

## VAZAMENTO DE DADOS E RESPONSABILIDADE CIVIL: O VALOR CONCRETO DE UM DADO PESSOAL

Vicente Fernando Bitencourt Wiesinieski<sup>1</sup> (UniSecal)  
Prof. Recieri de Tarso Zenardi<sup>2</sup> (Unisecal)

**Resumo:** Esta pesquisa aborda o vazamento de dados pessoais a partir da ótica do direito brasileiro contemporâneo, com ênfase em mensurar os efeitos da aplicação da responsabilidade civil ao assunto. Após definir o que são dados pessoais e seu vínculo com o direito à privacidade, com base em teorias e decisões judiciais, realizou-se uma análise acerca de cada esfera do dano causado, onde se busca avaliar de forma prática o valor de um dado vazado. Cada tipo de dado tem um potencial danoso específico, mas, quando efetivada a lesão, seus efeitos tendem a ferir a pessoa tanto no contexto material, ligado a valor monetário e uma perda concreta, quanto no âmbito moral, que a afeta em uma perspectiva subjetiva e emocional. O estudo explora a ideia de responsabilidade civil, principalmente após a Lei Geral de Proteção de Dados (LGPD), que criou obrigações para quem controla e opera dados, além de determinar punições administrativas e a criação de órgãos reguladores. Por último, ao avaliar como calcular o valor dos danos, a partir de jurisprudência recente, é possível concluir que a proteção precisa se desenvolver em diversos aspectos, com o intuito de garantir uma compensação justa para os dados pessoais difundidos sem autorização.

**Palavras-chave:** Vazamento de dados. Responsabilidade civil. Dados sensíveis. LGPD.

## DATA BREACH AND CIVIL LIABILITY: THE CONCRETE VALUE OF PERSONAL DATA

**Abstract:** This research addresses the leakage of personal data from the perspective of contemporary Brazilian law, with an emphasis on measuring the effects of applying civil liability to the issue. After defining what constitutes personal data and its connection to the right to privacy, based on legal theories and court decisions, an analysis was carried out on each sphere of the damage caused, aiming to practically assess the value of leaked data. Each type of data has a specific harmful potential; however, when a violation occurs, its effects tend to impact the individual both in a material sense, related to monetary value and tangible loss, and in a moral sense, affecting the person from a subjective and emotional standpoint. The study explores the concept of civil liability, especially following the enactment of the General Data Protection Law (LGPD), which established obligations for data controllers and processors, as well as administrative penalties and the creation of regulatory bodies. Finally, by examining recent case law on how to calculate damage values, the study concludes that data protection must evolve in various aspects to ensure fair compensation for personal data disclosed without authorization.

**Key words:** Data breach. Civil liability. Sensitive data. LGPD.

---

<sup>1</sup> Acadêmico do 9º período do Curso de Bacharelado em Direito - UniSecal - E-mail: vfbw17@gmail.com

<sup>2</sup> Professor especialista em Direito Digital e Lei Geral de Proteção de Dados do Centro Universitário Santa Amélia - Unisecal - e-mail zenardi.adv@gmail.com

## 1 INTRODUÇÃO

Em uma realidade onde praticamente todas as relações estão migrando para a internet, sejam privadas ou públicas, desde algo simples, como a compra de um eletrodoméstico online, até algo mais formal como o peticionamento de uma ação judicial, demonstra-se um cenário em que a tecnologia se tornou uma ferramenta onipresente e essencial para o cotidiano.

Dada essa perspectiva e a necessidade de evitar fraudes que não ocorreriam em tratativas presenciais, os órgãos ou empresas solicitam e armazenam dados que, em condições normais, não ficaram sobre sua posse, seja a digitalização de um documento de identidade, uma impressão digital ou até mesmo parâmetros referentes ao reconhecimento facial do indivíduo.

O risco associado à crescente coleta e disseminação de dados pessoais no ambiente digital tem evidenciado, mesmo que gradativamente, a relevância dessas informações, tanto para o usuário comum quanto para a sociedade como um todo.

