

**IV CONGRESSO INTERNACIONAL DE
DIREITO E INTELIGÊNCIA
ARTIFICIAL (IV CIDIA)**

RESPONSABILIDADE CIVIL E TECNOLOGIA

R434

Responsabilidade civil e tecnologia [Recurso eletrônico on-line] organização IV Congresso Internacional de Direito e Inteligência Artificial (IV CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: José Luiz de Moura Faleiros Júnior, Sérgio Henriques Zandoná Freitas e Arthur Pinheiro Basan – Belo Horizonte: Skema Business School, 2023.

Inclui bibliografia

ISBN: 978-65-5648-792-2

Modo de acesso: www.conpedi.org.br em publicações

Tema: Os direitos dos novos negócios e a sustentabilidade.

1. Direito. 2. Inteligência artificial. 3. Tecnologia. I. IV Congresso Internacional de Direito e Inteligência Artificial (1:2023 : Belo Horizonte, MG).

CDU: 34

skema
BUSINESS SCHOOL

LAW SCHOOL
FOR BUSINESS

IV CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (IV CIDIA) RESPONSABILIDADE CIVIL E TECNOLOGIA

Apresentação

O IV Congresso Internacional de Direito e Inteligência Artificial - CIDIA da SKEMA Business School Brasil, realizado nos dias 01 e 02 de junho de 2023 em formato híbrido, consolida-se como o maior evento científico de Direito e Tecnologia do Brasil. Estabeleceram-se recordes impressionantes, com duzentas e sessenta pesquisas elaboradas por trezentos e trinta e sete pesquisadores. Dezenove Estados brasileiros, além do Distrito Federal, estiveram representados, incluindo Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Pará, Pernambuco, Paraná, Rio de Janeiro, Rio Grande do Norte, Rondônia, Roraima, Rio Grande do Sul, Santa Catarina, Sergipe, São Paulo e Tocantins.

A condução dos trinta e três grupos de trabalho do evento, que geraram uma coletânea de vinte e cinco livros apresentados à comunidade científica nacional e internacional, contou com a valiosa colaboração de sessenta e três professoras e professores universitários de todo o país. Esses livros são compostos pelos trabalhos que passaram pelo rigoroso processo de double blind peer review (avaliação cega por pares) dentro da plataforma CONPEDI. A coletânea contém o que há de mais recente e relevante em termos de discussão acadêmica sobre a relação entre inteligência artificial, tecnologia e temas como acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, sustentabilidade, democracia e responsabilidade civil, entre outros temas relevantes.

Um sucesso desse porte não seria possível sem o apoio institucional de entidades como o CONPEDI - Conselho Nacional de Pesquisa e Pós-graduação em Direito; o Programa RECAJ-UFGM - Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais; o Instituto Brasileiro de Estudos de Responsabilidade Civil - IBERC; a Comissão de Inteligência Artificial no Direito da Ordem dos Advogados do Brasil - Seção Minas Gerais; a Faculdade de Direito de Franca - Grupo de Pesquisa Políticas Públicas e Internet; a Universidade Federal Rural do Semi-Árido - UFRSA - Programa de Pós-graduação em Direito - Laboratório de Métodos Quantitativos em Direito; o Centro Universitário Santa Rita - UNIFASAR; e o Programa de Pós-Graduação em Prestação Jurisdicional e Direitos Humanos (PPGPJDH) - Universidade Federal do Tocantins (UFT) em parceria com a Escola Superior da Magistratura Tocantinense (ESMAT).

Painéis temáticos do congresso contaram com a presença de renomados especialistas do Direito nacional e internacional. A abertura foi realizada pelo Professor Dierle Nunes, que discorreu sobre o tema "Virada tecnológica no Direito: alguns impactos da inteligência artificial na compreensão e mudança no sistema jurídico". Os Professores Caio Lara e José Faleiros Júnior conduziram o debate. No encerramento do primeiro dia, o painel "Direito e tecnologias da sustentabilidade e da prevenção de desastres" teve como expositor o Deputado Federal Pedro Doshikazu Pianchão Aihara e como debatedora a Professora Maraluce Maria Custódio. Para encerrar o evento, o painel "Perspectivas jurídicas da Inteligência Artificial" contou com a participação dos Professores Mafalda Miranda Barbosa (Responsabilidade pela IA: modelos de solução) e José Luiz de Moura Faleiros Júnior ("Accountability" e sistemas de inteligência artificial).

