Holstein GmbH, 5 de junho de 2018. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-210/16. Acesso em: 29 jun. 2024.
[113] Idem.

Além disso, enfatizou que tanto a *Wirtschaftsakademie* quanto o *Facebook* tinham a obrigação de fornecer informações claras e completas aos usuários sobre o tratamento de seus dados e garantir que seus direitos, à luz do GDPR, fossem respeitados. Isso porque, a decisão reconheceu que ambas as partes se beneficiavam do tratamento de dados. O *Facebook* usava os dados para seus próprios fins comerciais, enquanto a *Wirtschaftsakademie* usava os dados para melhorar seu alcance e interação com os visitantes da *fan page*. Vale citar trecho da decisão nesse sentido:

> 34 Estes tratamentos de dados pessoais visam, designadamente, permitir, por um lado, à Facebook melhorar o seu sistema de publicidade, que difunde através da sua rede, e, por outro, ao administrador da página de fãs obter estatísticas elaboradas pela Facebook a partir das visitas a esta página, para fins de gestão da promoção da sua atividade, permitindo-lhe conhecer, por exemplo, o perfil dos visitantes que apreciam a sua página de fãs ou que utilizam as suas aplicações, para que lhes possa propor um conteúdo mais pertinente e desenvolver funcionalidades suscetíveis de suscitar o seu interesse. 35 Ora, se o simples facto de utilizar uma rede social como o Facebook não torna um utilizador do Facebook corresponsável por um tratamento de dados pessoais efetuado por esta rede, importa, em contrapartida, sublinhar que o administrador de uma página de fãs alojada no Facebook, com a criação de tal página, oferece à Facebook a possibilidade de colocar cookies no computador ou em qualquer outro aparelho da pessoa que tenha visitado a sua página de fãs, independentemente de esta pessoa ter ou não conta no Facebook[114].

Essa decisão criou um precedente importante para a definição de controladoria conjunta na União Europeia, ao afirmar que mesmo entidades que não têm acesso direto aos dados pessoais, mas que influenciam ou se beneficiam do tratamento, podem ser consideradas controladores conjuntos, o que, consequentemente, amplia o escopo de possíveis agentes de tratamento responsáveis pelos dados.

Outra decisão importante do tribunal é a do caso C-40/17, envolvendo a empresa *Fashion ID GmbH & Co. KG* e uma organização de consumidores alemã, a *Verbraucherzentrale NRW eV.* A empresa é um e-commerce de moda que incorporou um plugin de terceiros, especificamente o botão "Curtir" do Facebook, em seu *website,* violando assim as regras de proteção de dados do GDPR ao coletar e transmitir dados pessoais dos visitantes de seu *site* para o *Facebook* sem o consentimento destes[115].

Uma das principais questões discutidas pelo acórdão foi se a *Fashion ID*, ao incorporar o plugin "Curtir" do *Facebook*, poderia ser considerada um controlador conjunto

[114] Idem.
[115] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, 29 de julho de 2019. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-40/17. Acesso em: 29 jun. 2024.

com o *Facebook* no que diz respeito ao tratamento de dados pessoais dos titulares visitantes do seu *website*. *In verbis:*

> 68 O Tribunal de Justiça considerou igualmente que uma pessoa singular ou coletiva que influencia, para fins que lhe são próprios, o tratamento de dados pessoais e participa, assim, na determinação das finalidades e dos meios desse tratamento pode ser considerada responsável pelo tratamento, na aceção do artigo 2.o, alínea d), da Diretiva 95/46 (Acórdão de 10 de julho de 2018, Jehovan todistajat, C‑25/17, EU:C:2018:551, n.o 68). 69 Por outro lado, a responsabilidade conjunta de vários intervenientes pelo mesmo tratamento, por força desta disposição, não pressupõe que cada um deles tenha acesso aos dados pessoais em causa (v., neste sentido, Acórdãos de 5 de junho de 2018, Wirtschaftsakademie Schleswig‑Holstein, C‑210/16, EU:C:2018:388, n.o 38, e de 10 de julho de 2018, Jehovan todistajat, C‑25/17, EU:C:2018:551, n.o 69). 70 Assim sendo, na medida em que o objetivo do artigo 2.o, alínea d), da Diretiva 95/46 é assegurar, através de uma definição ampla do conceito de «responsável», uma proteção eficaz e completa das pessoas em causa, a existência de responsabilidade conjunta não se traduz necessariamente em responsabilidade equivalente, para o mesmo tratamento de dados pessoais, dos diferentes intervenientes. Pelo contrário, os referidos intervenientes podem estar envolvidos em diferentes fases desse tratamento e em diferentes graus, pelo que o nível de responsabilidade de cada um deve ser avaliado tendo em conta todas as circunstâncias pertinentes do caso concreto (v., neste sentido, Acórdão de 10 de julho de 2018, Jehovan todistajat, C‑25/17, EU:C:2018:551, n.o 66)[116].

A decisão do Tribunal no caso ampliou ainda mais a interpretação de controladoria conjunta ao decidir que qualquer entidade que facilite a coleta de dados pessoais através da integração de *plugins* de terceiros pode ser considerada um controlador conjunto. Desse modo, muitas empresas que utilizam *plugins* de redes sociais ou outras ferramentas de terceiros em seus *websites* precisaram revisar suas práticas de tratamento para garantir a conformidade com o GDPR[117].

Outro ponto importante esclarecido na decisão é que o reconhecimento da controladoria conjunta não pressupõe que todos os agentes tivessem acesso a todos os dados pessoais tratados e nem que a responsabilidade deles seja igual, mesmo porque estes podem estar envolvidos em diferentes fases do tratamento e em diferentes graus, de modo que "o nível de responsabilidade de cada um deve ser avaliado tendo em conta todas as circunstâncias pertinentes do caso concreto"[118].

Outro caso interessante no contexto do GDPR e da União Europeia é o C-25/17 -Jehovan todistajat (Testemunhas de Jeová), cuja discussão levada ao Tribunal de Justiça da

[116] Idem.
[117] Idem.
[118] Idem.

União Europeia consistia em analisar se a congregação Testemunhas de Jeová poderia ser considerada um controlador conjunto com os pregadores individuais em relação ao tratamento de dados pessoais coletados durante a pregação de porta em porta realizada por estes[119].

O tribunal decidiu que, como controladores conjuntos, tanto a congregação quanto os pregadores individuais tinham a responsabilidade de garantir que os direitos dos titulares dos dados fossem respeitados e destacou que qualquer organização que exerça uma influência significativa sobre as atividades de coleta e tratamento de dados pode ser considerada um controlador conjunto, independentemente de quem realiza fisicamente a coleta dos dados[120]. Vide trecho da decisão:

> 72 Tais circunstâncias permitem considerar que a Comunidade das testemunhas de Jeová encoraja os seus membros pregadores a procederem a tratamentos de dados pessoais no âmbito da sua atividade de pregação. 73 Verifica‑se assim, tendo em conta os autos submetidos ao Tribunal de Justiça, que ao organizar, coordenar e incentivar a atividade de pregação dos seus membros para divulgar a sua fé, a Comunidade das testemunhas de Jeová participa, conjuntamente com os seus membros pregadores, na determinação da finalidade e dos meios de tratamento de dados pessoais das pessoas abordadas, o que cabe, no entanto, ao órgão jurisdicional de reenvio apreciar à luz de todas as circunstâncias do caso vertente. 74 Esta conclusão não pode ser posta em causa pelo princípio da autonomia organizacional das comunidades religiosas que decorre do artigo 17.o TFUE. Com efeito, o dever de respeitar as normas de direito da União em matéria de proteção de dados pessoais não pode ser considerado uma ingerência na autonomia organizacional das referidas comunidades (v., por analogia, Acórdão de 17 de abril de 2018, Egenberger, C‑414/16, EU:C:2018:257, n.o 58). 75 Tendo em conta as considerações precedentes, há que responder à terceira e quarta questões que o artigo 2.o, alínea d), da Diretiva 95/46, lido à luz do artigo 10.o, n.o 1, da Carta, deve ser interpretado no sentido de que permite considerar uma comunidade religiosa conjuntamente responsável com os seus membros pregadores pelo tratamento de dados pessoais efetuado por estes últimos no âmbito de uma atividade de pregação porta a porta organizada, coordenada e promovida por esta comunidade, não sendo necessário que a referida comunidade tenha acesso aos dados, nem que deva ser demonstrado que essa comunidade deu orientações escritas ou instruções a respeito desses tratamentos aos seus membros.

O *European Data Protection Board* é uma autoridade independente da União Europeia que assegura a aplicação das regras de proteção de dados (inclusive o GPDR) entre

---

[119] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-25/17, Jehovan todistajat (Testemunhas de Jeová), 10 de julho de 2018. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-25/17. Acesso em: 29 jun. 2024.
[120] Idem.

os estados membros. Uma das principais funções da autoridade é emitir diretrizes para ajudar os agentes a cumprirem suas obrigações de proteção de dados[121].

A autoridade emitiu um guia orientativo acerca do tema da controladoria conjunta que traz informações importantes sobre o tema, como a definição de critérios para identificar quando ocorre a controladoria conjunta. Nesse sentido, define que são considerados controladores conjuntos quando ambas as partes envolvidas no tratamento tiverem uma influência decisiva sobre as finalidades e o modo de tratamento dos dados, o que, em outras palavras significa que ambas participam ativamente da decisão ao invés de uma simplesmente seguir as instruções da outra[122].

A consequência prática do reconhecimento da controladoria conjunta é que as empresas respondem de forma solidária pelos danos causados aos titulares e pelo cumprimento das obrigações previstas no GDPR, o que significa que os titulares podem exercer seus direitos contra qualquer um dos controladores conjuntos.

No ordenamento jurídico brasileiro, o entendimento jurisprudencial permite que trabalhadores ou consumidores ajuízem ações contra empresas pertencentes ao mesmo grupo econômico, que atuam de forma integrada, com interesses comuns e controle unificado, tendo em vista que são solidariamente responsáveis pelas obrigações trabalhistas e de consumo.

Por esse motivo, a definição das obrigações contratuais entre essas empresas que atuam em controladoria conjunta é primordial, sobretudo para que restem claros os deveres de cada uma em relação ao cumprimento da legislação sobre proteção de dados, bem como sobre as medidas de segurança a serem adotadas e o ônus de prestar contas de suas atividade tanto aos titulares quanto às autoridades legais.

Quando essas obrigações não são definidas no âmbito contratual resta margem para que elas sejam ajustadas extracontratualmente, no âmbito do regime de responsabilidade civil adotado, criando o risco de que uma entidade arque com prejuízos não efetivamente causados por elas em relação a decisões sobre um tratamento que não tinha realmente controle.

Contudo, é importante ressaltar que a mera definição de responsabilidades contratuais entre os controladores conjuntos não é suficiente para afastar o reconhecimento da controladoria conjunta e suas consequências, devendo ainda ser observados os requisitos anteriormente estudados.

---

[121] EUROPEAN DATA PROTECTION BOARD. Guidelines on Joint Controllership. Disponível em: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en. Acesso em: 29 jun. 2024.
[122] Idem.

Por fim, compreende-se que identificar os controladores conjuntos é essencial para garantir a conformidade com a legislação de proteção de dados e proteger os direitos dos titulares e, principalmente, para garantir a responsabilização de todos os agentes que tenham poder decisório sobre o tratamento dos dados pessoais.

## 2.2 A responsabilidade do encarregado de dados

Tanto a legislação brasileira quanto a europeia mencionam a figura do encarregado de dados, ou data protection officer - DPO, que é o profissional designado por uma organização para supervisionar a conformidade com as leis de proteção de dados, como o GDPR e a LGPD.

O GDPR exige a nomeação de um encarregado em determinadas circunstâncias, como quando o processamento é realizado por uma autoridade ou órgão público, quando as atividades de processamento envolvem monitoramento regular e sistemático de pessoas em grande escala, ou quando envolve grandes volumes de dados sensíveis.

Segundo o art. 41 da LGPD, o controlador de dados deverá indicar um encarregado pelo tratamento de dados pessoais, mas não menciona situações específicas em que deverá fazê-lo, como feito pelo GDPR. Desse modo, compreende-se que o intuito da Lei era que todas as organizações às quais se aplicam a LGPD devessem nomear um encarregado.

A ANPD, no entanto, publicou a Resolução CD/ANPD nº 2, de 27 janeiro de 2022, que define critérios para a dispensa da obrigação de nomear um encarregado pelo tratamento de dados pessoais. Nos termos do art. 11 da Resolução "Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais", devendo, contudo "disponibilizar um canal de comunicação com o titular de dados para atender o disposto no art. 41, § 2º, I, da LGPD."

Ambas as legislações atribuem deveres importantes aos encarregados, deveres estes que, não cumpridos com diligência, podem acarretar prejuízos aos dados pessoais tratados pelo agente de tratamento.

Entre suas principais atividades definidas na LGPD, se encontra o dever de aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar as providências necessárias. Além disso, é sua responsabilidade receber comunicações da ANPD e tomar as ações apropriadas em resposta.

O encarregado também deve orientar os funcionários e contratados da entidade sobre as práticas adequadas a serem adotadas em relação à proteção de dados pessoais, garantindo

que todos estejam cientes das políticas e procedimentos de conformidade. Ele deve ainda executar outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares, assegurando que a organização mantenha suas operações dentro das regulamentações de proteção de dados. Essas atividades são fundamentais para garantir que a privacidade dos dados pessoais seja respeitada e protegida.

O GPDR traz uma lista de atribuições mais extensa ao encarregado, devendo ele, segundo o Artigo 39º do Regulamento, informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores envolvidos no tratamento de dados, sobre suas obrigações conforme a legislação vigente. Além disso, o DPO é responsável por monitorar a conformidade com o GDPR, com outras disposições de proteção de dados da União Europeia ou dos Estados-Membros, e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais. Isso inclui a repartição de responsabilidades, a sensibilização e formação do pessoal envolvido nas operações de tratamento de dados, e a realização de auditorias.

Apesar de ambas as legislações atribuírem deveres bastante delineados ao Encarregado do tratamento, nenhuma delas menciona especificamente a possibilidade de responsabilização direta deste profissional.