À mesma medida que a busca por praticidade nas relações digitais se intensifica, também aumentam os casos de exposição indevida de informações, o que, inevitavelmente, gera conflitos de interesse e aumenta o volume de demandas que avançam para a esfera judicial.

Consequentemente, a relevância deste tema para o Direito brasileiro é proporcional, pois ele passa a ser questionado e precisa oferecer respostas jurídicas adequadas aos obstáculos apresentados.

Diante desse contexto, surge a seguinte problemática: seria possível estabelecer critérios objetivos e padronizados para a quantificação do dano resultante do vazamento de um dado pessoal no Brasil?

Nesta pesquisa, o parâmetro adotado foi a metodologia qualitativa, onde há embasamento em pesquisas bibliográficas, como também na pesquisa documental, a partir de análise jurisprudencial e dispositivos previstos em lei.

Inicialmente, serão apresentados os conceitos básicos das áreas correlacionadas, principalmente no que se refere a dados pessoais e sua ligação intrínseca com o direito à privacidade, baseando-se nas ideias de autores como Danilo Doneda (2021), que defende uma proteção de dados robusta, equivalente a um direito fundamental.

A pesquisa avança com a diferenciação entre o dano material e o dano moral. Cada tipo de dado, seja sozinho ou combinado a outras informações, tem um potencial distinto de causar dano, mas, quando é efetivado, as consequências costumam afetar tanto no âmbito financeiro quanto na esfera mais íntima do indivíduo. A partir de Sergio Cavalieri Filho (2012) é possível realizar uma análise atemporal do conceito de responsabilidade civil, o que auxilia na compreensão do “dever de indenizar”.

Atentando-se especialmente às alterações introduzidas pela Lei Geral de Proteção de Dados (LGPD), que estabelece obrigações para as entidades que manipulam dados sigilosos e, até certo ponto, pune as violações. Nesse ponto, a análise se conecta com os estudos de Bruno Bioni e Daniel Dias (2020), que ligam a LGPD ao Código de Defesa do Consumidor, ressaltando a necessidade de uma proteção eficaz e adaptada.

Por fim, a base teórica é contraposta à jurisprudência e julgados recentes, com a análise do acórdão proferido no Agravo em Recurso Especial nº 2.130.619/SP, julgado pelo Superior Tribunal de Justiça (STJ), e de outras ações julgadas pelo TRF3 e TJPR.

Portanto, o foco é compreender, em um aspecto mais amplo, como a legislação vigente, a doutrina e a esfera judicial interpretam a proteção das informações pessoais, de que forma avaliam e reparam os prejuízos decorrentes da sua exposição. Desta forma, busca-se estabelecer um padrão sobre os entendimentos e analisar possíveis divergências.

## **2 OS DADOS PESSOAIS E O DIREITO À PRIVACIDADE**

Antes de iniciar uma abordagem mais aprofundada, deve-se observar que será tratado sobre um tema que conecta diversas áreas do conhecimento. Ao analisar tão somente os aspectos e conceitos jurídicos, a visualização gerada não seria suficiente para formular uma compreensão plena do assunto em questão, o valor concreto de um dado pessoal.

Intrinsecamente relacionado a tecnologia, a vulnerabilidade vinculada ao armazenamento de dados em geral e o risco associado à facilidade da difusão de informações no ambiente virtual são situações fundamentais para contextualizar o problema.

Dessa forma, os conceitos básicos e fundamentais de cada ramo serão abordados inicialmente, partindo do princípio de que um tema recente, complexo e intrincado será discutido.

## 2.1. DADO PESSOAL: DEFINIÇÃO E APLICABILIDADE

O “dado pessoal” é um termo chave que pode ser definido a partir de múltiplos conceitos, porém, para esta pesquisa, sua definição terá como base o que pode-se extrair diretamente da legislação brasileira.

Embora a Constituição Federal de 1988 não aborde explicitamente ou indique uma concepção para a expressão citada, há leis complementares atuais que têm este tema como objeto principal. Por exemplo, a Lei Geral de Proteção de Dados Pessoais (LGPD), que teve o início de sua vigência gradualmente entre 2018 e 2021.