Assim, a coletânea que agora é tornada pública possui um inegável valor científico. Seu objetivo é contribuir para a ciência jurídica e promover o aprofundamento da relação entre graduação e pós-graduação, seguindo as diretrizes oficiais da CAPES. Além disso, busca-se formar novos pesquisadores na área interdisciplinar entre o Direito e os diversos campos da tecnologia, especialmente o da ciência da informação, considerando a participação expressiva de estudantes de graduação nas atividades, com papel protagonista.

A SKEMA Business School é uma entidade francesa sem fins lucrativos, com uma estrutura multicampi em cinco países de diferentes continentes (França, EUA, China, Brasil e África do Sul) e três importantes creditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua dedicação à pesquisa de excelência no campo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital requer uma abordagem transdisciplinar.

Expressamos nossos agradecimentos a todas as pesquisadoras e pesquisadores por sua inestimável contribuição e desejamos a todos uma leitura excelente e proveitosa!

Belo Horizonte-MG, 14 de julho de 2023.

Prof^a. Dr^a. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Caio Augusto Souza Lara

Coordenador de Pesquisa – SKEMA Law School for Business

INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS E A NATUREZA 'IN RE IPSA' DO DANO EXTRAPATRIMONIAL CAUSADO

SECURITY INCIDENTS INVOLVING PERSONAL DATA AND THE 'IN RE IPSA' NATURE OF THE MORAL DAMAGE

José Luiz de Moura Faleiros Júnior ¹
Pedro Ruschel Ewald Vega Garcia ²

Resumo

O texto discute a natureza do dano moral decorrente de incidentes de segurança com dados pessoais, especialmente com a entrada em vigor da LGPD no Brasil. A exposição de informações pessoais pode afetar a vida privada e a reputação de uma pessoa, gerando prejuízos financeiros e emocionais difíceis de mensurar. É importante adotar uma abordagem indutiva para a análise do problema, levando em conta as diversas variáveis envolvidas. Propõe-se um estudo de caso sobre o AREsp nº 2.130.619/SP, julgado pelo STJ, para entender como a jurisprudência vem se posicionando sobre o tema.

Palavras-chave: Incidentes de segurança, Dano extrapatrimonial, Dano in re ipsa, Dados pessoais, Responsabilidade civil

Abstract/Resumen/Résumé

The paper aims to discuss the nature of moral damages arising from personal data security incidents, especially with the entry into force of LGPD in Brazil. The exposure of personal information can directly affect one's private life and reputation, generating financial and emotional damages that are difficult to quantify. It is important to adopt an inductive approach to analyzing the problem, taking into account the various variables involved. A case study is proposed on AREsp No. 2.130.619/SP, judged by STJ, to understand how jurisprudence has been positioning itself on the issue.

Keywords/Palabras-claves/Mots-clés: Security incidents, Moral damage, In re ipsa damage, Personal data, Civil liability

¹ Doutorando em Direito pela USP e pela UFMG. Mestre e Bacharel em Direito pela UFU. Advogado e Professor da SKEMA Law School. Orientador.

² Especialista em Direito Digital pelo Instituto de Direito e Sociedade do Rio de Janeiro - ITS Rio.

1 Introdução

O tema-problema em questão trata da natureza *in re ipsa* do dano moral decorrente de incidentes de segurança com dados pessoais. Esse é um assunto de grande relevância na atualidade, especialmente com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) no Brasil, que define as regras para o tratamento de informações pessoais pelos diversos setores da sociedade.

Para entender a discussão sobre a natureza *in re ipsa* do dano moral em casos de incidentes de segurança com dados pessoais, é preciso levar em conta a complexidade do tema. Afinal, a exposição de informações pessoais pode afetar diretamente a vida privada e a reputação de uma pessoa, gerando prejuízos financeiros e emocionais que muitas vezes são difíceis de mensurar.

No entanto, é preciso ter cautela em relação ao regime de responsabilização definido na LGPD para que se extraia conclusões contextuais. É nesse ponto que se destaca a proposta de Helen Nissenbaum sobre a "privacy in context", que propõe a análise do tratamento de informações pessoais em seu contexto específico, levando em conta as diversas variáveis envolvidas, tais como a natureza das informações, o tipo de empresa envolvida e o grau de exposição dos dados.