No contexto europeu, há algumas decisões que destacam a importância das obrigações do DPO, mas reafirma que a responsabilidade principal permanece sobre o agente de tratamento[123] [124]. É o caso do acórdão no caso C-453/21, em que o Tribunal de Justiça da União Europeia determinou que os DPO's devem manter independência em suas funções e que a demissão de um DPO só pode ocorrer por justa causa, não podendo ser penalizados por cumprir suas obrigações sob o GDPR. O caso envolveu a empresa X-FAB Dresden, onde o Tribunal afirmou que a combinação das funções de DPO com outras funções dentro da organização (como presidente do conselho de trabalhadores) pode criar um conflito de interesses[125]. Segue trecho da referida decisão:

> Tendo em conta as considerações precedentes, há que responder à primeira questão que o artigo 38.o, n.o 3, segundo período, do RGPD deve ser interpretado no sentido de que não se opõe a uma regulamentação nacional que prevê que um responsável pelo tratamento ou um subcontratante só pode despedir um encarregado da proteção de dados que seja um elemento do seu

[123] DREWER, D.; MILADINOVA, V. The canary in the data mine. Computer Law & Security Review, v. 34, p. 806-815, 2018. Disponível em: https://doi.org/10.1016/J.CLSR.2018.05.019. Acesso em: 29 jun. 2024.
[124] ŠIDLAUSKAS, A. (2021). The Role and Significance of the Data Protection Officer in the Organization. Sociedade e Tecnologia, 44(1), 8–28. DOI: https://doi.org/10.15388/Soctyr.44.1.1.
[125] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-453/21, X-FAB Dresden, 9 de fevereiro de 2023. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-453/21. Acesso em: 29 jun. 2024.

> pessoal com justa causa, mesmo que o despedimento não esteja relacionado com o exercício das funções desse encarregado, desde que essa regulamentação não comprometa a realização dos objetivos do RGPD.

A decisão reforça a necessidade de o DPO manter independência no desempenho de suas funções ao decidir que este não deve ser penalizado por cumprir suas obrigações de maneira independente, conforme os requisitos do Artigo 38 do GDPR, de modo que a responsabilidade final por qualquer falha na conformidade com o GDPR deve recair sobre o agente de tratamento.

Fazendo uma analogia de institutos, no Brasil, muito embora um funcionário de uma empresa responda por ela legalmente, é possível, através de uma ação de regresso, responsabilizar o sujeito que efetivamente causou o dano. O Código Civil Brasileiro, em seus artigos 932 e 933, estabelece a responsabilidade dos empregadores pelos atos de seus empregados, mas também permite a ação de regresso contra o agente causador do dano.

Desse modo, tendo em vista a omissão da LGPD em relação ao tema, seria possível responsabilizar regressivamente o encarregado em casos de negligência, imprudência ou imperícia no exercício da sua função que resultem em prejuízos ao titular de dados mesmo que a LGPD tenha sido omissa em relação ao tema?

Tanto a LGPD quanto o GDPR enfatizam, na descrição do princípio da responsabilização, que os agentes de tratamento são os responsáveis pela adequação do tratamento aos princípios aplicáveis à proteção de dados pessoais.

No entanto, a realidade do tratamento de dados das empresas e entidades que processam dados pessoais pode ser muito mais complexa do que os legisladores são capazes de prever. O início da vigência da LGPD no Brasil foi regada a uma série de incertezas acerca de como as normas seriam aplicadas pelos Tribunais e qual seria a função dos diversos agentes envolvidos no tratamento de dados pessoais.

Pela falta de conhecimento acerca da adequação legal às normas de proteção de dados somado ao receio dos agentes de serem penalizados nas severas sanções previstas na Lei, houve um aumento na procura de especialistas para realizar a adequação desses agentes. Este fenômeno gerou um aumento significativo na demanda pela profissão de DPO, ou encarregado de proteção de dados[126].

---

[126] PITOMBO, Clara. LGPD aumenta a busca por executivo de proteção de dados. Valor Econômico, São Paulo, 23 set. 2021. Carreira. Disponível em: https://valor.globo.com/carreira/noticia/2021/09/23/lgpd-aumenta-a-busca-por-executivo-de-protecao-de-dados.ghtml. Acesso em: 21 jun. 2024.

A LGPD não especificou que o encarregado pelo tratamento de dados deveria necessariamente ser uma pessoa física, o que tem aberto margem para interpretação de que este pode ser uma pessoa jurídica. O reconhecimento da possibilidade de que o DPO possa ser uma empresa tem algumas implicações de ordem prática.

A primeira delas é que em todos os regimes de responsabilidade empresas são responsabilizadas de modo distinto de pessoas físicas. As empresas podem ter sua responsabilidade financeira limitada pela figura da pessoa jurídica enquanto a pessoa física não. Além disso, as empresas possuem mais liberdade de estabelecer contratualmente os limites da sua responsabilidade no caso de ocorrência de prejuízos ao titular.

Um importante questionamento a ser feito é se o entendimento de que somente os agentes de tratamento possam ser responsabilizados em casos de tratamento irregular, sob a argumentação de que eles tomam as decisões acerca dos dados, reflete a realidade da terceirização do tratamento de dados aos DPO's pessoas jurídicas.

Devido à especificidade da atividade de tratamento de dados e à especialidade do encarregado, que conhece a fundo as técnicas de tratamento e as legislações aplicáveis, a realidade demonstra que frequentemente as decisões acerca do tratamento são praticamente terceirizadas a essas empresas e/ou profissionais, os quais, apesar de serem teoricamente encarregados cumprem a função de um agente de tratamento.

Isso levanta a questão sobre a verdadeira natureza das responsabilidades e decisões no âmbito do tratamento de dados. Se o encarregado, sendo uma pessoa jurídica, assume a responsabilidade pelas decisões de tratamento, isso implica que essa entidade deveria ser reconhecida como um agente de tratamento. Dessa forma, a responsabilidade pelo tratamento de dados passa a ser compartilhada ou transferida para a empresa contratada, o que pode alterar significativamente o panorama de responsabilização em casos de violações da LGPD.

Ademais, a contratação de encarregados pessoas jurídicas pode gerar um afastamento entre o controlador dos dados e a atividade de tratamento, tornando a cadeia de tratamento de dados mais complexa. Isso pode dificultar a identificação de responsabilidades e a adoção de medidas corretivas em caso de incidentes de segurança.

Por fim, a prática de terceirizar o papel do DPO para uma pessoa jurídica pode significar uma forma de os controladores transferirem parte do risco e da responsabilidade relacionada ao tratamento de dados, distanciando o titular da atividade de tratamento e dificultando o exercício de seus direitos sobre os seus dados.

## 2.3 A responsabilidade do sub-operador

A dinâmica de tratamento de dados pessoais na sociedade atual faz com que a atividade de tratamento de dados possa ser mais complexa do que a legislação consegue prever. Essa complexidade decorre do volume e diversidade de dados tratados, a globalização e aumento da necessidade de transferência de dados entre múltiplos agentes, bem como os próprios riscos envolvidos na atividade de tratamento.

Uma consequência direta desse cenário é que, apesar de a LGPD no Brasil ter previsto apenas as figuras do controlador e do operador de dados, a realidade demonstra a importância de um terceiro agente nessa dinâmica. Na União Europeia, esse terceiro é conhecido como sub-operador.

Segundo a LGPD são agentes de tratamento o controlador e o operador de dados, definidos na Lei como a pessoa natural ou jurídica, de direito público ou privado "a quem competem as decisões referentes ao tratamento de dados pessoais" e "que realiza o tratamento de dados pessoais em nome do controlador"[127] respectivamente. Estes agentes de tratamento desempenham papéis distintos e complementares no tratamento de dados pessoais.

O controlador, conforme o art. 37 da LGPD, é responsável por determinar as finalidades e os meios do tratamento de dados pessoais. Isso inclui manter registros detalhados das operações de tratamento realizadas, especialmente quando baseadas no legítimo interesse. Esses registros devem documentar as atividades realizadas com os dados pessoais, como sua coleta, utilização, compartilhamento e armazenamento[128].

Além disso, o controlador, conforme previsto no art. 38, deve estar preparado para elaborar relatórios de impacto à proteção de dados, os quais são especialmente necessários quando o tratamento envolve dados sensíveis.

Por outro lado, o operador, conforme o art. 39, atua na execução do tratamento de dados em conformidade com as instruções fornecidas pelo controlador. Essas instruções são definidas pelo controlador, que monitora o cumprimento das normas e diretrizes estabelecidas para garantir a proteção dos dados pessoais[129]. O operador deve seguir rigorosamente estas instruções, assegurando que todas as atividades de processamento estejam alinhadas com os propósitos estabelecidos pelo controlador.

---

[127] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 19 jun. 2024.
[128] Idem.
[129] Idem.

Como mencionado, a realidade de tratamento de dados demonstra que muitas vezes o operador precisa terceirizar as responsabilidades atribuídas pelo controlador, como no caso de empresas que armazenam os dados por ela tratados em uma plataforma de um provedor de serviços em nuvem, por exemplo[130]. Com o aumento da quantidade de dados tratados pelas empresas, cresce também a complexidade desses dados e aumenta a necessidade de se especializar a atividade de tratamento, expandindo assim a cadeia de tratamento. O Guia Orientativo para Definições dos Agentes de Tratamento elaborado pela ANPD apresenta o seguinte exemplo hipotético da situação supramencionada:

> A empresa ALPHA deseja contratar uma pesquisa de mercado para alavancar suas vendas. Para isso, contrata a empresa de pesquisas BRAVO, que envia os resultados para a empresa ALPHA. Com a autorização da empresa ALPHA, a empresa BRAVO contrata os serviços de armazenamento em nuvem da empresa CHARLIE. A empresa ALPHA pode ser considerada controladora pois verifica-se que foram cumpridos os seguintes requisitos: i) a empresa A teve poder decisório em relação ao tratamento de dados; ii) os elementos essenciais do tratamento foram definidos pela empresa A: finalidade, titulares (por exemplo mulheres da faixa etária de 20 a 30 anos, residentes em Brasília/DF), tipos de dados (por exemplo nome, idade, endereço, preferência alimentar) etc. Ainda que possa decidir quanto às técnicas a ser empregadas no processo de tratamento de dados para gerar os resultados da pesquisa, a empresa de pesquisas BRAVO realiza os tratamentos de dados de acordo com a finalidade e as instruções determinadas pela empresa ALPHA, atuando, portanto, como operadora. A empresa CHARLIE atua conforme diretrizes da empresa BRAVO e seria, portanto, suboperadora. É recomendável que BRAVO obtenha autorização formal de ALPHA para a subcontratação de CHARLIE.

Diante da omissão da LGPD em relação ao tema, a ANPD elaborou um Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, visando fornecer maior clareza sobre as responsabilidades e funções de cada agente envolvido no tratamento de dados pessoais, incluindo a figura do sub operador, que, apesar de não ser mencionada explicitamente na LGPD, desempenha um papel importante no tratamento de dados[131].

Segundo o Guia Orientativo, a relação direta do sub-operador é com o operador e não com o controlador e independentemente dos arranjos institucionais entre operador e sub

---

[130] BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, DF: ANPD, maio de 2021, p. 20. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf> Acesso em: 19. jun. 2024.

[131] BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, DF: ANPD, maio de 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf> Acesso em: 19. jun. 2024.

operador, ambos podem, conforme o caso concreto, desempenhar a função de operador e, assim, são responsáveis perante a ANPD[132]. Recomenda ainda que, tendo em vista que o operador realiza o tratamento em nome do controlador, este tenha a autorização formal do controlador para a contratar o sub-operador[133].

Tal recomendação inspira-se no texto do GDPR que previu a figura do subcontratante e autoriza que este realize a contratação de um outro subcontratante sob a condição de que o responsável pelo tratamento forneça autorização específica ou geral para tanto[134].

O texto do Guia Orientativo vai além, estabelecendo, a respeito das responsabilidades, que "o sub-operador pode ser equiparado ao operador perante a LGPD em relação às atividades que foi contratado para executar". Com a devida vênia ao entendimento adotado pela Autoridade, criar uma equiparação de agente de tratamento para fins de responsabilização destes não se encontra na esfera de competência da ANPD, uma vez que a própria LGPD não prevê explicitamente essa figura.

Muito embora LGPD tenha um forte apelo ao interesse público no tratamento de dados pessoais, bem como que compete à ANPD a regulação complementar de matérias relacionadas à proteção de dados, ainda há que se observar que a definição de um regime de responsabilidade, bem como a determinação dos agentes responsáveis, ainda é uma matéria que deve ser tratada no âmbito legislativo.

Isso porque, o reconhecimento do sub-operador como um agente de tratamento traz implicações e sanções tanto no âmbito administrativo quanto judicial, assim como impõe uma série de deveres e responsabilidades a serem observadas em relação aos dados pessoais dos titulares.

Além do mais, a LGPD impõe sanções severas aos agentes de tratamento, inclusive aos operadores, que possuem teoricamente menos responsabilidade que os controladores. A falta de previsão legal para responsabilizar os sub-operadores cria uma grande instabilidade jurídica, podendo acarretar prejuízos para as entidades que tratam dados pessoais e dificultar a identificação da cadeia de agentes de tratamento, tornando a reparação ao titular de dados mais difícil.

---

[132] Ibidem, p. 19.
[133] Idem.
[134] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados - RGPD). Art. 28. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 19. jun. 2024.

# 3 AS DECISÕES JUDICIAIS CONDENATÓRIAS EM RESPONSABILIDADE CIVIL NOS SISTEMAS BRASILEIRO E EUROPEU

## 3.1 Análise dos acórdãos proferidos pelos Tribunais de Justiça brasileiros nos primeiros anos de vigência da LGPD

O Centro de Direito, Internet e Sociedade - CEDIS, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP, juntamente com o Jusbrasil, no projeto Painel LGPD nos Tribunais, realizou um importante levantamento qualitativo e quantitativo de decisões envolvendo a LGPD nos seus primeiros anos de vigência[135].

O projeto é uma iniciativa do Jusbrasil, em parceria com o CEDIS do IDP, e com o apoio do Programa das Nações Unidas para o Desenvolvimento - PNUD. O painel reúne e facilita o acesso a decisões judiciais relevantes sobre a LGPD nos tribunais brasileiros, permitindo consultas detalhadas e gratuitas.

O CEDIS é um núcleo de pesquisa dedicado a fortalecer os direitos fundamentais no ambiente digital, com ênfase na promoção da privacidade, proteção de dados pessoais e liberdade de expressão, além do estímulo à liberdade de expressão, à concorrência e à inovação, por intermédio de diversas iniciativas e estudos.

O Jusbrasil é uma plataforma online que facilita o acesso a informações jurídicas no ordenamento jurídico brasileiro. Ele oferece uma vasta base de dados com conteúdos como decisões judiciais, leis, jurisprudência, notícias e artigos relacionados ao direito. A plataforma é amplamente utilizada por advogados, estudantes de direito, profissionais do setor jurídico e cidadãos em geral para pesquisar e acompanhar casos e legislações.

Já a PNDU, apoiadora do projeto, é uma agência da ONU que trabalha para erradicar a pobreza e reduzir as desigualdades no mundo. No Brasil, o PNUD apoia projetos que promovem o desenvolvimento sustentável, fortalecem a democracia, protegem os direitos humanos e promovem a inclusão social. A agência colabora com governos, sociedade civil e

[135] Centro de Direito, Internet e Sociedade (CEDIS-IDP); Jusbrasil. Painel LGPD nos Tribunais: Jurisprudência do 2º ano de vigência da Lei Geral de Proteção de Dados. Última atualização: Abril de 2023 (com dados de setembro de 2022). Disponível em: <https://painel.jusbrasil.com.br/>. Acesso em: 27 ago. 2023.

setor privado para implementar políticas públicas que atendam aos Objetivos de Desenvolvimento Sustentável (ODS).