Segundo o art. 5º da LGPD, os dados pessoais são descritos como qualquer “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018). Ou seja, esses dados englobam as informações que ao serem utilizadas, isoladamente ou em conjunto, tornam possível reconhecer e indicar um indivíduo particular.

A lei não apresenta um rol taxativo para o conteúdo das informações comuns protegidas, portanto, não há uma lista de opções fixas e determinadas que sirvam como base para mensurar a abrangência do conceito.

Partindo desta análise, é possível observar que a interpretação consegue abarcar tanto a proteção dos dados que eram a preocupação no passado quanto legislar sobre novas informações que poderiam não existir na época ou que ainda não haviam sido mapeadas como relevantes pela sociedade.

Segundo Danilo Doneda (2011, p.93-94), jurista brasileiro que teve destaque durante a elaboração da LGPD e ex-membro do conselho da Agência Nacional de Proteção de Dados (ANPD), a compreensão dos dados pessoais transcendem a mera identificação imediata.

Em paralelo ao disposto em lei, o autor defende e disserta sobre o conceito de que os dados pessoais são informações capazes de identificar um indivíduo, seja de forma direta ou indireta.

A identificação de um indivíduo pode ocorrer indiretamente quando uma informação isolada não é suficiente para produzir o resultado, porém, ao ser unido a outras informações, torna possível identificar uma pessoa. (DONEDA, 2011, p.92)

Para Doneda (2011, p. 92), vivemos atualmente em um contexto onde enormes volumes de dados são coletados, armazenados e processados a todo momento. Essas informações passam a assumir uma posição de proeminência, sendo vistas praticamente como uma extensão da própria personalidade do sujeito.

A analogia do doutrinador sugere que os dados pessoais não são mais meras informações sem valor, mas elementos intimamente vinculados à identidade e à dignidade do ser humano.

Com base na lei, podemos distinguir os dados em dois tipos: os dados comuns e os dados sigilosos. Segundo o art. 5º, II, da Lei Geral de Proteção de Dados (LGPD), dados sensíveis são aqueles que se referem à:

Origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além de dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural. (BRASIL, 2018)

Esses dados, diferentemente dos mais comuns, exigem um nível maior de sigilo e proteção, por sua capacidade de gerar discriminação ou afetar a dignidade do usuário. Como explica a Diretora da ANPD, Miriam Wimmer (2021):

Os dados sensíveis demandam maior cautela no tratamento justamente por seu potencial de causar danos mais graves ao titular, seja por afetar sua esfera íntima, seja por possibilitar formas de exclusão ou preconceito. (p.115)

Dessa forma, estabelecendo um paralelo com o direito à privacidade, proteger esses dados significa também preservar os direitos fundamentais do indivíduo, reconhecendo a abordagem subjetiva e o seu valor na construção da identidade.

Portanto, desde dados mais básicos da pessoa, como, por exemplo, nome completo e CPF, e até dados mais específicos, como o que o indivíduo consome ou busca na internet, são informações protegidas, que não podem ser compartilhadas sem o consentimento expresso do proprietário, em virtude da proteção estabelecida pelas legislações complementares e de direitos fundamentais.

## 2.2 DO DIREITO À PRIVACIDADE

A garantia à privacidade é um direito fundamental assegurado pela Constituição Federal de 1988, previsto no artigo 5º, inciso X, onde a intimidade, a vida privada, a honra e a imagem das pessoas são protegidas e consideradas invioláveis. (BRASIL, 1988)

Ao discutir a privacidade no ambiente digital, é possível traçar um paralelo com a aplicação desse conceito no mundo real. Por lei, nem mesmo o Estado, por meio do poder de polícia, pode ter livre acesso ao lar de um indivíduo, pois é necessária uma motivação concreta e/ou uma decisão judicial que valide a realização de tal ato.

Diferentemente, dentro do ambiente digital, é possível observar que a intimidade do indivíduo é frequentemente tratada como um produto pelas empresas, suprimida por decisões unilaterais do Estado e sujeita a invasões maliciosas em virtude das vulnerabilidades presentes na rede virtual.

Por exemplo, pode-se citar os dados coletados e armazenados pelas empresas, com base nos hábitos de consumo e preferências dos usuários, são vendidos constantemente para personalização e filtragem de anúncios publicitários.