Nesse contexto, é importante adotar uma abordagem indutiva para a análise do problema, a fim de se obter uma visão mais abrangente e contextualizada da questão. Para isso, propõe-se um estudo de caso sobre o AREsp nº 2.130.619/SP, julgado pelo Superior Tribunal de Justiça (STJ), a fim de se entender como a jurisprudência vem se posicionando sobre o tema.

2 Um importante precedente: o AREsp nº 2.130.619/SP, julgado pelo STJ

O incidente de segurança com dados pessoais, do qual o vazamento é espécie, nada mais é que uma falha indesejável e que pode gerar consequências negativas para as pessoas afetadas. No entanto, o simples fato de ocorrer um vazamento não significa que haja dano moral indenizável. Essa é a posição adotada pela Segunda Turma do Superior Tribunal de Justiça (STJ), por ocasião do julgamento do AREsp nº 2.130.619/SP. De acordo com o entendimento do STJ, é preciso que o titular dos dados comprove o efetivo prejuízo gerado pela exposição dessas informações para que haja direito a uma indenização por danos morais.

O caso em análise envolve a Eletropaulo e uma cliente que teve seus dados pessoais vazados em meio a um incidente de segurança da concessionária de energia elétrica, que culminou no compartilhamento indevido dos dados pessoais de seus clientes no Município de

Osasco/SP. Tal incidente ocorreu em novembro de 2020 e envolveu dados de milhares de titulares, resultando em uma profusão de ações perante o Judiciário paulista¹, nas quais os titulares de dados pediam a condenação empresa ao pagamento de uma indenização a título de danos morais.

Na lide relacionada ao precedente sob análise, a cliente alegou que dados pessoais como nome, data de nascimento, endereço e número do documento de identificação foram vazados e acessados por terceiros, gerando potencial perigo de fraude e importunações. O Tribunal de Justiça de São Paulo (TJSP) havia condenado a Eletropaulo a pagar indenização por danos morais de R\$ 5 mil em virtude do vazamento, mas o STJ reformou essa decisão por entender que os dados vazados eram de natureza comum e não sensíveis, e que não houve comprovação de efetivo dano moral.

Em sua decisão, o STJ se alinhou à tese de que a Lei Geral de Proteção de Dados Pessoais (LGPD) traz um rol taxativo dos dados pessoais considerados sensíveis e que exigem tratamento diferenciado, embora parte da doutrina entenda que a definição de dados pessoais sensíveis da LGPD é meramente exemplificativa (MULHOLLAND, 2020, p. 109-124). Entre esses dados estão informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, assim como dados referentes à saúde sexual e outros de natureza íntima. No caso em questão, os dados vazados eram de natureza comum e não se enquadravam nessas categorias.

O STJ também deixou claro que o dano moral pelo vazamento de dados não é presumido e que é preciso que o titular dos dados demonstre ter havido efetivo dano com o vazamento e o acesso de terceiros. Em outras palavras, o simples fato de os dados terem sido vazados não é suficiente para gerar direito a uma indenização por danos morais. É preciso que haja uma comprovação efetiva de prejuízo decorrente desse vazamento.

Trata-se de importante precedente porque estabelece critérios mais claros para a responsabilidade das empresas em relação ao vazamento de dados pessoais. As empresas têm a obrigação de proteger os dados de seus clientes e usuários, mas isso não significa que qualquer vazamento resultará em dano moral indenizável. É preciso que haja uma análise cuidadosa do caso para determinar se houve efetivo prejuízo e, em caso positivo, qual seria o valor adequado para uma indenização.

¹ A título de exemplo, vide os seguintes processos, dentre tantos outros: 1004903-86.2021.8.26.0564; 1000407-06.2021.8.26.0405; 1025180-52.2020.8.26.0405; 1002694-39.2021.8.26.0405; 1000331-24.2021.8.26.0003; 1024189-76.2020.8.26.0405; e 1003086-21.2021.8.26.0003

Essa decisão também destaca a importância de a LGPD ser seguida pelas empresas quando do tratamento de dados pessoais. A LGPD tem como objetivo garantir a privacidade e a proteção dos dados pessoais dos cidadãos brasileiros, estabelecendo regras claras para a coleta, armazenamento, uso e compartilhamento desses dados pessoais. Ela também incentiva a adoção, por parte das empresas, de medidas efetivas de prevenção, eliminação e mitigação do risco inerente ao tratamento de dados pessoais, notadamente por meio de programas de integridade e políticas de governança de dados. Tais medidas podem, inclusive, balizar a responsabilidade das empresas quando da ocorrência de incidentes de segurança (MARTINS; FALEIROS JÚNIOR, 2020, p. 263-298).