Segundo informações fornecidas no site oficial do projeto, a pesquisa realizada teve um caráter empírico e exploratório, focando na experiência do judiciário brasileiro com a aplicação da LGPD entre setembro de 2020 e setembro de 2022. Inicialmente, foi feita uma análise quantitativa dos dados coletados, utilizando estatística descritiva para resumir, categorizar e interpretar as informações. Os documentos foram obtidos através de um sistema de Inteligência Artificial do Jusbrasil, que utilizou algoritmos de busca e categorização. Todos os dados coletados são públicos, disponíveis em diários oficiais e páginas de jurisprudência dos tribunais.

Os 50 pesquisadores que compõem o projeto conduziram a análise de 1.789 documentos ao longo de um período de 2 anos de estudo. Os dados coletados abrangem informações até setembro de 2022.

Como se trata de um tema recentemente legislado, a jurisprudência acerca da responsabilidade civil em proteção de dados não está suficientemente consolidada nos Tribunais Superiores, de modo que serão utilizados principalmente os acórdãos proferidos pelos Tribunais de Justiça dos Estados e as poucas decisões do Superior Tribunal de Justiça.

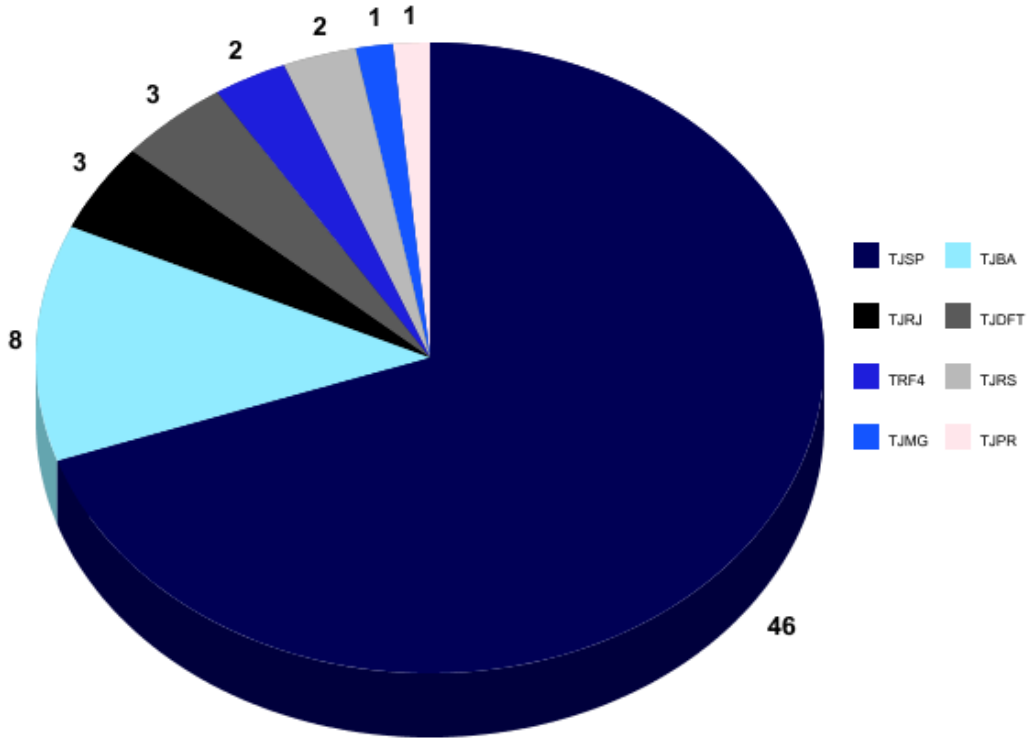
Foram utilizados os seguintes filtros, aplicados no campo “Lista de Decisões Relevantes na Íntegra”, para selecionar as decisões a serem analisadas.

No campo “Pertinência do Debate sobre a LGPD”, foi aplicado o filtro “LGPD é a questão central do caso”. Já no campo “Filtro por Tribunal “ foram selecionados todos os Tribunais.

No “Filtro por área”, foram selecionados todos os campos, no “Filtro por problema” foram selecionados todos os campos que continham o termo “Responsabilidade Civil” e no “Filtro por Capítulo” foram selecionados todos os campos.

A inserção dos referidos filtros resultou na seleção de 65 acórdãos, sendo 1 do TJMG, 21 do TJSP, 2 do TJBA, 1 do TJPR, 1 do TJAM, e 2 do TJRS, os quais serão analisados no presente estudo. A inserção dos filtros pré-selecionados resultou na seleção de 65 acórdãos, em sua maioria do Tribunal de Justiça do Estado de São Paulo - TJSP, conforme se verifica do gráfico abaixo:

**Gráfico 1 - Quantidade de acórdãos julgados por Tribunal**

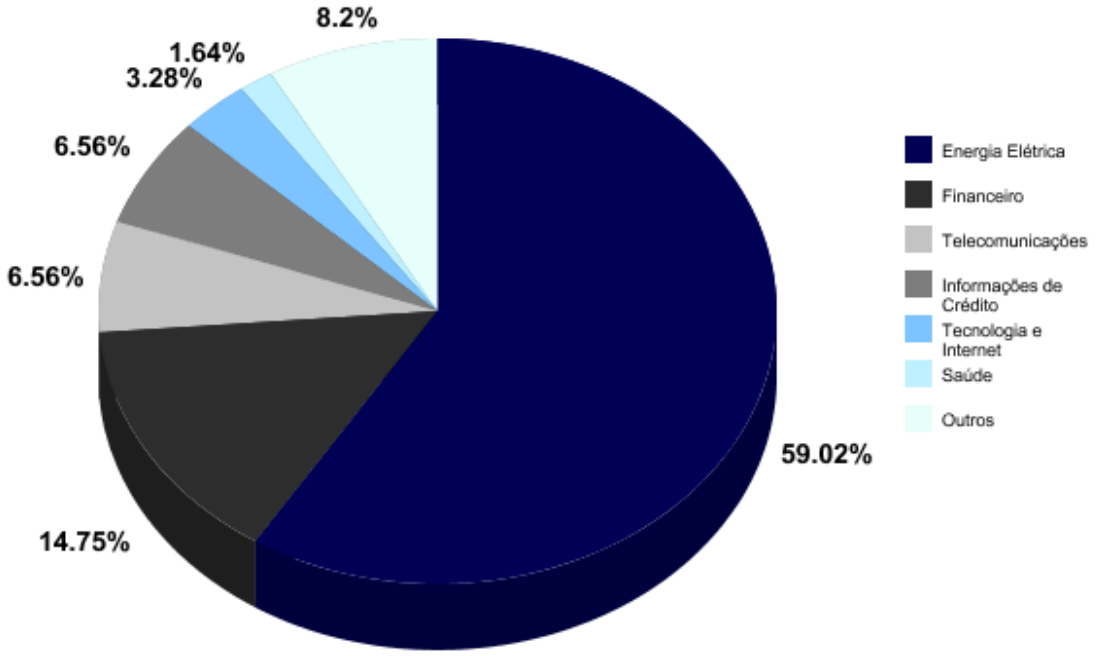



Fonte: Elaborado pela autora.

Após a leitura e análise de todos os acórdãos filtrados, verificou-se a existência de 2 (dois) acórdãos em que a LGPD não é a questão central, 5 (cinco) acórdãos em que o mérito não é enfrentado e 4 (quatro) acórdãos que se encontram em segredo de justiça, dos quais, a 3 (três) não foi possível a leitura do conteúdo da decisão. Desse modo, foram analisadas os 55 (cinquenta e cinco) acórdãos restantes.

Os setores dos principais agentes de tratamento de dados mencionados nos acórdãos são variados, incluindo empresas do setor privado, como instituições financeiras, empresas de telecomunicações, concessionárias de serviços públicos e órgãos públicos, como se verifica do gráfico abaixo:

**Gráfico 2: Setores  dos agentes de tratamento mais recorrentes**




Fonte: Elaborado pela autora.

O setor de energia elétrica ocupa 59.02% do gráfico, o que representa 36 (trinta e seis) ocorrências. A Eletropaulo Metropolitana Eletricidade de São Paulo S/A é recorrente ou recorrida em 32 (trinta e dois) dos acórdãos encontrados, enquanto a ENEL Distribuição São Paulo S/A é em 3 (três) e a CPFL Companhia Piratininga de Força e Luz aparece em 1 (uma ocorrência.

Importante mencionar que as 2 (duas) primeiras companhias foram incorporadas após a compra da Eletropaulo pela Enel energia em 2018. Isso significa que quase 60% do gráfico que apresenta as empresas indicadas como agentes de tratamento de dados nos acórdãos proferidos nos Tribunais brasileiros nos 2 (dois) primeiros anos de vigência da LGPD é ocupado pela mesma empresa.

Alguns acórdãos em que as empresas de energia elétrica são os agentes de tratamento mencionam que, após a divulgação de uma reportagem sobre o vazamento de dados pessoais da empresa Eletropaulo Metropolitana Eletricidade De São Paulo S/A, foram ajuizadas diversas ações judiciais semelhantes, todas relacionadas ao mesmo incidente de segurança[136].

[136] TRIBUNAL DE JUSTIÇA DE SÃO PAULO. 10011381020218260176 SP 1001138-10.2021.8.26.0176, Relator: Daniel Torres Dos Reis, Data de Julgamento: 18/05/2022, 2ª Turma Cível, Criminal e Fazenda - Itapecerica da Serra, Data de Publicação: 27/05/2022.

É de conhecimento geral que a repercussão midiática dos acontecimentos possui muita influência na elaboração e aprovação de novas leis. A reformulação do Código Florestal Brasileiro em 2012, que foi precedida por uma ampla cobertura midiática sobre os impactos ambientais da agricultura e pecuária no país e a criação da Lei Maria da Penha, em 2006, que foi fortemente impulsionada pela mídia e pela mobilização da sociedade civil após o caso emblemático de Maria da Penha Maia Fernandes, são apenas alguns exemplos desse fenômeno.

Contudo, não é tão clara a influência que a mídia exerce sobre a tomada de decisão dos indivíduos sobre ajuizar ou não uma ação indenizatória ou na própria decisão dos julgadores acerca do deferimento de tais pedidos e na definição do quantum indenizatório.

No pequeno recorte desta pesquisa, nota-se que a divulgação do incidente de segurança em veículo de comunicação de grande repercussão foi um fator relevante para que o setor de energia elétrica ocupasse mais da metade dos recursos envolvendo casos de violação à proteção de dados.

É importante notar ainda que dos 55 (cinquenta e cinco) acórdãos analisados apenas 15 (quinze) contam com indenização por danos morais, sendo que, destes, apenas 1 (um) diz respeito aos casos em que as empresas de energia elétrica são agentes de tratamento, apesar destas representaram mais de 60% dos acórdãos analisados.

Apenas 2 (dois) acórdãos mencionam a violação a dados pessoais sensíveis (dados de saúde e sobre opinião política) e ambos resultaram em condenação de indenização por danos morais no valor de R$ 10.000,00 (dez mil reais)[137].

O valor médio da indenização por danos morais concedida é de R$ 5.833,33 (cinco mil oitocentos e trinta e três reais e trinta e três centavos), sendo que o valor mais alto concedido foi de R$ 20.000,00 em um caso envolvendo venda de dados pessoais e o mais baixo R$ 2.000,00 em 2 (dois) casos.

Dentre as decisões que não reconhecem o direito à indenização por danos morais, 40 (quarenta) acórdãos no total, as fundamentações mais recorrentes são: (i) a não demonstração de nexo de causalidade; (ii) a inexistência de danos concretos ou de danos efetivos aos direitos de personalidade; (iii) a violação aos dados representa mero dissabor e; (iv) dados vazados de pouca relevância ou de fácil acesso.

---

[137] TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Acórdão no Agravo de Instrumento nº 1049096-26.2021.8.26.0100. Relator: Pedro de Alcântara da Silva Leme Filho. Data de Julgamento: 04 de maio de 2022. 8ª Câmara de Direito Privado. Data de Publicação: 06 de maio de 2022. Disponível em: <https://cjo.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15646200&cdForo=0>. Acesso em: 19 jun. 2024.

O acórdão no Recurso Cível nº 5000339-43.2021.4.04.7127/RS negou provimento ao Recurso Inominado interposto pelo autor contra a decisão que julgou improcedentes os pedidos de condenação do Instituto Nacional de Seguridade Social - INSS ao pagamento de danos morais decorrentes da violação aos seus dados pessoais[138].

A decisão fundamentou a improcedência dos pedidos na ausência de nexo de causalidade entre o fato ocorrido (o vazamento de dados) e o dano provocado (o contato de diversas instituições financeiras oferecendo ao titular empréstimo consignado). Segundo a decisão:

> [...] o acervo probatório não permite concluir que o vazamento tenha ocorrido da base de dados do INSS. Na realidade, não há demonstração do nexo de causalidade entre a atividade de armazenamento dos dados pessoais da autora, pelo INSS, e a utilização dos referidos dados pessoais pelas pessoas jurídicas de direito privado que tentam convencê-lo a firmar contratos de empréstimo[139].

O acórdão não entra no mérito do modo com que os dados pessoais são tratados pelo INSS e não há discussão acerca da possível inversão do ônus probatório em favor do titular de dados pessoais. Quanto ao primeiro ponto, nota-se um esforço dos julgadores em identificar o nexo de causalidade entre o dano sofrido e a conduta específica do agente de tratamento que gerou o dano.

Na Apelação Cível nº 0006500-94.2021.8.19.0211, em que é Apelado o Banco do Brasil S/A, foi julgado improcedente o pedido da apelante (titular de dados) de condenação da instituição financeira pelo tratamento irregular de seus dados, em razão de ter sofrido uma tentativa de fraude por terceiros que detinham suas informações cadastrais junto ao banco[140].

A fundamentação utilizada foi de que a dinâmica dos acontecimentos não demonstrou se os dados pessoais vazados da titular (apelante) foram obtidos junto à instituição financeira ou outro agente de tratamento[141]. Esse entendimento demonstra uma típica aplicação da lógica tradicional da responsabilidade civil extracontratual. Ocorre que o nexo de causalidade nas

---

[138] TRIBUNAL REGIONAL FEDERAL DA 4ª REGIÃO. Acórdão no Recurso Cível nº 5000339-43.2021.4.04.7127. Relator: Andrei Pitten Velloso. Data de Julgamento: 16 de dezembro de 2021. Quinta Turma Recursal do RS. Disponível em: <https://consulta.trf4.jus.br/trf4/controlador.php?acao=consulta_processual_resultado_pesquisa&selForma=NU&txtValor=50003394320214047127&chkMostrarBaixados=S&todasfases=&todosvalores=&todaspartes=&txtDataFase=&selOrigem=RS&sistema=&txtChave=>. Acesso em: 15 de jun. 2024.