Nesse sentido, Alexandre Veronese (2021, p.116) ressalta que a privacidade precisa ser vista como um direito que se adapta e varia conforme o contexto, demandando uma nova abordagem legal, considerando a grande quantidade de dados pessoais que as plataformas digitais possuem.

Para Veronese (2021), a autodeterminação informativa, ou seja, o poder do titular decidir sobre o uso de seus dados, deve ser protegida, como reflexo direto da dignidade da pessoa humana:

Nesse sentido, nada melhor do que começar com o princípio da dignidade da pessoa humana e duas de suas principais – para a proteção de dados pessoais – expressões, designadamente, o direito ao livre desenvolvimento da personalidade e o direito à livre autodeterminação informativa. (p.62)

Em que pese não se tratar de premissa válida para todos os direitos fundamentais, porquanto nem todo direito fundamental tenha um fundamento direto e um conteúdo em dignidade, no caso do direito à proteção dos dados pessoais, o princípio da dignidade da pessoa humana pode e deve ser acionado, seja para a justificação da fundamentalidade daquele direito, seja para a determinação de parte de seu conteúdo, com destaque para a identificação de alguns pontos de contato com outros princípios e direitos fundamentais. (p.62-63)

Desse modo, a proteção jurídica da privacidade surge como um instrumento crucial para equilibrar as relações entre indivíduos e organizações públicas/privadas no ambiente digital, exigindo responsabilidade na gestão de dados confidenciais.

### **3 O VÍNCULO ENTRE O DANO E A VIOLAÇÃO À PRIVACIDADE**

Antes de abordar sobre o dano em si, que trata-se de um conceito acessório, é necessário compreender o objeto principal, o que é um bem jurídico. Carlos Roberto Gonçalves (2012, p.141, 200-203), em sua doutrina de noções do direito civil, define bens jurídicos como qualquer coisa com valor material ou imaterial que a lei protege, sendo a vida humana o “bem supremo”. Essa proteção se apresenta como um dos pilares para o convívio em sociedade.

A noção de dano abrange a lesão a um bem jurídico protegido, resultando em prejuízo para seu possuidor. Tal lesão pode ser de caráter patrimonial, impactando os bens econômicos do indivíduo, ou extrapatrimonial, afetando direitos da personalidade, como honra, imagem, saúde e, especialmente relevante para o tema em questão, a privacidade. (GUERRA & BENACCHIO, 2015, p.77)

Cavaliere Filho (2012) afirma que o dano é "a subtração ou diminuição de um bem jurídico, qualquer que seja a sua natureza, quer se trate de um bem patrimonial, quer se trate de um bem integrante da própria personalidade da vítima, como a honra, a imagem, a liberdade, a saúde, a integridade física e psíquica". (p.77)

A privacidade, como um direito fundamental e autônomo, encontra amparo em diversas legislações e instrumentos. Sua violação, por si só, pode configurar um dano, mesmo que não haja um prejuízo econômico direto demonstrável. Isso porque a invasão da esfera privada de um indivíduo atinge um valor intrínseco à sua dignidade e autonomia. (DONEDA, 2019, p.43)

Doneda (2019, p. 156-158), ao discutir a proteção de dados pessoais, argumenta que a violação da privacidade pode gerar danos de diversas ordens, desde o constrangimento e a angústia até prejuízos materiais decorrentes do uso indevido de informações. O autor destaca a importância de reconhecer o dano existencial, aquele que afeta o projeto de vida do indivíduo, como uma possível consequência da violação de dados.

#### **4 DA RESPONSABILIDADE CIVIL E O DEVER DE INDENIZAR**

A responsabilidade civil é um dos principais conceitos tratados na esfera do Direito Civil, que tem como objetivo principal, simplificadamente, estabelecer o dever de reparar os danos causados a outra pessoa.

Aplicando ao tema da pesquisa o que está descrito no artigo 927 do Código Civil Brasileiro de 2002, qualquer pessoa física ou jurídica, que por ação, violar direito e causar dano a outrem, tem o dever de indenizá-la. O dever de indenizar tem caráter reparatório, ou seja, tem como objetivo ressarcir a pessoa que foi lesada.