A decisão do STJ sob análise não entrou nesse mérito, limitando-se a concluir pela inoccorrência de qualquer dano à autora. Contudo, no primeiro grau, a sentença da juíza Denise Cavalcante Fortes Martins, da 4ª Vara Cível do Foro de Osasco, reformada pelo TJSP e posteriormente restabelecida pelo STJ, levou em consideração as providências tomadas pela Eletropaulo “para amenizar os possíveis danos que o vazamento de dados poderia causar aos seus clientes”.

3 O dano moral ‘*in re ipsa*’ e os incidentes de segurança

O legislador optou por estipular um regime de responsabilidade civil repleto de nuances e particularidades para a LGPD. Em grande sintonia com os artigos 24, 25 e 26 do RGPD europeu, o artigo 42 da LGPD é a principal base estrutural do tema. Pela literalidade do *caput*, observa-se que se falou em dano “patrimonial, moral, individual ou coletivo”, denotando uma amplitude reparatória semelhante à descrita pelo artigo 82, n.º 1, do RGPD europeu. A par disso, deve-se fazer expressa menção aos estudos de Helen Nissenbaum (2010, p. 231-233), que defende existir um valor social atribuível às informações pessoais, servindo como uma ‘régua’ para a conceituação do que seja apropriado ou não. Nesse plano, a autora defende a utilização de uma “privacidade contextual” como processo decisional heurístico no qual o centro de análise redonda na captura do significado completo da privacidade e nos sucedâneos de eventual violação.

Em casos extremos, os danos causados podem ser enormes, acarretando a perpetuação de seus efeitos pelo fato de a informação permanecer armazenada na Internet – é nesse contexto que se cogita de um direito ao esquecimento, figura jurídica que já produziu grande quantidade de exemplos e precedentes para se tornar uma preocupação premente do legislador – e, sendo a Internet um ambiente propício à replicação quase imediata da informação, certamente impõe

riscos muito maiores do que se imagina quanto à coleta e ao tratamento dispensado aos dados pelos agentes respectivos.

Significa dizer que, para além de diversas situações específicas e evidentemente danosas, é de se esperar que a averiguação de eventual violação – especialmente para fins de aferição da responsabilidade civil – transcenda a mera verificação objetiva do fato e adentre aos meandros contextuais do dano e da utilização do dado.

Um elemento da responsabilidade civil especialmente delicado nos episódios de vazamentos de dados pessoais na internet é a investigação sobre a possibilidade de estabelecimento do nexo causal. Tal investigação pode se mostrar tormentosa, já que muitas vezes a relação entre causa e efeito não é de fácil constatação. Nesse sentido, discute-se se seria necessário existir uma relação de necessidade absoluta entre causa e efeito ou se haveria um grau mínimo aceitável de probabilidade para que se estabelecesse o nexo causal.

A presunção de probabilidade é relativa em alguns contextos e pode ser elidida por qualquer prova idônea, a fim de tornar o trabalho etiológico o mais eficiente e adequado possível. Não obstante, na prática, o nexo causal em casos de difícil verificação se define intuitivamente. A ideia de que seja admissível o nexo probabilístico de causalidade parece, à primeira vista, ter o efeito de rachar um dos pilares fundamentais da responsabilidade, a saber, a comprovação da efetiva contribuição causal de um determinado evento para a produção de um dano. (SOARES, 2023, p. VIII-IX). De qualquer forma, conclui-se que a distribuição do ônus da prova em ações relacionadas à responsabilidade por danos morais em razão de vazamentos de dados pessoais é uma tarefa complexa, nomeadamente diante das previsões sobre o tema no Código de Defesa do Consumidor – que será aplicável na maior parte das vezes – e no Código de Processo Civil.