[139] Idem.

[140] TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. Acórdão no Apelação nº 0006500-94.2021.8.19.0211. Relator: Des(a). Luiz Felipe Miranda de Medeiros Francisco. Data de Julgamento: 31 de março de 2022. Nona Câmara Cível. Data de Publicação: 01 de abril de 2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-rj/1476846272>. Acesso em: 12 jun. 2024.

[141] Idem.

condutas lesivas aos dados pessoais não é tão simples de ser identificado como em outros tipos de danos ou relações jurídicas.

Por essa razão, o regime de responsabilidade trazido pela LGPD possui como uma das suas características a ênfase à conduta do agente de tratamento. O artigo 44 da referida Lei enfatiza que o tratamento de dados pessoais torna-se irregular quando o agente responsável não cumpre a legislação vigente ou falha em proporcionar a segurança adequada esperada pelo titular dos dados[142]. Isso inclui avaliar o modo como o tratamento é conduzido, os resultados previstos e os riscos envolvidos, considerando as técnicas disponíveis à época[143].

Na definição das sanções administrativas (art. 52 e seguintes), a Lei estabelece que a adoção de políticas de boas práticas e governanças são levadas em consideração para a determinação do quantum sancionatório[144].

A preocupação da LGPD em incentivar uma cultura de boas práticas no tratamento de dados pessoais considera principalmente a dificuldade que costuma ser identificar o agente de tratamento que efetivamente causou o dano ao titular de dados pessoais. Em muitos casos, considerando que diversos agentes tratam os mesmos dados pessoais de um titular simultaneamente, é extremamente difícil e oneroso identificar de onde efetivamente um dado pessoal específico vazou, por exemplo. O tratamento de dados pessoais na internet, ao contrário de outras condutas tradicionalmente contempladas pela responsabilidade civil, não deixam facilmente rastros para fins de prova aptos a identificar a conduta e o causador do dano[145].

Um exemplo hipotético que é capaz de ilustrar essa questão é o seguinte: Imagine que um determinado titular de dados pessoais tenha suas informações vazadas na internet devido a um incidente de segurança. Esses dados foram coletados e tratados por várias empresas diferentes ao longo do tempo, incluindo redes sociais, serviços de *e-commerce* e provedores de serviços online. Após o vazamento, o titular enfrenta problemas sérios de fraudes financeiras e comprometimento de sua privacidade.

Diante deste cenário, identificar qual agente de tratamento efetivamente causou o vazamento pode ser desafiador. As informações pessoais do titular foram compartilhadas e

---

[142] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 16 jun. 2024.

[143] Idem.

[144] Ibidem, at. 52.

[145] SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. Revista Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021. DOI: 10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 26 jun. 2024.

processadas por múltiplos agentes de tratamento, cada um com seus próprios sistemas de segurança e protocolos de proteção de dados. A falta de rastreabilidade dificulta determinar precisamente de onde ocorreu o vazamento inicial e quem foi o responsável direto pelo incidente.

Essa complexidade ilustra a importância das regras de boas práticas e governança estabelecidas pela LGPD. É essencial que todos os agentes de tratamento envolvidos no tratamento de dados adotem medidas rigorosas de segurança e estejam preparadas para responder de maneira adequada a incidentes de segurança, mesmo quando o dano é resultado da ação conjunta de vários agentes de tratamento.

A decisão no Recurso Inominado de nº 0160075-63.2021.8.05.0001 em sentido diverso ao acórdão supramencionado, firmou entendimento de que a ação de um terceiro fraudador não afasta o nexo causal entre a conduta do agente de tratamento que realizou o tratamento irregular de dados e o dano sofrido pelo titular[146]. Isso porque, "os danos causados ao lesado advêm diretamente do incremento do risco criado pela lucrativa atividade desenvolvida pelas instituições financeiras"[147].

Nesse mesmo sentido, na Apelação Cível de nº 1025180-52.2020.8.26.0405, os julgadores entenderam que os sistemas envolvidos no incidente eram seguros e adotavam as melhores práticas de segurança disponíveis, além de estarem em conformidade com as exigências legais da LGPD[148]. Sob a fundamentação supramencionada, foi atribuída a culpa ao terceiro fraudador para romper o nexo de causalidade, isentando o agente de tratamento da responsabilidade pelo dano[149]. Nota-se que a ênfase na definição da responsabilidade não foi a conduta do agente de tratamento em relação ao dano sofrido pelo titular, mas sim no modo com que usualmente o agente trata os dados pessoais.

Outras decisões reconhecem o tratamento irregular de dados pelo agente de tratamento, em violação à LGPD, mas indeferem o pedido de indenização ao titular de dados, sob a fundamentação de inexistência de danos concretos ou de danos efetivos aos direitos de personalidade.

---

[146] BRASIL. Tribunal de Justiça da Bahia. Recurso Inominado n.º 01600756320218050001. Relator: Mary Angelica Santos Coelho. Quarta Turma Recursal. Data de publicação: 18 jul. 2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ba/1581087053/inteiro-teor-1581087056>. Acesso em: 19 jun. 2024.

[147] Idem.

[148] BRASIL. Tribunal de Justiça de São Paulo. Apelação Cível n.º 1025180-52.2020.8.26.0405. Relator: Arantes Theodoro. 36ª Câmara de Direito Privado. Data de julgamento: 26 ago. 2021. Data de publicação: 26 ago. 2021. Disponível em: <https://cjo.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14957864&cdForo=0>. Acesso em: 19 jun. 2024.

[149] Idem.

No julgamento do Recurso Inominado de nº 1024060-71.2020.8.26.0405, ajuizado pelo titular de dados vazados pela Enel Distribuidora São Paulo, firmou o entendimento de que "não basta a ação negligente da ré para ensejar indenização, mas também o efetivo dano, que deve ser comprovado, não havendo que se falar em presunção"[150].

O teor de tais decisões levanta questionamentos acerca de quais danos são efetivamente tutelados pela LGPD. Apenas os danos materiais e morais foram tutelados, tal como no Código de Defesa do Consumidor? A violação ao direito à autodeterminação informativa pode ser indenizada? A responsabilização civil pelo tratamento irregular de dados está condicionada à violação de direitos de personalidade?

Quanto aos danos materiais, observou-se dos acórdão analisados que em grande parte das decisões em que houve condenação por danos materiais (oito acórdãos no total) a efetiva indenização fundamentou-se em outros dispositivos legais e não na LGPD.

Nos Recursos Inominados Civeis de nº 0715585-63.2020.8.07.0007[151], nº 0160075-63.2021.8.05.0001[152], nº 0040126-45.2021.8.05.0001[153], nº 0004533-05.2021.8.05.0146[154], nº 0000354-53.2022.8.05.0191[155] e na Apelação Cível de nº 0007499-94.2021.8.19.0066[156], a fundamentação para fixação da indenização por danos materiais por fraude aplicada a partir do uso indevido de dados pessoais do titular adveio da Súmula 479 do STJ, que dispõe que "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". Muito embora sejam utilizados dispositivos da LGPD para a

---

[150] BRASIL. Tribunal de Justiça de São Paulo. Recurso Inominado n.º 1024060-71.2020.8.26.0405. Relator: Mariana Parmezan Annibal. 2ª Turma Cível. Data de julgamento: 25 jun. 2021. Data de publicação: 25 jun. 2021. Disponível em: <https://cjo.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=1281920&cdForo=9015> Acesso em: 16 jun. 2024.

[151] BRASIL. Tribunal de Justiça do Distrito Federal. Recurso Inominado n.º 0715585-63.2020.8.07.0007. Relator: Arnaldo Corrêa Silva. Segunda Turma Recursal. Data de julgamento: 22 nov. 2021. Data de publicação: 1 dez. 2021. Disponível em: <https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj>. Acesso em: 16 jun. 2024.

[152] BRASIL. Tribunal de Justiça da Bahia. Recurso Inominado n.º 01600756320218050001. Relatora: Mary Angelica Santos Coelho. Quarta Turma Recursal. Data de publicação: 18 jul. 2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ba/1581087053/inteiro-teor-1581087056>. Acesso em: 16 jun. 2024.

[153] BRASIL. Tribunal de Justiça da Bahia. Recurso Inominado n.º 00401264520218050001. Relatora: Mary Angelica Santos Coelho. Quarta Turma Recursal. Data de publicação: 14 jul. 2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ba/1576546003> Acesso em: 19 jun. 2024.

[154] BRASIL. Tribunal de Justiça da Bahia. Recurso Inominado n.º 00045330520218050146. Relatora: Mary Angelica Santos Coelho. Quarta Turma Recursal. Data de publicação: 29 jun. 2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ba/1560881450>. Acesso em: 16 jun. 2024.

[155] BRASIL. Tribunal de Justiça da Bahia. Recurso Inominado n.º 00003545320228050191. Relatora: Mary Angelica Santos Coelho. Quarta Turma Recursal. Data de publicação: 01 ago. 2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-ba/1597901518>. Acesso em: 16 jun. 2024.

[156] BRASIL. Tribunal de Justiça do Rio de Janeiro. Apelação n.º 00074999420218190066. Relator: Des(a). Humberto Dalla Bernardina de Pinho. Data de julgamento: 29 jun. 2022. Vigésima Quarta Câmara Cível. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/1562593815>. Acesso em: 16 jun. 2024.

demonstração dos atos ilícitos cometidos em relação ao tratamento de dados, o regime de responsabilidade adotado é o do CDC. As demais decisões, os Recurso Inominados de nº 0183387-68.2021.8.05.0001[157] e nº 0149420-32.2021.8.05.0001[158], fundamentam-se tão somente nos dispositivos da LGPD para determinar a condenação em indenização por danos materiais.

É importante mencionar que, nos acórdãos em que houve condenação por danos materiais, apenas um dos agentes de tratamento não é uma instituição financeira. Isso demonstra uma predominância de condenações por danos materiais relacionadas ao tratamento irregular de dados entre as instituições financeiras.

Percebe-se, portanto, que mesmo nos casos em que a LGPD é citada, a fundamentação jurídica para a responsabilidade e indenização por danos materiais ainda depende fortemente de outros regimes legais, como o CDC. Este fato destaca a importância de uma interpretação mais clara e consistente da LGPD em relação à responsabilização por danos.

Em relação aos danos imateriais, é recorrente nas decisões que rejeitam a indenização por danos morais a fundamentação de inexistência de danos concretos ou de danos efetivos aos direitos de personalidade do titular. Em outras palavras, tais decisões condicionam a responsabilização à ocorrência de danos materiais ou à ocorrência de violação a algum direito de personalidade. O acórdão proferido nos autos da Apelação Cível nº 1008308-35.2020.8.26.0704[159], decidiu que:

> Ausência de provas, todavia, de violação à dignidade humana do autor e seus substratos, isto é, liberdade, igualdade, solidariedade e integridade psicofísica. Autor que não demonstrou, a partir do exame do caso concreto, que, da violação a seus dados pessoais, a ocorrência de danos morais. Dados que não são sensíveis e são de fácil acesso a qualquer pessoa[160].

O acórdão na Apelação Cível nº 1000580-66.2021.8.26.0005, em sentido parecido, indeferiu a condenação em danos morais pleiteada pelo titular sob o fundamento de que, embora tenha havido irregularidade no tratamento dos dados pessoais do autor, não há provas

---

[157] BRASIL. Tribunal de Justiça da Bahia. Recurso Inominado n.º 01833876820218050001. Relatora: Mary Angelica Santos Coelho. Quarta Turma Recursal. Data de publicação: 22 abr. 2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/1471609557>. Acesso em: 17 jun. 2024.

[158] BRASIL. Tribunal de Justiça da Bahia. Recurso Inominado n.º 01494203220218050001. Relatora: Mary Angelica Santos Coelho. Quarta Turma Recursal. Data de publicação: 22 abr. 2022. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/1471604865>. Acesso em: 17 jun. 2024.

[159] BRASIL. Tribunal de Justiça de São Paulo. Apelação Cível n.º 1008308-35.2020.8.26.0704. Relator: Alfredo Attié. 27ª Câmara de Direito Privado. Data de julgamento: 16 nov. 2021. Data de publicação: 16 nov. 2021. Disponível em: <https://cjo.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15191762&cdForo=0>. Acesso em: 17 jun. 2024.

[160] Idem.

de transtornos significativos ou uso indevido das informações que configurem dano moral indenizável[161]. *In verbis*:

> Sem razão, contudo, o apelante, não se podendo dizer, pelas informações disponíveis nos autos, tenha ele passado por um nível tal de transtorno que ultrapasse a barreira do mero aborrecimento e resvale para o plano da ofensa efetiva a valores da personalidade. Não há nos autos, com efeito, sequer prova das perturbações de que teria o autor sido alvo após o vazamento dos dados, como mensagens e ligações telefônicas, citadas na narrativa padronizada da petição inicial. Inexiste, ademais, qualquer notícia de que tenha ele sido vítima de fraude pelo uso das informações correspondentes[162].

São recorrentes  nas fundamentações a negativa de indenização por danos morais ante a inocorrência ou não demonstração de ofensa aos direitos de personalidade, como à honra, à imagem, à intimidade, etc.

Na Apelação Cível nº 1000580-66.2021.8.26.0005[163], julgada pelo Tribunal de Justiça de São Paulo, em que é apelada a Eletropaulo Metropolitana Eletricidade De São Paulo S/A, o acórdão indeferiu a indenização por danos morais com base na ausência de provas suficientes nos autos que demonstrassem que o titular sofreu danos emocionais ou psicológicos significativos em decorrência do vazamento de seus dados pessoais. As alegações apresentadas não foram consideradas suficientes para ultrapassar o limite do mero aborrecimento e configurar uma ofensa aos direitos da personalidade, como a honra e a intimidade.

Em sentido parecido tem compreendido os Tribunais Europeus quanto à compensação por danos não materiais decorrentes de violação ao GDPR. A *Österreichische Post* é a empresa responsável pelo serviço postal na Áustria e vem coletando informações pessoais de milhões de cidadãos do país desde 2017[164]. Constatou-se que a empresa utilizava algoritmos para estimar a afinidade dos titulares com diferentes partidos políticos com base em características sociodemográficas, para fins de gerar publicidade direcionada[165].

Um usuário irresignado com o fato de ter tido seus dados pessoais tratados para tal finalidade ajuizou uma ação perante o Landesgericht für Zivilrechtssachen Wien (Tribunal

---

[161] BRASIL. Tribunal de Justiça de São Paulo. Apelação Cível n.º 1000580-66.2021.8.26.0005. Relator: Fabio Tabosa. 29ª Câmara de Direito Privado. Data de julgamento: 10 nov. 2021. Data de publicação: 12 nov. 2021. Disponível em: <https://cjo.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15186143&cdForo=0>. Acesso em: 17 jun. 2024.
[162] Idem.
[163] Idem.
[164] LI, Shu. Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. Maastricht Journal of European and Comparative Law, v. 30, n. 3, p. 335-345, 2023. Disponível em: https://doi.org/10.1177/1023263X231208835. Acesso em: 27 jun. 2024.
[165] Idem.