Existem diferentes tipos de responsabilidade civil, sendo os principais a responsabilidade civil subjetiva e a objetiva. A responsabilidade civil subjetiva é baseada na prova de culpa, seja dolo ou culpa. Já a responsabilidade civil objetiva independe da prova de culpa e está fundamentada no risco da atividade desenvolvida. (FILHO, 2012, p.17-18)

#### **4 A PROTEÇÃO DE DADOS PESSOAIS NA LEGISLAÇÃO BRASILEIRA**

O ordenamento jurídico brasileiro tem à disposição normas de caráter geral que, embora anteriores à expansão do ambiente virtual, seguem sendo fundamentais para a proteção dos direitos da personalidade.

A Constituição Federal de 1988 (CF), que dá origem a esses direitos como fundamentais, e o Código Civil de 2002 (CC), ao tratar da responsabilidade civil e dos direitos da personalidade, fornecem bases sólidas para a interpretação e aplicação do direito em qualquer ambiente.

Já no contexto das relações virtuais, se destacam dois marcos legais centrais: o Marco Civil da Internet, que estabelece princípios e diretrizes para o uso da rede no Brasil, e a Lei Geral de Proteção de Dados (LGPD), que regula o tratamento de dados pessoais, tanto no setor público quanto no privado.

##### **4.1 MARCO CIVIL DA INTERNET**

O Marco Civil da Internet (Lei nº 12.965/2014) é amplamente reconhecido como a "Constituição da Internet" no Brasil, um marco regulatório que "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil". (BRASIL, 2014)

Entre os objetivos centrais do Marco Civil, encontra-se a criação de um arcabouço regulatório, com a finalidade primordial de assegurar a plena liberdade de expressão. (SOUZA & LEMOS, 2016, p.22-23)

Adicionalmente, a lei busca garantir a inviolabilidade da privacidade dos usuários, protegendo seus dados pessoais e comunicações online contra acessos e usos indevidos.

Outro princípio estrutural estabelecido pelo Marco Civil é o da neutralidade da rede, que assegura que todo tráfego de dados na internet seja tratado de forma isonômica, sem discriminação ou priorização baseada em conteúdo, origem, destino ou serviço, garantindo assim uma internet aberta e plural. (SOUZA & LEMOS, 2016, p.115-116)

#### 4.2 LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), referenciada pela sigla LGPD, surgiu possuindo como um de seus objetivos o de complementar o marco civil da internet, em um contexto onde era necessário regulamentar uma nova realidade e aprimorar conceitos ainda pouco explorados, proporcionando, assim, “diretrizes para o tratamento de dados pessoais, [...], realizado por pessoa natural ou por pessoa jurídica de direito público ou privado”. (SOUZA, 2020, p.300)

A LGPD estabelece que o tratamento de dados pessoais deve ocorrer somente mediante consentimento do titular, ou nas hipóteses previstas em lei. O objetivo da LGPD é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. (TEPEDINO & TEFFÉ, 2020, p.209).

Vale ressaltar que ao tratar de LGPD e vazamento de informações pessoais, a responsabilidade das entidades é objetiva, devendo reparar o dano causado, sejam elas privadas ou públicas.

Esta abordagem assegura, em um primeiro momento, que as instituições tenham um incentivo a adotar medidas eficazes de proteção de dados, como também, agrega valor ao material manipulado e a intimidade do usuário.

#### **4.2.1 DAS MULTAS ADMINISTRATIVAS**

A LGPD, através do artigo 55-A, estabelece a criação da Autoridade Nacional de Proteção de Dados (ANPD), que tem a permissão de impor sanções a indivíduos ou empresas que não cumprirem as normas durante o processamento de dados, vide art. 52 da mesma lei. (BRASIL, 2018) Essas penalidades pecuniárias servem como uma medida que visa evitar comportamentos inadequados e incentivar a busca pela proteção de dados.