Outra ponto relevante, a despeito de eventual controvérsia sobre a natureza do regime de responsabilização previsto no artigo 42 da LGPD², é trazer à baila as nuances complexas nas atividades de tratamento de dados pessoais, que devem ser conjecturadas a partir dos limites de previsibilidade de riscos e resultados (elementos expressamente descritos no art. 44, II, da lei, ao tratar do conceito de tratamento irregular de dados³). À vista disso, uma definição clara sobre

² Defendendo posição objetivista, tem-se MULHOLLAND, 2020, p. 122; MIRAGEM, 2019, p. 27 *et seq*; DRESCH; FALEIROS JÚNIOR, 2019, p. 74; ROSENVALD, 2021. Em sentido diverso, analisando o referido dispositivo e defendendo a natureza subjetiva do regime de responsabilidade civil em questão, tem-se, por todos, GUEDES, MEIRELES, 2019, p. 231-232; DANTAS BISNETO, p. 228.

³ No contexto das relações de consume, mas com grande eloquência, mister a menção ao entendimento de Juliano Madalena quanto à natureza *in re ipsa* do dever de indenizar por violação à esperada segurança que descreve o art.

os limites conceituais dos agentes de tratamento é essencial para que a responsabilidade civil seja melhor trabalhada e analisada na LGPD e para permitir a distinção entre controlador(es) e operador(es) em um contexto amplo e permeado por múltiplos agentes. (EHRHARDT JÚNIOR, 2022, p. 396-400).

Por fim, é necessário tratar da questão dos danos morais *in re ipsa* em razão de vazamentos de dados pessoais sensíveis. Um trecho do voto do relator, Ministro Francisco Falcão, acena nesse sentido ao afastar a presunção de danos morais nos vazamentos de dados pessoais e dispor que “diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural”. Tal racional requer cautela.

Ora, a quantidade de dados pessoais que se enquadram na categoria de dados pessoais sensíveis é imensa, sobretudo para os adeptos da tese de que o conceito previsto no art. 5º, inc. II, da LGPD é meramente exemplificativo. Para ficar apenas nos dados sensíveis sobre saúde, há desde informações sobre o tipo sanguíneo de um indivíduo, até informações sobre contágio por doenças infecciosas, como o HIV.

Destarte, embora a LGPD não faça essa gradação, na prática é possível observar a existência de diversos níveis de sensibilidade dos dados pessoais sensíveis, desde os mais corriqueiros, mas que ainda assim se enquadram no conceito, aos ultrassensíveis, cuja divulgação é capaz de gerar prejuízos imensos e irreversíveis aos seus titulares. Para tais, parece adequada a presunção de dano moral em caso de vazamento.

Ressalte-se que a presente discussão não visa diminuir a proteção aos dados pessoais sensíveis, que é sólida, rigorosa, e está prevista de forma pormenorizada na LGPD, mas sim limitar a aplicação do conceito de dano moral presumido aos casos em que ele realmente se faz necessário, sob pena de excessos prejudiciais à inovação e, em última análise, à sociedade como um todo.

4 Considerações finais

É fato que os dados pessoais são um bem jurídico merecedor de tutela. Inclusive, com a promulgação da Emenda Constitucional nº 115/2022, a proteção dos dados pessoais foi alçada

44 da lei: “Em assim sendo, a responsabilidade pelo descumprimento do dever de segurança possui previsão expressa no art. 44 da mesma norma, que refere a responsabilidade do controlador ou operador pela violação da segurança dos dados (...). Portanto, a LGPD ao escolher o sistema de responsabilidade civil subjetiva funda o dever de indezar na culpa e mitiga os efeitos adversos da sua escolha com a possibilidade de inversão do ônus da prova, também prevista no CDC. Entretanto, ao nosso ver, o dano causado pela exposição dos direitos da personalidade é *in re ipsa*: o fato de descumprir com culpa o dever de segurança e gerar dano faz com que se origine o dever de indenizar.” MADALENA, 2021, p. 258. Esse tema, aliás, já foi objeto de enfrentamento em decisões judiciais brasileiras. Para um resumo panorâmico de seus principais pontos, conferir CARDOSO, 2021, p. 133-153.

à categoria de direito fundamental, cláusula pétrea da Constituição. Tampouco se discutem os diversos prejuízos que um titular pode sofrer em razão do vazamento de seus dados pessoais.