Regional de Assuntos Civis em Viena), na qual requer a procedência de uma liminar a fim de cessar o tratamento dos seus dados pessoais e uma compensação de 1000 euros pelos danos não materiais sofridos[166]. O caso foi levado ao Supremo Tribunal da Áustria e o Tribunal decidiu por suspender o processo e remeter três questões ao Tribunal de Justiça da União Europeia:

> The three questions are: (1) does the award of compensation under Article 82 of [the GDPR] also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation? (2) Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence? (3) Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence [or effect] of the infringement of at least some weight that goes beyond the upset caused by that infringement?[167]

Basicamente, em tradução livre, as perguntas remetidas ao Tribunal de Justiça da União Europeia buscam responder: (i) Se a concessão de compensação nos termos do Artigo 82 do GDPR exige, além da violação das disposições do GDPR, que o requerente tenha sofrido um dano, ou se a violação das disposições do GDPR por si só é suficiente para a concessão de compensação; (ii) Se a avaliação da compensação depende de requisitos adicionais da legislação da UE além dos princípios de eficácia e equivalência; (iii) Se é compatível com a legislação da UE considerar que a concessão de compensação por danos não materiais pressupõe a existência de uma consequência ou efeito da infração de pelo menos algum peso que vá além do aborrecimento causado por essa infração[168].

O Tribunal de Justiça da União Europeia, proferiu julgamento, respondendo aos questionamentos encaminhados. Em resposta à primeira questão, o Tribunal concluiu que "não se pode considerar que toda e qualquer «violação» das disposições do RGPD confere, por si só, o referido direito de indemnização em benefício do titular dos dados, conforme definido no artigo 4.o, ponto 1, deste regulamento"[169], isto é, a indenização só pode ser concedida em caso de danos concretos.

---

[166] UNIÃO EUROPEIA. Tribunal de Justiça. Case C-300/21, UI v. Österreichische Post AG. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3020662. Acesso em: 27 jun. 2024.

[167] LI, Shu. Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. Maastricht Journal of European and Comparative Law, v. 30, n. 3, p. 335-345, 2023. Disponível em: https://doi.org/10.1177/1023263X231208835. Acesso em: 27 jun. 2024.

[168] Idem.

[169] UNIÃO EUROPEIA. Tribunal de Justiça. Case C-300/21, UI v. Österreichische Post AG. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3020662. Acesso em: 27 jun. 2024.

Quanto ao segundo questionamento, o Tribunal entendeu que a indenização deve observar as normas internas de cada Estado-Membro e não apenas os princípios da eficácia e equivalência, *in verbis*:

> 53 A este respeito, importa recordar que, em conformidade com jurisprudência constante, na falta de regras da União na matéria, cabe à ordem jurídica interna de cada Estado‑Membro estabelecer as regras processuais das ações judiciais destinadas a garantir a salvaguarda dos direitos dos particulares, ao abrigo do princípio da autonomia processual, desde que essas regras não sejam, nas situações abrangidas pelo direito da União, menos favoráveis do que as que regulam situações semelhantes submetidas ao direito interno (princípio da equivalência) e não tornem impossível, na prática, ou excessivamente difícil o exercício dos direitos conferidos pelo direito da União (princípio da efetividade) (v., neste sentido, Acórdãos de 13 de dezembro de 2017, El Hassani, C‑403/16, EU:C:2017:960, n.o 26, e de 15 de setembro de 2022, Uniqa Versicherungen, C‑18/21, EU:C:2022:682, n.o 36). 54 No caso em apreço, há que salientar que o RGPD não contém nenhuma disposição que tenha por objeto definir as regras relativas à avaliação da indemnização por perdas e danos a que um titular dos dados, na aceção do artigo 4.o, ponto 1, deste regulamento, pode invocar, ao abrigo do artigo 82.o, quando a violação do referido regulamento lhe causou um dano. Por conseguinte, na falta de regras do direito da União na matéria, cabe à ordem jurídica de cada Estado‑Membro fixar as modalidades das ações destinadas a garantir a salvaguarda dos direitos conferidos aos litigantes por esse artigo 82.o, em particular, os critérios que permitem determinar o alcance da indemnização devida nesse âmbito, sem prejuízo do respeito dos referidos princípios da equivalência e da efetividade (v., por analogia, Acórdão de 13 de julho de 2006, Manfredi e o., C‑295/04 a C‑298/04, EU:C:2006:461, n.os 92 e 98)[170].

A respeito da terceira questão, o Tribunal entendeu que o artigo 82 º, nº 1, do RGPD se opõe a qualquer norma ou prática nacional que subordine a indenização por dano imaterial à condição de que o dano atinja um certo grau de gravidade[171]. Tal entendimento garante que qualquer dano, independentemente de sua gravidade, seja potencialmente indenizado, promovendo uma proteção uniforme e eficaz dos direitos dos titulares dos dados em toda a União Europeia.

A aplicação da LGPD condicionada exclusivamente à violação dos direitos de personalidade, como honra e intimidade, para se justificar a reparação por danos morais, contudo, merece ser repensada. A LGPD visa proteger não apenas os direitos de personalidade, mas principalmente a privacidade e a segurança dos dados pessoais dos indivíduos, independentemente de ter havido uma ofensa direta a esses direitos específicos.

A legislação estabelece princípios e diretrizes para o tratamento adequado e seguro dos dados pessoais, garantindo que sejam coletados, armazenados e utilizados de maneira

[170] Idem.
[171] Idem.

consentida e segura. Isso significa que a simples ocorrência de um vazamento de dados já configura uma violação à LGPD, independentemente de o titular dos dados ter sofrido danos emocionais ou psicológicos comprovadamente significativos.

Portanto, a aplicação da LGPD não se restringe à proteção dos direitos de personalidade no sentido estrito, como a honra e a intimidade, mas abrange a proteção da privacidade dos dados e autodeterminação do titular sobre eles. Mesmo que não haja prova de danos emocionais ou psicológicos diretos, a ocorrência do vazamento de dados pessoais por si só já representa uma violação à privacidade e à segurança dessas informações, justificando medidas reparatórias ou punitivas conforme previsto na lei.

Assim, compreende-se que a proteção dos dados pessoais e a responsabilidade por sua segurança são deveres que transcendem a mera violação aos direitos de personalidade, refletindo um compromisso mais amplo com a proteção da privacidade dos indivíduos em um contexto digital cada vez mais complexo e vulnerável.

Nesse sentido, é importante lembrar que a proteção de dados foi inserida no rol de direitos fundamentais do art. 5º da Constituição Federal, por intermédio da Emenda Constitucional nº 115 de 10 de fevereiro de 2022. Vale a pena rememorar que o § 1º do art. 5º da Constituição dispõe que "as normas definidoras dos direitos e garantias fundamentais têm aplicação imediata"[172].

Ao incluir a proteção de dados no âmbito dos direitos fundamentais, a Constituição Federal reafirma a necessidade de que esses direitos sejam respeitados e protegidos de forma imediata e efetiva. Isso significa que as normas da LGPD, que regulam o tratamento de dados pessoais e estabelecem medidas de segurança e privacidade, têm aplicação direta e podem ser invocadas perante o Poder Judiciário para garantir a proteção dos direitos dos indivíduos.

A aplicação imediata das normas de proteção de dados não se restringe apenas a casos onde há violações diretas aos direitos de personalidade, como honra e intimidade. Ela abrange qualquer situação em que haja um tratamento inadequado ou não consentido dos dados pessoais, incluindo vazamentos de informações sensíveis que possam comprometer a privacidade e a segurança dos indivíduos.

Portanto, a LGPD não apenas estabelece direitos e deveres para os agentes que tratam dados pessoais, mas também proporciona uma base legal robusta para que os titulares de dados possam exigir a proteção de seus direitos, independentemente de terem sofrido danos

---

[172] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 19 jun. 2024.

morais específicos. A simples violação dos princípios e diretrizes estabelecidos na legislação já configura uma infração que pode resultar em sanções administrativas e reparatórias, conforme previsto na própria lei.

Mais uma vez, uma interpretação restrita do regime de responsabilidade civil levando-se em conta a sua tradicional aplicação a outras áreas do direito não colabora com o debate no âmbito da proteção de dados pessoais, campo com peculiaridades e especificidades do mundo globalizado e digital[173].

Em sentido contrário à maioria das decisões que indeferiram a condenação por danos morais, o acórdão proferido nos do Recurso Inominado nº 0002183-58.2021.8.26.0405 que a divulgação dos dados pessoais do titular sem o seu consentimento gera, em tese, dano moral *in re ipsa*[174].

Percebe-se novamente a visão binária dos magistrados acerca da responsabilidade civil, como se as únicas possibilidades possíveis fossem ou o indeferimento da indenização por ausência de danos morais ou o reconhecimento do dano moral *in re ipsa*.

É recorrente nas decisões a fundamentação de que os dados vazados são de pouca relevância ou de fácil acesso, fazendo com que o vazamento não represente um prejuízo relevante o suficiente para gerar o dever de indenizar.

Apesar de ter reconhecido, no julgamento da Apelação Cível nº 1008308-35.2020.8.26.0704[175], do TJSP, em que é apelada a Eletropaulo Metropolitana Eletricidade De São Paulo S/A, que é "incontroverso, dos autos, que o autor teve dados pessoais não sensíveis (nome, número de CPF, data de nascimento, idade, telefones fixo e celular e endereço de e-mail) expostos indevidamente pela ré", o acórdão indeferiu o pedido de indenização por danos morais sob a fundamentação de que os dados vazados se referem a informações essencialmente públicas ou de fácil acesso por terceiros. *In verbis:*

> Os dados vazados, no caso, dizem respeito a informações essencialmente públicas ou de fácil acesso a terceiros, isto é, nome, CPF, data de nascimento e idade. Quanto aos números de telefone fixo e celular, bem como o endereço de e-mail, muito embora tais informações não sejam, em regra, de

---

[173] Šidlauskas, A. (2021). The Role and Significance of the Data Protection Officer in the Organization. Sociedade e Tecnologia, 44(1), 8–28. p. 11. Disponível em: https://doi.org/10.15388/Soctyr.44.1.1. Acesso em: 21 jun. 2024.

[174] BRASIL. Tribunal de Justiça de São Paulo. Apelação Cível n.º 1000580-66.2021.8.26.0005. Relator: Fabio Tabosa. 29ª Câmara de Direito Privado. Data de julgamento: 10 nov. 2021. Data de publicação: 12 nov. 2021. Disponível em: <https://cjo.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15186143&cdForo=0>. Acesso em: 17 jun. 2024.

[175] BRASIL. Tribunal de Justiça de São Paulo. Apelação Cível n.º 1000580-66.2021.8.26.0005. Relator: Fabio Tabosa. 29ª Câmara de Direito Privado. Data de julgamento: 10 nov. 2021. Data de publicação: 12 nov. 2021. Disponível em: <https://cjo.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15191762&cdForo=0>. Acesso em: 17 jun. 2024.

> caráter público, também não revelam qualquer dado sensível ou que, por si só, possa comprometer a dignidade do autor, caso de conhecimento público. Eventual recebimento de mensagens ou incômodo, embora não mereça menosprezo, é fato que cabe ser imputado a seus causadores, e se for o caso de admitir-se qualquer reparo nesse sentido[176].

Nesse sentido, é importante lembrar que a LGPD possui como um dos seus principais fundamentos proteger os direitos fundamentais de liberdade e privacidade[177]. A proteção dos dados pessoais é um direito garantido pela Constituição, independentemente da suposta relevância ou da facilidade de acesso aos dados. Desse modo, compreende-se que qualquer violação desse direito é uma afronta à autodeterminação informativa, à dignidade e à privacidade do titular. A lei não diferencia os dados com base na sua importância ou facilidade de acesso, mas na responsabilidade dos manipuladores de dados em garantir a segurança e proteção dos dados.

Além disso, a argumentação de que os dados são de pouca relevância é subjetiva e pode variar de caso a caso. Informações que parecem insignificantes para alguns podem ser extremamente sensíveis para outros e podem vir a causar danos ao titular. Por exemplo, um número de telefone ou um endereço de e-mail, que podem parecer dados simples, podem ser usados para fins de uma série de fraudes. Além disso, a agregação de dados que individualmente podem parecer triviais pode levar a perfis detalhados e invasivos sobre os indivíduos, expondo-os a riscos como discriminação, roubo de identidade e outras violações de seus direitos.

Outro ponto importante a ser destacado consiste no fato de que a LGPD impõe aos responsáveis pelo tratamento de dados a obrigação de implementar medidas de segurança adequadas para proteger esses dados contra acessos não autorizados e outras formas de tratamento inadequado.

A falha em proteger qualquer tipo de dado, mesmo que seja considerado como de "fácil acesso", demonstra uma falta de diligência e responsabilidade que a Lei busca corrigir e penalizar. A existência de um vazamento de dados é, por si só, um indicativo de que os padrões de segurança e proteção não foram seguidos adequadamente.

Ademais, minimizar a importância de determinados dados pode criar um perigoso precedente de complacência no tratamento de dados pessoais. Isso pode encorajar

---

[176] Idem.

[177] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 18 jun. 2024.

organizações a desconsiderarem suas obrigações legais e a adotarem práticas inadequadas de segurança, aumentando a probabilidade de novos incidentes de vazamento de dados. Tal postura vai contra o espírito da LGPD, que busca fomentar uma cultura de proteção de dados pessoais e responsabilização por parte das organizações.

Assim, o argumento de que os dados vazados não são muito importantes ou de fácil acesso não é suficiente para rejeitar a indenização por violação da LGPD. Isso porque, a Lei foi criada para proteger todos os dados pessoais, independentemente da percepção das pessoas acerca da sua importância, bem como para garantir que as organizações adotem medidas adequadas de proteção e segurança, respeitando os direitos fundamentais dos indivíduos.

O Tribunal Constitucional Federal Alemão, no caso Volkszählungsurteil (Censo Alemão), afirmou que não há dados pessoais sem importância, uma vez que a relevância de uma informação não depende apenas se ela atinge a intimidade, mas do contexto e das possibilidades da sua utilização desses dados[178]. Nesse sentido:

> O Tribunal esclarece que, para poder limitar o direito à autodeterminação informativa, deve-se considerar todas as possibilidades de utilização e combinação das informações na análise da proporcionalidade, e não o grau de "intimidade" da informação em si. Para Limbeck, mesmo que não exista um dado sem importância, há um núcleo da personalidade que é intocável pelo poder público. Por isso, ainda que o direito à autodeterminação informativa possa ser limitado quando o interesse público superar o privado, as restrições devem obedecer ao critério da proporcionalidade. De qualquer forma, qualquer utilização de dados pessoais pelo Estado deverá ser justificada e acompanhada de regras para a proteção do indivíduo[179].