A penalidade mais comuns são a advertência e a multa simples, esta que pode chegar a até 2% da receita da empresa ou do grupo econômico no Brasil, com um limite de R\$ 50 milhões por violação. Contudo, a aplicação das multas deve seguir o processo legal adequado, garantir o direito à defesa e observar aos princípios, conforme o §1º do art. 52 da LGPD. (BRASIL, 2018)

Ademais, a LGPD define que as sanções devem levar em conta aspectos como o grau de dano e o tipo da infração, boa-fé do agente, a reincidência, a existência de políticas internas de gestão e supervisão. Isso significa que o “agente de tratamento de dados” que buscam boas práticas ou tem um preparo pré-planejado para solucionar os problemas, podem ter suas punições reduzidas.

Neste mesmo sentido, de acordo com Danilo Doneda (2021):

“As multas previstas na LGPD não têm apenas o caráter de punição, mas exercem uma função pedagógica e preventiva, sendo instrumentos de pressão para que os agentes de tratamento adotem condutas mais diligentes em relação aos dados pessoais.” (p.198)

Além da multa e advertência, a LGPD contempla outras sanções administrativas, como o bloqueio ou a exclusão de informações, e a divulgação pública da infração. A definição da medida dependerá do grau de impacto da violação sobre os direitos dos indivíduos e da atitude do agente de tratamento.

#### **5 A RESPONSABILIDADE CIVIL VINCULADA ÀS RELAÇÕES VIRTUAIS**

No contexto das relações virtuais, a responsabilidade civil assume uma perspectiva distinta, considerando o risco de danos vinculados ao uso impróprio das informações e a omissão de cuidados ou negligência durante o armazenamento.

Casos de violação de privacidade e compartilhamento de dados pessoais são comuns, e a legislação busca assegurar que os direitos dos indivíduos sejam

respeitados. Sobre a LGPD e a responsabilidade civil, argumentam Bioni e Dias (2020):

A LGPD estabelece duas hipóteses para a configuração da responsabilidade civil dos agentes de tratamento de dados: a “violação à legislação de proteção de dados pessoais” e a “violação da segurança dos dados”. Ambos são calibrados pela noção de tratamento irregular, previsto no artigo 44, o qual procura sistematizar critérios para aferição da culpa dos agentes de tratamento de dados a esse respeito. Ressalta-se desde logo, contudo, que não parece haver razão para tal bifurcação, uma vez que as consequências são as mesmas (obrigação de indenizar) e, em especial, que essas duas hipóteses de responsabilidade civil são reunidas no artigo 44 sob a noção ampla de “tratamento irregular” (p.9)

Sendo um tema de crescente importância para o direito brasileiro, as disposições do Marco Civil da Internet e da LGPD buscam fornecer uma base normativa sólida para a proteção desses direitos, impondo responsabilidades e sanções claras e objetivas aos controladores/operadores de dados.

A responsabilidade civil objetiva aplicada, portanto, é um mecanismo essencial para assegurar que as violações sejam evitadas, pois torna interessante ao agente desenvolver ferramentas para a segurança das informações e, eventualmente, retira a possibilidade de discutir a culpa da entidade sobre o incidente.

Para além da esfera administrativa, partindo de uma perspectiva do indivíduo, quando efetivado um episódio de vazamento de dados, pode-se analisar o dano causado ao usuário comum a partir de duas segmentações principais: o dano material e o dano moral.

## 5.1 DA VALORAÇÃO DO DANO MATERIAL

O dano material pode ser compreendido como toda perda concreta que atinge o patrimônio de uma pessoa, seja ela física ou jurídica. É o prejuízo que se reflete no âmbito financeiro/monetário do indivíduo. (CAVALIERI, 2012, p.183-184)

Quando os dados pessoais de um indivíduo são indevidamente vazados, o dano material, pelo menos, se manifesta de forma objetiva. Os dados bancários, informações de cartão de crédito e CPF podem ser utilizados por terceiros para praticar fraudes, como compras não autorizadas, abertura de contas em banco e financiamentos.

Neste mesmo sentido, Nelson Rosenvald (2020) afirma:

O dano material decorrente da violação à proteção de dados pode ser perfeitamente demonstrado, sobretudo quando há uso fraudulento da identidade digital do titular, o que gera consequências patrimoniais diretas, como saques, compras ou contratação de empréstimos indevidos. (p.243)

Assim, a valoração do dano material deve levar em conta não apenas o valor financeiro imediato perdido, mas também os custos adicionais e o impacto no cotidiano da vítima.