A caracterização da responsabilidade civil em casos de vazamentos de dados pessoais é complexa e repleta de meandros, desde o estabelecimento do nexos causal até a distinção entre controladores e operadores em operações de tratamento de dados intrincadas e com múltiplos agentes.

Nesse sentido, a tese da ocorrência de danos morais *in re ipsa* em caso de vazamento de quaisquer tipos de dados pessoais simplifica de forma demasiada a questão, que requer uma análise minuciosa e contextualizada. Além disso, é potencialmente danosa, na medida em que cria um risco excessivo para as empresas que lidam com o tratamento de dados, desestimulando investimentos, principalmente no setor de tecnologia. Há ainda a questão do potencial enriquecimento sem causa de titulares que tiveram dados corriqueiros vazados, sem maiores repercussões para suas vidas, bem como da inviabilidade prática do pagamento das indenizações nos casos de vazamentos envolvendo os dados pessoais de milhares – ou milhões – de titulares. Assim, andou bem o STJ ao condicionar os danos morais em vazamentos de dados pessoais à comprovação dos prejuízos deles decorrentes.

A situação é outra quando tratamos do vazamento de dados pessoais sensíveis. Nesse caso, a presunção de dano moral exige uma análise contextualizada que envolva a natureza do dado pessoal sensível vazado e os potenciais prejuízos do vazamento.

Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, 15 ago. 2018, p. 59. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 05 abr. 2023.

CARDOSO, João Victor Gontijo. O dano moral ‘in re ipsa’ e o tratamento indevido de dados sob o prisma dos julgados: REsp 1.758.799/MG e ADI 6387 MC-REF. **Revista IBERC**, Belo Horizonte, v. 4, n. 1, p. 133-153, jan./abr. 2021.

DANTAS BISNETO, Cícero. Dano moral pela violação à legislação de proteção de dados: um estudo de direito comparado entre a LGPD e o RGPD. *In*: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (coord.). **Proteção de dados pessoais na sociedade da informação: entre dados e danos**. Indaiatuba: Foco, 2021.

DRESCH, Rafael de Freitas Valle; FALEIROS JÚNIOR, José Luiz de Moura. Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). *In*: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). **Responsabilidade civil: novos riscos**. Indaiatuba: Foco, 2019

DRESCH, Rafael de Freitas Valle; MELO, Gustavo da Silva. Art. 43 (Da Responsabilidade e do Ressarcimento de Danos). In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Comentários à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)**. Indaiatuba: Foco, 2022. p. 401-403.

EHRHARDT JÚNIOR, Marcos. Art. 42 (Da Responsabilidade e do Ressarcimento de Danos). In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Comentários à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)**. Indaiatuba: Foco, 2022. p. 396-400.

FALEIROS JÚNIOR, José Luiz de Moura. O que é, afinal, um “vazamento” de dados? **Migalhas de Proteção de Dados**, 10 set. 2021. Disponível em: <https://s.migalhas.com.br/S/23C5D9> Acesso em: 05 abr. 2023.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Venceslau. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019

LIMBERGER, Têmis; BASAN, Arthur Pinheiro. Análise do "Caso Cyrela": o direito ao sossego do consumidor e a proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 136, p. 233-253, jul./ago. 2021.

MADALENA, Juliano. A responsabilidade civil decorrente do vazamento de dados pessoais. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (coord.). **Lei Geral de Proteção de Dados: aspectos relevantes**. Indaiatuba: Foco, 2021

MARTINS, Guilherme Magalhães ; FALEIROS JÚNIOR, José Luiz de Moura . Compliance digital e responsabilidade civil na Lei Geral de Proteção de Dados. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.). **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco, 2020.

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

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.). **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco, 2020.

NISSENBAUM, Helen. **Privacy in context: technology, policy and the integrity of social life**. Stanford: Stanford University Press, 2010.

ROSENVALD, Nelson. O compliance e a redução equitativa da indenização na LGPD. **Migalhas de Proteção de Dados**, 19 mar. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342032/o-compliance-e-a-reducao-equitativa-da-indenizacao-na-lgpd>. Acesso em: 07 abr. 2023.

ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. *Accountability* e mitigação da responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021.

SOARES, Flaviana Rampazzo. Dano presumido e dano 'in re ipsa' – distinções necessárias. **Revista IBERC**, Belo Horizonte, v. 6, n. 1, Editorial, jan./abr. 2023.