Mais uma vez nota-se a tendência errônea por parte dos julgadores de compreenderam a proteção dos dados pessoais tão somente sob o aspecto da proteção dos direitos de personalidade, como se a única função da proteção de dados pessoais fosse proteger os tais direitos[180].

---

[178] ALEMANHA. Tribunal Constitucional Federal. Volkszählungsurteil - BVerfGE 65, 1. 15 de dezembro de 1983. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 28 jun. 2024.

[179] CUNHA, Anita Spies da; SCHIOCCHET, Taysa. A constitucionalidade do DNA na persecução penal: o direito à autodeterminação informativa e o critério de proporcionalidade no Brasil e na Alemanha. The constitutionality of DNA in criminal prosecution: the right to informative self-determination and the proportionality criterion in Brazil and Germany. Revista de Investigação Constitucional, Curitiba, v. 8, n. 2, p. 529-554, maio/ago. 2021. DOI: https://revistas.ufpr.br/rinc/article/view/74420. Acesso em: 27 jun. 2024.

[180] SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. Revista Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021. DOI: 10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 26 jun. 2024.

## 3.2 Análise dos acórdãos do Superior Tribunal de Justiça

Além das decisões dos Tribunais de Justiça brasileiros, o Superior Tribunal de Justiça - STJ possui em seu banco de dados de acórdãos 8 (oito) decisões colegiadas nos quais a LGPD consta como referência legislativa. Para a pesquisa de tais acórdãos, foi inserido, no sistema de pesquisas do STJ, no campo "Pesquisa por campos específicos", o filtro "legislação" e escolhida a norma "LGPD-2018", a qual resultou em 8 (oito) acórdãos[181].

O Recurso Especial nº 2.077.278 - SP traz uma discussão mais aprofundada acerca da identificação do nexo de causalidade entre o vazamento de dados pessoais pela instituição financeira recorrida e a fraude cometida por estelionatários que ocasionaram prejuízos materiais à recorrente[182].

Os autos de origem tratam de ação declaratória de inexigibilidade de débitos por vazamento de dados bancários. A titular dos dados pessoais e recorrente foi vítima de um golpe praticado por estelionatários que, de posse de seus dados pessoais e informações sigilosas sobre seu financiamento bancário junto à recorrida, emitiram boletos falsos e os enviaram à recorrente, que efetuou os pagamentos[183].

A titular ajuizou a ação declaratória de inexigibilidade de débito por vazamento de dados bancários, cumulada com indenização por danos morais e repetição de indébito, contra BV Financeira S/A. A sentença de primeira instância foi favorável à recorrente, validando o pagamento realizado com o boleto falso e ordenando a devolução das parcelas pagas após 23/10/2019, com correção e juros[184].

No entanto, em apelação, o Tribunal de Justiça de São Paulo reformou a sentença e julgou improcedentes os pedidos da recorrente, alegando que o golpe do boleto ocorreu por falta de diligência dela e que não houve falha na prestação de serviços da financeira. Insatisfeita, a titular interpôs recurso especial, sustentando que houve violação de diversos artigos do Código Civil e da LGPD, argumentando que o golpe foi facilitado pelo vazamento de seus dados pessoais pela BV Financeira[185]. O acórdão, sob a relatoria da ministra Nancy Andrighi, conheceu do recurso especial e lhe deu provimento, mantendo a decisão de

---

[181] BRASIL. Superior Tribunal de Justiça (STJ). Jurisprudência do STJ. Disponível em: https://processo.stj.jus.br/SCON/. Acesso em: 25 jun. 2024.
[182] BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 2.077.278 - SP (2023/0190979-8). Relatora: Ministra Nancy Andrighi. Recorrente: Daniela Ferreira Ramos. Recorrido: BV Financeira S.A. Crédito Financiamento e Investimento. Disponível em: https://processo.stj.jus.br/SCON/. Acesso em: 10 jun. 2024.
[183] Idem.
[184] Ibidem, p. 2.
[185] Idem.

primeiro grau e condenando a instituição financeira pelos prejuízos decorrentes da fraude sofrida pela recorrente.

Segundo o entendimento da Terceira Turma, na ausência de elementos concretos que evidenciem o nexo causal entre o vazamento de dados pessoais e a fraude cometida por estelionatários, não se pode sustentar a imputação de responsabilidade às instituições financeiras pelo vazamento de informações utilizadas por criminosos para a execução de fraudes.

Contudo, considerou que os dados sobre as operações financeiras deveriam ser tratados somente pelas instituições financeiras e o fato de os fraudadores terem acesso a tais informações coloca em xeque o adequado tratamento dos dados pessoais dos titulares pela instituição, *in verbis*:

> Por outro lado, os dados sobre operações financeiras são, em regra, presumivelmente de tratamento exclusivo pelas instituições financeiras. No ponto, a Lei Complementar 105/2001 estabelece que "as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados" (art. 1º), constituindo dever jurídico dessas entidades "não revelar, salvo justa causa, as informações que venham a obter em virtude de sua atividade profissional" (FURLAN, Fabiano Ferreira. Sigilo Bancário. Belo Horizonte: Fórum, 2008. p. 21-22). 15. Portanto, dados pessoais vinculados a operações e serviços bancários são sigilosos e cujo tratamento com segurança é dever das instituições financeiras. Desse modo, seu armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento dessas informações e causem prejuízos ao consumidor, configura falha na prestação do serviço (art. 14 do CDC e 43 da LGPD)[186].

A identificação do nexo de causalidade entre a conduta do agente de tratamento e os danos ao titular dos dados certamente é um elemento importante a ser analisado nesse contexto. No entanto, a simples fundamentação de que o nexo causal não foi identificado porque os dados são de fácil acesso ou porque houve vazamentos anteriores destes mesmos dados, como visto em decisões anteriores, representa uma interpretação inadequada da responsabilidade das instituições financeiras.

O acórdão no O REsp. nº 2.077.278, demonstra como o tratamento irregular dos dados que deveriam ser tratados em sigilo pela instituição financeira afetou diretamente os direitos e interesses do titular das informações que sofreu a fraude. Muito embora não tenha sido identificado como ou quando esses dados foram vazados e a extensão da culpa dos agentes de tratamento no vazamento, a decisão reconhece o nexo causal pelo simples fato de que os dados não deveriam ter sido acessados por terceiros, tendo em vista a sua natureza sigilosa.

---

[186] Ibidem, p. 9.

Percebe-se que há um desvio no foco da conduta que gerou o dano para a responsabilidade das instituições financeiras em proteger adequadamente os dados pessoais de seus clientes.

A responsabilidade, portanto, não se limita apenas à identificação do exato momento ou forma do vazamento, mas sim à obrigação das instituições financeiras de implementar medidas eficazes de segurança para proteger as informações confidenciais de seus clientes[187]. Nesse sentido, a decisão reforça, seguindo a linha de governança de dados fortemente incentivada na LGPD, a importância de uma gestão responsável e segura dos dados pessoais, capaz de garantir a integridade e a confiança nas relações entre as instituições financeiras e seus clientes.

Em sentido diverso compreenderam os julgadores do REsp nº 1.995.458 - SP, de relatoria da ministra Nancy Andrighi, que firmou o entendimento de que para atribuir a responsabilidade das instituições financeiras pelo vazamento de dados pessoais, é essencial assegurar que a origem do incidente ocorreu no sistema bancário, *in verbis*:

> 20. Como ensina a jurista Laura Schertel Mendes, a Lei Geral de Proteção de Dados inaugura um modelo ex-ante de proteção de dados (MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: os dois lados de uma mesma moeda. Internet & Regulação. coords.: Laura Schertel Mendes, Sérgio Garcia Alves, Danilo Doneda. - São Paulo: Saraiva Educação, 2021.) Nesta perspectiva, o legislador criou uma série de deveres de conduta que impactarão na mensuração da responsabilidade dos agentes em eventual vazamento de dados. 21. Assim, a Lei Geral de Proteção de Dados destina-se a indicar a responsabilidade dos agentes que detêm dados pessoais que foram vazados, importando as medidas adotadas para evitar este vazamento, conforme estabelecidos nos artigos 43 e 44, da LGPD. 22. Notório, portanto, que a fim de imputar a responsabilidade das instituições financeiras no que tange ao vazamento de dados pessoais, deve-se garantir que a origem do vazamento foi o sistema bancário, bem como observar se as devidas medidas protetivas quanto aos dados pessoais sob domínio da instituição financeira foram adotadas[188].

O acórdão do AREsp nº 2.130.619 - SP traz luz sobre um importante questionamento para a responsabilidade civil em proteção de dados, afirmando que o rol trazido pela LGPD em seu art. 5º, II, é taxativo ao determinar quais são os dados pessoais sensíveis[189]. Em

---

[187] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.995.458 - SP (2022/0097188-3). Relatora Ministra Nancy Andrighi. Recorrente: Reginald Jose Costa. Recorridos: Itaú Unibanco S.A.; Banco Itaucard S.A. Ementa. Disponível em: <https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202200971883&dt_publicacao=18/08/2022>. Acesso em: 26. jun. 2024.

[188] Idem.

[189] BRASIL. Superior Tribunal de Justiça. Agravo em Recurso Especial nº 2.130.619 - SP (2022/0152262-2). Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravado: Maria Edite de Souza. Relator: Ministro Francisco Falcão. Brasília, DF: Superior Tribunal de Justiça, 2022. Disponível em: <https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023>. Acesso em: 26 jun. 2024.

sentido contrário ao entendimento trazido pelo julgado, o acórdão reformado afirmava que alguns dados não listados no art. 5º, inciso II, da LGPD eram dados pessoais sensíveis. Segundo a Lei supracitada:

> Art. 5º Para os fins desta Lei, considera-se:
>
> [...]
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Os dados pessoais sensíveis são especialmente relevantes do ponto de vista do livre desenvolvimento da personalidade humana, uma vez que estão diretamente relacionados a aspectos da vida íntima dos indivíduos que o homem médio não costuma desejar que sejam divulgados ou acessados por terceiros[190].

Por esse motivo, tais informações pessoais receberam um tratamento diferenciado pela LGPD, uma vez que tocam em princípios caríssimos para o ordenamento constitucional brasileiro, como o direito à igualdade, à liberdade de consciência e crença, o direito de imagem e à privacidade, dentre outros. Justamente por isso é importante resguardar a banalização do sistema, impedindo que o tratamento inadequado dessas informações possa comprometer a integridade e a privacidade dos indivíduos em aspectos tão íntimos da sua vida privada.

Segundo Vieira, citado por Sarlet e Ruaro, a personalidade envolve um processo de desenvolvimento em que o indivíduo reconhece a si mesmo e aos outros como seres humanos[191]. Nesse sentido, o livre desenvolvimento da personalidade humana se dá em dois aspectos: da sua vida íntima e privada (aspecto interno) e das suas interações sociais e públicas (aspecto externo)[192]. O livre desenvolvimento da personalidade humana em seu aspecto interno é protegido normativamente pelo direito à privacidade, à liberdade, dentre outros, enquanto o seu aspecto externo é protegido pelo direito de imagem, à honra, ao nome, etc.

---

[190] SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. Revista Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021. DOI: 10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 26 jun. 2024.
[191] Ibidem, p. 93.
[192] Idem.

Como observado por Bruno Bioni, o surgimento dos direitos de personalidade remontam ao direito grego e romano, uma vez que, diferentemente de culturas jurídico-legais anteriores, que focavam na integridade física, os direitos de personalidade passaram a abarcar também o campo moral, como a tutela da honra[193].

Após a Segunda Guerra Mundial, com a proliferação do princípio da dignidade humana nas constituições e a Declaração Universal dos Direitos Humanos, o direito passou a assegurar de modo mais frequente os interesses existenciais da pessoa humana, como os direitos de personalidade[194].

No Brasil, mesmo sob o Código Civil de 1916, a doutrina já reconhecia implicitamente os direitos da personalidade, mas a sistematização desses direitos só ganhou força com o Código Civil de 2002, que incluiu um capítulo específico sobre os direitos da personalidade, como o direito ao nome, à imagem, à liberdade, à honra, à integridade física e os direitos autorais[195].

O autor ainda enfatiza que os direitos da personalidade não representam apenas uma inovação no ordenamento jurídico brasileiro, mas também uma nova hermenêutica que coloca o ser humano no centro do direito civil contemporâneo. Eles fazem parte de uma cláusula geral de proteção e promoção da pessoa humana, o que permite sua adaptação a novas situações, como a proteção dos dados pessoais[196]. Afirma, como conclusão dessa adaptação, que:

> Sob essa perspectiva, um dado, atrelado à esfera de uma pessoa, pode se inserir dentre os direitos da personalidade. Para tanto, ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular. E, nesse sentido, cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses signos identificadores do cidadão. Trata-se de um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações. Isso acaba por justificar dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade, assegurando, por exemplo, que uma pessoa exija a retificação de seus dados pessoais para que a sua projeção seja precisa. Por isso, os dados pessoais não estão relacionados somente com a privacidade, transitando dentre mais de uma das espécies dos direitos da personalidade[197].

---

[193] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 93. ISBN 978-85-309-8328-4.
[194] Ibidem, p. 95.
[195] Idem.
[196] Idem.
[197] Ibidem, p. 99.

A importância de atribuir o caráter de direito de personalidade aos dados pessoais se encontra no fato de que estes representam uma extensão da personalidade dos indivíduos, o que implica que os dados pessoais são protegidos não apenas sob a ótica patrimonial, mas também sob a ótica moral, assegurando que qualquer violação a esses dados seja considerada uma afronta à dignidade da pessoa humana.

Essa interpretação está em consonância com a mudança de paradigma acerca de como se enxergar os dados pessoais trazida pela LGPD, isto é, visando proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. O reconhecimento pelo STJ do caráter de direito de personalidade dos dados pessoais fortalece a aplicação da LGPD e garante uma proteção mais robusta e abrangente aos indivíduos.

Dessa forma, ao atribuir aos dados pessoais o caráter de direito de personalidade, o STJ contribui para a construção de um arcabouço jurídico mais protetivo e alinhado com as necessidades e direitos contemporâneos dos cidadãos, promovendo um ambiente mais seguro e justo para a gestão de informações pessoais.

## CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo principal analisar a responsabilidade civil dos agentes de tratamento de dados pessoais em casos de violação à proteção de dados, comparando os sistemas normativos e jurisprudenciais do Brasil e da Europa, de modo a identificar qual o regime de responsabilidade adotado pela LGPD, a quem ele se aplica e em que medida o modo com que o sistema de responsabilidade civil em proteção de dados brasileiro foi delineado de modo a permitir a reparação aos titulares.

A hipótese inicial levantada na pesquisa aponta que a legislação brasileira apresenta algumas lacunas a respeito de qual é o regime de responsabilidade efetivamente adotado e a quem este regime pode ser aplicado e a Europa, pode servir de referência para a busca por interpretação dessas questões omissas.