## 5.2 DA VALORAÇÃO DO DANO MORAL

Como já abordado anteriormente, o dano moral consiste na lesão aos direitos da personalidade, afetando a esfera íntima e psicológica do indivíduo, como honra, imagem e privacidade, causando dor, sofrimento ou humilhação. (CAVALIERI, 2012, p.187-189) O vazamento ou comércio indevido de dados pessoais representa uma violação desses direitos, expondo informações privadas e sensíveis.

Essa exposição pode gerar diversas consequências danosas, como constrangimento, discriminação, assédio, roubo de identidade e fraudes financeiras, caracterizando o dano moral pela ofensa à dignidade e aos direitos do titular dos dados.

## 6 ESTUDOS DE CASO E JURISPRUDÊNCIA

Com o passar do tempo, devido a rapidez do progresso tecnológico, não há como desconsiderar a influência da tecnologia no cotidiano, aberturas de contas em bancos digitais com pouco clicks, migração de serviços que antes ocorriam fisicamente passando para ambiente digital, como guias de IPTU e processos judiciais.

Nesse cenário, o tratamento inadequado de dados pessoais e os consequentes vazamentos tornam-se temas recorrentes na esfera judicial. A análise de decisões recentes é fundamental para compreender como os tribunais vêm aplicando os princípios da responsabilidade civil e as disposições da LGPD na reparação dos danos causados aos titulares de dados.

A seguir, serão apresentados alguns estudos de caso e jurisprudência que ilustram, de maneira prática, sobre a matéria, permitindo avaliar a aplicabilidade da norma e se os ideais expressos na doutrina refletem na prática.

## 6.1 Análise Jurisprudencial: Agravo em Recurso Especial nº 2.130.619 - SP

Uma das decisões mais relevantes que aborda sobre o assunto foi a proferida no Agravo em Recurso Especial nº 2.130.619 - SP (2022/0152262-2) pela Segunda Turma do STJ, cujo relator era o Ministro Francisco Falcão:

PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO.

I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais.

II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa.

III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente:

AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020.

IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis.

V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.

VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido.

(AREsp n. 2.130.619/SP, relator Ministro Francisco Falcão, Segunda Turma, julgado em 7/3/2023, DJe de 10/3/2023.)

Tratava-se de uma ação de indenização por dano moral movida por um particular contra uma concessionária de energia elétrica, em decorrência do vazamento de dados pessoais.

O Tribunal de Justiça do Estado de São Paulo havia reformado a sentença de primeira instância para condenar a concessionária ao pagamento de indenização, mas, a partir da interposição do recurso para instância superior, o Superior Tribunal de Justiça (STJ) deu parcial provimento ao recurso especial.

O STJ decidiu que o vazamento de dados pessoais, por si só, não gera dano moral presumido, sendo necessária a comprovação do dano efetivo pelo titular dos dados, vide grifo:

O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.

Diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural. (p.10-11)

Além disso, o Tribunal diferenciou dados pessoais comuns de dados pessoais sensíveis, conforme a Lei Geral de Proteção de Dados (LGPD), esclarecendo que o tratamento e a indenização por vazamento podem variar dependendo de sua natureza.

No caso em questão, os dados vazados foram considerados comuns, e não houve comprovação de dano moral que justificasse a indenização. Assim, a decisão unânime do STJ reforça a necessidade de comprovação de efetivo dano à honra, dignidade ou atributo da personalidade para que se configure o dano moral indenizável em casos de vazamento de dados pessoais.

## 6.2 ESTUDO DE CASO: AÇÃO CIVIL PÚBLICA CONTRA A SERASA S.A.

Em janeiro de 2021, tornou-se público um dos maiores vazamentos de dados pessoais já registrados no Brasil, envolvendo a Serasa S.A. e mais de 223 milhões de CPFs, onde foram revelados inclusive documentos de pessoas já falecidas. (MPF, 2023)

Em resposta ao ocorrido, o Ministério Público Federal (MPF), em conjunto com o Instituto Sigilo, propôs uma Ação Civil Pública contra a empresa, o qual pode

ser consultado sob o nº 5002936-86.2021.4.03.6100, atualmente em tramitação no Tribunal Regional Federal da 3ª Região.