A partir de uma metodologia jurídico-dogmática, dedutiva, qualitativa e funcionalista, a pesquisa analisou as principais disposições do GPDR e da LGPD, as decisões dos Tribunais de Justiça brasileiros e do STJ, bem como do Tribunal de Justiça da União Europeia, que abordam o tema da responsabilidade civil em proteção de dados pessoais.

A proposta do Capítulo 1 foi trazer um panorama do desenvolvimento da proteção de dados no Brasil e na Europa, assim como identificar e compreender as bases principiológicas que regem as suas normas de proteção de dados e compreender a relação destes princípios com a reparação de danos aos titulares de dados.

O resultado da pesquisa demonstrou que o Brasil e a Europa seguiram uma trajetória semelhante no desenvolvimento do direito à proteção de dados, iniciando com o reconhecimento da proteção de dados como um direito autônomo, passando pelo reconhecimento de que o titular é o verdadeiros “dono” dos seus dados pessoais, que os dados representam uma extensão da personalidade humana e, portanto, é um direito de personalidade, para, então, reconhecê-lo como um direito fundamental e, finalmente, criando um sistema de responsabilidade civil arrojado, dando ao tema a relevância que este possui no mundo digitalizado.

Ademais, demonstrou-se que o GDPR representou uma mudança de perspectiva para o mundo em relação ao modo de tratar os dados pessoais dos indivíduos e influenciou profundamente o modo com que o sistema de proteção de dados brasileiro foi delineado. O Brasil exportou conceitos como o de *privacy by design*, autodeterminação informativa e o próprio reconhecimento da proteção de dados como um direito fundamental.

Além disso, concluiu-se que os princípios possuem uma importância fundamental no desenvolvimento da unidade sistêmica ao recém-criado sistema de proteção de dados brasileiro, tendo em vista que fornecem uma base principiológica sólida para a efetiva aplicação dos direitos contidos nas normas de proteção de dados e, consequentemente, para a reparação dos titulares que tenham sofrido violações aos seus dados pessoais.

A LGPD trouxe ao ordenamento jurídico brasileiro uma nova perspectiva de como se enxergar e lidar com os dados pessoais dos indivíduos, importando a tendência europeia de tratar os dados pessoais levando-se em conta a finalidade do tratamento, a necessidade dos dados, o respeito à autodeterminação informativa, a transparência no tratamento e a responsabilização dos agentes, etc.

Apesar da clara inspiração na legislação europeia, nota-se algumas diferenças na escolha dos princípios importados para a legislação brasileira. A LGPD optou por não inserir o princípio da licitude no seu rol de princípios, antes, preferiu trazer um artigo com as bases legais que justificam o tratamento de dados, enquanto o GDPR, por sua vez, afirma categoricamente que a obediência ao princípio da licitude se encontra adstrita às hipóteses listadas no art. 6º, 1, do Regulamento.

Esta escolha principiológica, apesar de sutil, revela que no GDPR, a licitude é um princípio norteador de toda a atividade de tratamento, enquanto na LGPD as bases legais são apresentadas como condições nas quais o tratamento de dados é permitido. A consequência prática disso é que, em termos legislativos, bases legais podem ser mais facilmente acrescidas, limitadas ou modificadas, mas os princípios não podem ser alterados sem modificar todo o sistema de proteção de dados estabelecido na lei.

Ademais, demonstrou-se que o princípio da autodeterminação informativa é um conceito relevante em ambos os ordenamentos, uma vez que serve como norte e fundamento para uma série de outros princípios e normas relacionados à proteção de dados pessoais. Além disso, demonstrou-se que a autodeterminação informativa é um corolário importante do livre desenvolvimento da personalidade humana, uma vez que os dados pessoais representam, no mundo digitalizado, uma extensão da personalidade dos indivíduos.

No Capítulo 2, demonstrou-se, inicialmente, que o direito à proteção de dados pessoais, embora seja uma evolução do direito à privacidade, possui sentido próprio e autonomia em relação a este e a tutela jurídica da proteção de dados pessoais traz consigo a necessidade de um regime próprio de responsabilidade, capaz de coibir e reparar as condutas danosas aos dados dos titulares.

Ademais, concluiu-se que as disposições trazidas sobre a responsabilização dos agentes de tratamento na LGPD não permitem a interpretação imediata de que o regime de responsabilidade adotado é objetivo, tendo em vista que, nos termos do art. 927 do Código Civil, a lei não previu expressamente o regime de responsabilidade civil objetiva e não é possível afirmar que todas as atividade de tratamento de dados são, por natureza, atividade de risco.

Isso porque o risco, para fins de responsabilização objetiva, precisa estar atrelado à natureza da atividade desenvolvida e, como demonstrado, nem todas as entidades que realizam tratamento de dados possuem conhecimento técnico da atividade de tratamento realizada. Além disso, para afirmar que o tratamento de dados é uma atividade de risco, é preciso demonstrar que a própria essência dessa atividade envolve um perigo inerente e constante de causar prejuízos. Isso implica considerar fatores como a sensibilidade dos dados tratados, a extensão e a gravidade dos danos decorrentes de um tratamento irregular, bem como a capacidade técnica do agente para gerenciar e mitigar esses riscos.

Conclui-se que exige um esforço interpretativo significativo para reconhecer a responsabilidade civil objetiva, sem que a legislação pertinente tenha claramente a estabelecido, sem considerar as distinções significativas da atividade de tratamento de dados em relação a outras atividades. Essas distinções são primordiais nesse sentido, pois o tratamento de dados no mundo digitalizado possui características e riscos específicos que não estão presentes em outras atividades e devem ser considerados para fins de aferição da responsabilidade dos agentes de tratamento.

Por outro lado, reconhecer por exclusão que a LGPD adotou um regime de responsabilidade civil subjetiva nos padrões tradicionais, sobretudo em um contexto de constante evolução tecnológica, torna a discussão binária e não coopera para o debate e para a evolução do tema da responsabilidade civil dos agentes de tratamento em casos de violação aos dados pessoais dos titulares.

Além da identificação do regime de responsabilidade adotado no Brasil, observou-se uma lacuna legislativa acerca do tipo e extensão dos danos reparáveis. Concluiu-se que a LGPD trouxe uma mudança de paradigma significativa acerca do tema, uma vez que o dano é a própria exposição ao tratamento irregular e não precisa estar atrelado a um dano a um direito de privacidade, de imagem ou até mesmo um dano patrimonial. Essa perspectiva reconhece não apenas os danos tangíveis, mas também os danos imateriais decorrentes da perda de controle sobre os próprios dados, trata-se de verdadeira ofensa ao princípio da autodeterminação informativa. Contudo, tanto a jurisprudência europeia quanto brasileira tem

se encaminhado no sentido de compreender que, para reivindicar indenização é necessário comprovar que o dano material ou imaterial resultou em um prejuízo ou desvantagem real e palpável ao titular.

Ainda no Capítulo 2, foi abordado o tema da responsabilidade civil dos agentes de tratamento em casos de controladoria conjunta. A LGPD não abordou o tema, contudo, o GDPR estabeleceu alguns parâmetros importantes para a definição da responsabilidade dos agentes que, em conjunto com outros, determinam as finalidades e os meios do tratamento de dados pessoais. Estes parâmetros são importantes para auxiliar a interpretação dos Tribunais brasileiros quando este tema, inevitavelmente, começar a ser trazido aos Tribunais.

Concluiu-se que a principal consequência do reconhecimento da controladoria conjunta é que as empresas podem responder de forma solidária pelos danos causados aos titulares, o que significa que estes podem exercer seus direitos contra qualquer um dos controladores conjuntos que tenham poder decisório sobre o tratamento dos dados pessoais, tendo, assim, mais chances de serem reparados pelos prejuízos sofridos pelo tratamento irregular dos seus dados pessoais.

Outro tema não mencionado expressamente na LGPD é a responsabilidade civil do encarregado de dados, o profissional designado pela empresa para supervisionar a conformidade com as leis de proteção de dados. A jurisprudência europeia tem se posicionado no sentido de não ser possível a responsabilização direta desses agentes, contudo, a realidade do tratamento de dados das empresas demonstra que frequentemente as decisões acerca do tratamento são terceirizadas a esses profissionais, que cumprem, na prática, a função de um agente de tratamento.

Concluiu-se que, se o encarregado, sendo uma pessoa jurídica, assume a responsabilidade pelas decisões de tratamento de dados, deve, potencialmente, a depender do caso concreto, ser reconhecida como um agente de tratamento. Isso implica que a responsabilidade pelo tratamento de dados passa a ser compartilhada entre a empresa contratante e o encarregado.

Além disso, verificou-se que a contratação de encarregados que sejam pessoas jurídicas pode criar um distanciamento entre o controlador dos dados e a atividade de tratamento, resultando em uma cadeia de tratamento de dados mais complexa, o que pode dificultar a identificação de responsabilidades e a implementação de medidas corretivas em casos de incidentes de segurança.

Quanto à responsabilidade do sub-operador, verificou-se que seu reconhecimento como agente de tratamento impõe a ele uma série de deveres e responsabilidades, de modo

que a falta de previsão legal clara para responsabilizá-lo gera uma considerável instabilidade jurídica, o que pode resultar em prejuízos para as empresas que tratam dados pessoais e dificultar a identificação da cadeia de agentes de tratamento, tornando a reparação ao titular de dados mais difícil.

Por fim, no Capítulo 3, foram identificadas e analisadas as decisões dos Tribunais brasileiros que tratam da responsabilidade civil dos agentes de tratamento em casos de violação aos dados pessoais, bem como as decisões do Superior Tribunal de Justiça e do Tribunal de Justiça da União Europeia.

A análise revelou que mais da metade do número de empresas demandadas nos acórdãos proferidos pelos Tribunais de Justiça nos 2 (dois) primeiros anos de vigência da LGPD pertencem ao setor de energia elétrica. Conclui-se que a divulgação de um incidente de segurança em um grande veículo de comunicação foi determinante para que o setor de energia elétrica ocupasse essa posição, tendo em vista que a maior parte dos acórdãos apresentam como agente de tratamento a mesma empresa.

Verificou-se, ainda, que ainda por volta de 27% dos acórdãos analisados condenam os agentes de tratamento ao pagamento de indenização por danos, com um valor médio de indenização de R$ 5.833,33. O não reconhecimento de danos morais fundamenta-se, principalmente, na não demonstração de nexo causalidade, na inexistência de danos aos direitos de personalidade, no entendimento de que a violação aos dados representa mero dissabor e que os dados vazados possuem pouca relevância ou são de fácil acesso.

Da análise das decisões, conclui-se que o nexo de causalidade nas condutas lesivas aos dados pessoais não é tão simples de ser identificado como em outros tipos de danos ou em outros tipos de relações jurídicas, o que dificulta a averiguação da responsabilidade do agente causador do dano e, consequentemente, a reparação do titular. Demonstrou-se que o regime de responsabilidade adotado pela LGPD possui como uma das suas características a ênfase à conduta do agente de tratamento, de modo que o tratamento de dados pessoais torna-se irregular quando o agente de tratamento não cumpre a legislação vigente ou falha em proporcionar a segurança adequada esperada pelo titular dos dados.

Observou-se que não há, efetivamente, uma preocupação dos Tribunais em aferir a ou incentivar uma cultura de boas práticas de tratamento e que há uma tendência de analisar os casos de violação à proteção de dados pessoais sob a ótica tradicional da responsabilidade civil.

Notou-se também que mesmo nos casos em que a LGPD é citada, a fundamentação jurídica para a responsabilidade e indenização por danos materiais ainda depende fortemente

de outros regimes legais, fator que demonstra a dificuldade que os julgadores ainda apresentam em manusear as disposições em relação à responsabilidade por danos aos titulares da LGPD.

Concluiu-se ainda que há uma tendência de não reconhecer a violação aos dados pessoais e o direito à indenização quando não verificado um efetivo dano a outros direitos de personalidade, como ao direito de imagem, de privacidade, à honra, etc. na jurisprudência pátria. Demonstrou-se, ainda, que o Tribunal de Justiça da União Europeia tem compreendido a questão em sentido semelhante, reconhecendo que é necessário a aferição de um dano concreto, não bastando a mera violação das disposições do GDPR.

No entanto, a presente pesquisa concluiu que a aplicação das normas previstas na legislação de proteção de dados não deve estar restrita à proteção dos direitos de como a honra e a intimidade, mas abrange a proteção da privacidade dos dados e autodeterminação do titular sobre eles. Ainda que não haja prova de danos emocionais ou psicológicos diretos, a ocorrência do vazamento de dados pessoais representa uma violação à privacidade e à segurança dessas informações, justificando medidas reparatórias ou punitivas conforme previsto na lei. Isso porque, o ordenamento jurídico brasileiro conferiu autonomia ao direito à proteção de dados pessoais ao considerá-lo um direito fundamental e ao criar um sistema normativo próprio de responsabilização.

A análise das decisões do STJ demonstrou uma interpretação distinta e mais aprofundada acerca dos critérios de responsabilização, destacando-se o Recurso Especial nº 2.077.278 - SP, que considerou que o fato de fraudadores terem acesso a informações financeiras de dados de financiamento do titular, dados estes que só deveriam ser tratados pelas instituições, coloca em xeque o adequado tratamento dos dados pessoais dos titulares pelo banco.

Demonstrou-se que a fundamentação da responsabilidade do agente de tratamento não deve se limitar apenas à identificação do exato momento ou forma do vazamento, mas sim à obrigação dos agentes de tratamento de implementar medidas eficazes de segurança para proteger as informações confidenciais de seus clientes.

Ademais, identificou-se que o STJ atribuiu o caráter de direito de personalidade aos dados pessoais em algumas decisões colegiadas e reforçou-se a importância de tal reconhecimento, tendo em vista que os dados pessoais representam uma extensão da personalidade dos indivíduos. Essa atribuição de direito de personalidade implica que os dados pessoais são protegidos não apenas sob a ótica patrimonial, mas também sob a ótica

moral, assegurando que qualquer violação a esses dados seja considerada uma afronta direta à dignidade da pessoa humana.

Por fim, demonstrou-se que essa interpretação está em consonância com a LGPD, que visa proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. O reconhecimento pelo STJ do caráter de direito de personalidade dos dados pessoais fortalece a aplicação da LGPD e garante uma proteção mais robusta e abrangente aos indivíduos.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALEMANHA. Tribunal Constitucional Federal. Volkszählungsurteil - BVerfGE 65, 1. 15 de dezembro de 1983. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html.

ALEXY, Robert. Teoria dos Direitos Fundamentais. 5. ed. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2015. ISBN 978-85-392-0073-3. p. 90.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. civilistica.com, ano 9, n. 3, 2020, p. 2. Disponível em: https://civilistica.com.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 93. ISBN 978-85-309-8328-4.

BIONI, Bruno. Tratado de Proteção de Dados Pessoais. São Paulo: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/.

BIONI, Bruno Ricardo (Org.). Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BORRILLO, Barbara. La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR. Dirittifondamentali.it.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, DF: ANPD, maio de 2021, p. 20. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

BRASIL. Constituição da República Federativa do Brasil de 1988. Promulgada em 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988.

BRASIL. Lei n. 4.657, de 4 de setembro de 1942. Lei de Introdução às Normas do Direito Brasileiro. Art. 2º, §2º. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4657.htm.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=12/09/1990&jornal=1&pagina=1&totalArquivos=144.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Dispõe sobre a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União, Brasília, DF, 10 jun. 2011. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/06/2011&jornal=1&pagina=2&totalArquivos=204.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/11/2011&jornal=1000&pagina=1&totalArquivos=12.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Art. 6º, inciso I. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Centro de Direito, Internet e Sociedade (CEDIS-IDP); Jusbrasil. Painel LGPD nos Tribunais: Jurisprudência do 2º ano de vigência da Lei Geral de Proteção de Dados. Última atualização: Abril de 2023 (com dados de setembro de 2022). Disponível em: https://painel.jusbrasil.com.br/.

DA SILVA, Rafael Peteffi. Antijuridicidade como requisito da responsabilidade civil extracontratual: amplitude conceitual e mecanismos de aferição. Revista de Direito Civil Contemporâneo, São Paulo, v. 18, p. 169-214, 2024. Disponível em: https://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/568f.

COLOMBO, C.; BERNI, D. L. M. Privacy no direito italiano: tríade de decisões judiciais rumo a insights sobre limites conceituais, deslocamento geográfico e transparência do corpo eletrônico . Revista IBERC, Belo Horizonte, v. 5, n. 1, p. 112–131, 2022. DOI: 10.37963/iberc.v5i1.205. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/205.

CUNHA, Anita Spies da; SCHIOCCHET, Taysa. A constitucionalidade do DNA na persecução penal: o direito à autodeterminação informativa e o critério de proporcionalidade no Brasil e na Alemanha. The constitutionality of DNA in criminal prosecution: the right to informative self-determination and the proportionality criterion in Brazil and Germany. Revista de Investigação Constitucional, Curitiba, v. 8, n. 2, p. 529-554, maio/ago. 2021. DOI: https://revistas.ufpr.br/rinc/article/view/74420.

CURY, Paula Maria Nasser. Métodos de Direito Comparado: desenvolvimento ao longo do século XX e perspectivas contemporâneas/Methods of Comparative Law: Developments in the 20th century and contemporary perspectives. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD), ISSN-e 2175-2168, Vol. 6, Nº. 2, 2014 (Ejemplar dedicado a: Julho/Setembro).

DREWER, D.; MILADINOVA, V. The canary in the data mine. Computer Law & Security Review, v. 34, p. 806-815, 2018. Disponível em: https://doi.org/10.1016/J.CLSR.2018.05.019.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados. 2. ed. revista e atualizada [Recurso eletrônico]. São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia LTDA, 2020, p. 190. Disponível em: https://www.livrariart.com.br/e-book-da-privacidade-a-protecao-de-dados-pessoais/p.

EUROPEAN DATA PROTECTION BOARD. Guidelines on Joint Controllership. Disponível

em:
https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

GDPR. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://gdpr.eu/tag/gdpr/.

HIJMAN, Hielke; RAAB, Charles. Ethical Dimensions of the GDPR, AI Regulation, and Beyond. RDP, Brasília, Volume 18, n. 100, p. 63-90, out./dez. 2021, p. 65. DOI: https://doi.org/10.11117/rdp.v18i100.6197.

LANDIM NETO, José Emiliano Paes. Responsabilidade Civil dos Agentes de Tratamento à Luz da Lei Geral de Proteção de Dados: Análise Jurisprudencial dos Tribunais Estaduais. 2022. 74 f. Dissertação (Mestrado Profissional em Direito Econômico e Desenvolvimento) - Instituto Brasileiro de Ensino, Pesquisa e Desenvolvimento (IDP), Brasília, DF, 2022.

LIMA, Cíntia Rosa Pereira de. Comentários à Lei Geral de Proteção de Dados. Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796, p. 128. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/.

LI, Shu. Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. Maastricht Journal of European and Comparative Law, v. 30, n. 3, p. 335-345, 2023. Disponível em: https://doi.org/10.1177/1023263X231208835.

MARANHÃO, J. S. de A.; CAMPOS, R. R. Proteção De Dados De Crédito Na Lei Geral De Proteção De Dados. Direito Público, [S. l.], v. 16, n. 90, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3739.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 4. ed. rev. e atual. São Paulo: Saraiva, 2009. 590 p. ISBN 978-85-02-07819-2.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor. vol. 120. ano 27. p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018.

MENDES, Laura S. Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental, 1ª Edição. ISBN 9788502218987. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502218987/. Acesso em: 20 dez. 2023. E-book. São Paulo: Editora Saraiva.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. 1ª ed. São Paulo: Saraiva Jur - Sob Demanda, 2013. 248 p. ISBN 978-8502218963.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS (MPDFT). MPDFT e Netshoes firmam acordo para pagamento de danos morais coletivos após vazamento de dados. 2019. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noti

cias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados.

RODOTÀ, Stefeano. Tecnologie e Diritti (Capítulo 1) [eBook]. Editora Il Mulino. Disponível em: vbk://YPrZGkvqzGQ9IvvWK88v7QpG61rGm0eThywySx24dUs.

SANTOS, Rômulo Marcel Souto dos; LEITÃO, André Studart; WOLKART, Erik Navarro. A responsabilidade civil na Lei Geral de Proteção de Dados Pessoais e a regra de Hand. Civil responsibility in the General Personal Data Protection Law and the Hand Rule. Responsabilidad civil en la Ley General de Protección de Datos Personales y la regla de Hand. Revista de Direito, v. 20, n. 34, p. 60-84, 2022. Editora responsável: Profa. Dra. Fayga Bedê. Submetido em: 24 nov. 2021. Aprovado em: 21 dez. 2021. DOI: 10.12662/2447-6641oj.v20i34.p60-84.2022. Disponível em: https://orcid.org/0000-0001-6444-2631.

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

ŠIDLAUSKAS, A. (2021). The Role and Significance of the Data Protection Officer in the Organization. Sociedade e Tecnologia, 44(1), 8–28. p. 11. Disponível em: https://doi.org/10.15388/Soctyr.44.1.1.

SIQUEIRA, D. P.; SANTOS DE MORAES, F. S. de M.; PLAZA TENA, L. Do reconhecimento da autodeterminação informativa como direito da personalidade e do princípio da segurança. Revista Direito em Debate, [S. l.], v. 31, n. 57, p. 4, 2022. DOI: 10.21527/2176-6622.2022.57.12476. Disponível em: https://revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/12476.

SPIECKER GENANNT DÖHMANN, I. A Proteção de Dados Pessoais sob o Regulamento de Proteção de Dados da União Europeia. Direito Público, [S. l.], v. 17, n. 93, 2020. DOI: 10.11117/rdp.v17i93.4235., P. 20. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4235.

UNIÃO EUROPEIA; CONSELHO DA EUROPA. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo: Serviço das Publicações da União Europeia, 2014. ISBN 978-92-871-9939-3 (Conselho da Europa). ISBN 978-92-9239-498-1 (FRA). doi:10.2811/73790.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados - RGPD). Art. 28. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

PITOMBO, Clara. LGPD aumenta a busca por executivo de proteção de dados. Valor Econômico, São Paulo, 23 set. 2021. Carreira. Disponível em: https://valor.globo.com/carreira/noticia/2021/09/23/lgpd-aumenta-a-busca-por-executivo-de-protecao-de-dados.ghtml.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis

no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. Revista Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021. DOI: 10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. Fundamentos do direito civil: responsabilidade civil. 2. ed. Rio de Janeiro: Forense, 2021.

ZANINI, L. E. de A. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. Revista Brasileira de Direito Civil, [S. l.], v. 3, n. 01, 2017. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/107.

## APÊNDICE A - Lista de decisões analisadas - Tribunais de Justiça e Tribunais Regionais

| Número Unificado | Tribunal | Violação da LGPD | Danos materiais | Danos morais | Decisão na íntegra |
|---|---|---|---|---|---|
| 5071091-33.2021.4.04.7000 | TRF-4 | não | não | não | link |
| 5002557-77.2020.8.13.0407 | TJMG | sim | não | não | link |
| 5000339-43.2021.4.04.7127 | TRF-4 | não | não | não | link |
| 1049096-26.2021.8.26.0100 | TJSP | sim | não | R$ 10.000,00 | link |
| 1041607-35.2021.8.26.0100 | TJSP | sim | não | R$ 10.000,00 | link |
| 1034681-38.2021.8.26.0100 | TJSP | segredo de justiça | segredo de justiça | segredo de justiça | link |
| 1033634-56.2021.8.26.0576 | TJSP | não | não | não | link |
| 1025347-69.2020.8.26.0405 | TJSP | sim | não | não | link |
| 1025180-52.2020.8.26.0405 | TJSP | | não | não | link |
| 1025007-28.2020.8.26.0405 | TJSP | sim | não | não | link |
| 1024189-76.2020.8.26.0405 | TJSP | sim | não | R$5.000,00 | link |
| 1024060-71.2020.8.26.0405 | TJSP | sim | não | não | link |
| 1024016-52.2020.8.26.0405 | TJSP | sim | não | não | link |
| 1023689-10.2020.8.26.0405 | TJSP | sim | não | não | link |
| 1022842-08.2020.8.26.0405 | TJSP | sim | não | não | link |
| 1014355-73.2021.8.26.0224 | TJSP | sim | não | não | link |
| 1013341-62.2021.8.26.0577 | TJSP | sim | não | R$ 20.000,00 | link |
| 1012425-28.2021.8.26.0577 | TJSP | segredo de justiça | segredo de justiça | segredo de justiça | link |
| 1010207-69.2020.8.26.0348 | TJSP | sim | não | não | link |
| 1010190-49.2021.8.26.0008 | TJSP | sim | não | não | link |
| 1009507-51.2021.8.26.0577 | TJSP | sim | não | R$ 3.000 | link |

| | | | | | |
|---|---|---|---|---|---|
| 1008308-35.2020.8.26.0704 | TJSP | sim | não | não | link |
| 1006311-89.2020.8.26.0001 | TJSP | sim | não | R$ 10.000,00 | link |
| 1005347-71.2020.8.26.0268 | TJSP | sim | não | não | link |
| 1004903-86.2021.8.26.0564 | TJSP | não | não | não | link |
| 1004863-05.2021.8.26.0597 | TJSP | não | não | não | link |
| 1004684-78.2020.8.26.0024 | TJSP | sim | não | R$ 2.000,00 | link |
| 1004206-95.2021.8.26.0554 | TJSP | sim | não | não | link |
| 1003469-68.2021.8.26.0562 | TJSP | sim | não | não | link |
| 1003122-23.2020.8.26.0157 | TJSP | sim | não | R$ 2.000 | link |
| 1003110-49.2021.8.26.0003 | TJSP | sim | não | não | link |
| 1003086-21.2021.8.26.0003 | TJSP | sim | não | R$ 5.000,00. | link |
| 1002607-85.2020.8.26.0157 | TJSP | sim | não | R$ 2.500,00 | link |
| 1001810-10.2021.8.26.0405 | TJSP | sim | não | não | link |
| 1001627-84.2021.8.26.0002 | TJSP | não | não | não | link |
| 1001559-22.2021.8.26.0589 | TJSP | não | não | não | link |
| 1001447-46.2021.8.26.0462 | TJSP | não fica claro | não | não | link |
| 1001188-73.2021.8.26.0002 | TJSP | sim | não | não | link |
| 1001138-10.2021.8.26.0176 | TJSP | sim | não | não | link |
| 1000654-84.2021.8.26.0405 | TJSP | sim | não | não | link |
| 1000580-66.2021.8.26.0005 | TJSP | não | não | não | link |
| 1000537-44.2021.8.26.0001 | TJSP | segredo de justiça | segredo de justiça | segredo de justiça | link |
| 1000522-27.2021.8.26.0405 | TJSP | não | não | não | link |
| 1000397-59.2021.8.26.0405 | TJSP | não | não | não | link |

| | | | | | |
|---|---|---|---|---|---|
| 0715585-63.2020.8.07.0007 | TJDFT | sim | sim | não | link |
| 0183387-68.2021.8.05.0001 | TJBA | sim | sim | R$ 3.000,00 | link |
| 0160075-63.2021.8.05.0001 | TJBA | sim | sim | não | link |
| 0149420-32.2021.8.05.0001 | TJBA | sim | sim | R$ 3.000,00 | link |
| 0108370-26.2021.8.05.0001 | TJBA | não | não | não | link |
| 0076618-93.2018.8.16.0014 | TJPR | sim | não | R$ 5.000,00 | link |
| 0040126-45.2021.8.05.0001 | TJBA | sim | sim | não | link |
| 0007499-94.2021.8.19.0066 | TJRJ | sim | sim | R$ 5.000,00 | link |
| 0006500-94.2021.8.19.0211 | TJRJ | não | não | não | link |
| 0005697-07.2021.8.05.0113 | TJBA | sim | não | R$ 4.000,00 | link |
| 0004533-05.2021.8.05.0146 | TJBA | sim | sim | não | link |
| 0002183-58.2021.8.26.0405 | TJSP | não | não | não | link |
| 0000354-53.2022.8.05.0191 | TJBA | sim | sim | não | link |
| 5037066-84.2021.8.21.7000 | TJRS | sim | não | não | link |

## APÊNDICE B - Lista de decisões analisadas - Superior Tribunal de Justiça

| Número do acórdão | Tribunal | Decisão na íntegra |
|---|---|---|
| REsp 2092096 / SP | STJ | link |
| REsp 2077278 / SP | STJ | link |
| AREsp 2.130.619 - SP | STJ | link |
| REsp 2135783 / DF | STJ | link |
| REsp nº 1.995.458 | STJ | link |
| REsp nº 1.914.596 - RJ | STJ | link |

## APÊNDICE C - Lista de decisões analisadas - Tribunal de Justiça da União Europeia

| Caso | Partes | País de origem | Link |
|---|---|---|---|
| C-300/21 | UI vs Österreichische Post AG | Áustria | link |
| C-210/16 | Wirtschaftsakademie Schleswig-Holstein GmbH vs Verbraucherzentrale NRW eV | Alemanha | link |
| C-40/17 | Fashion ID GmbH & Co. KG vs Verbraucherzentrale NRW eV | Alemanha | link |
| C-25/17 | Jehovan todistajat vs Finland | Finlândia | link |
| C-453/21 | X-FAB Dresden vs Other | Alemanha | link |
| C-131/12 | Google Spain SL e Google Inc. vs Agencia Española de Protección de Datos (AEPD) e Mario Costeja González | Espanha | link |