A ação foi motivada por indícios de que a Serasa estaria comercializando, de forma indevida, dados sensíveis e pessoais por meio de plataformas como “Lista Online”, “Prospecção de Clientes” e “Lista PEP”, práticas que afrontam diretamente a LGPD e o Marco Civil da Internet. (MPF, 2023)

Dado o contexto, o MPF pleiteou a condenação da empresa ao pagamento de uma indenização no valor de 30 mil reais para cada pessoa afetada pelo episódio, além de uma multa coletiva de, no mínimo, R\$ 200 milhões (valor que pode chegar a até 10% do faturamento anual da Serasa). (MPF, 2023)

A ação também voltou-se contra a ANPD, que, segundo o MPF (2023), teria cometido omissão quanto ao seu papel de fiscalização e controle preventivo, contribuindo com a ocorrência do acontecimento.

A sentença proferida no caso extinguiu o processo sem resolução do mérito, com base na falta de legitimidade ativa do Instituto Sigilo, autor da ação. O juízo entendeu que a associação possuía um objeto social genérico, sem comprovação de vínculo com um grupo específico ou lesado, nem demonstração de representação efetiva de titulares afetados.

### 6.3 ANÁLISE DE JULGADOS: PADRÕES DECISÓRIOS DO TRIBUNAL DE JUSTIÇA DO PARANÁ (TJPR)

Com o objetivo de compreender como a jurisprudência paranaense tem tratado os casos de vazamento de dados pessoais, serão analisadas duas decisões recentes proferidas pela 2ª Turma Recursal do Tribunal de Justiça do Estado do Paraná:

RECURSO INOMINADO. BANCÁRIO. INVESTIMENTO EM PREVIDÊNCIA PRIVADA. EXPOSIÇÃO DE INFORMAÇÕES PARA TERCEIRO. **DADOS PESSOAIS NÃO CLASSIFICADOS COMO SENSÍVEIS (LGPD, ART. 5º, II). DANO MORAL QUE NÃO É PRESUMIDO.** NECESSIDADE DO TITULAR DOS DADOS COMPROVAR EVENTUAL DANO DECORRENTE DA EXPOSIÇÃO DESSAS INFORMAÇÕES. AUSÊNCIA DE PROVA DE PREJUÍZO CONCRETO EM RAZÃO DA DIVULGAÇÃO. DANOS MORAIS AFASTADOS. RECURSO DO AUTOR NÃO CONHECIDO. RECURSO DO RÉU PROVIDO.

(TJPR - 2ª Turma Recursal - 0001835-32.2023.8.16.0184 - Curitiba - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS ALVARO RODRIGUES JUNIOR - J. 26.07.2024)

RECURSO INOMINADO. VAZAMENTO DE DADOS. LEGITIMIDADE PASSIVA ANALISADA A PARTIR DA TEORIA DA ASSERTÃO. EXPOSIÇÃO DE INFORMAÇÕES PARA TERCEIROS. **DADOS PESSOAIS NÃO CLASSIFICADOS COMO SENSÍVEIS (LGPD, ART. 5º, II). DANO MORAL QUE NÃO É PRESUMIDO**. NECESSIDADE DO TITULAR DOS DADOS COMPROVAR EVENTUAL DANO DECORRENTE DA EXPOSIÇÃO DESSAS INFORMAÇÕES. **VERIFICADO PREJUÍZO CONCRETO EM RAZÃO DA DIVULGAÇÃO**. DANOS MORAIS MANTIDOS. DEVER DA RÉ EM SUSPENDER O CONTATO DE TERCEIROS COM O AUTOR. OBRIGAÇÃO IMPOSSÍVEL. RECURSO PARCIALMENTE PROVIDO.

(TJPR - 2ª Turma Recursal - 0032691-19.2022.8.16.0182 - Curitiba - Rel.: JUIZ DE DIREITO DA TURMA RECURSAL DOS JUIZADOS ESPECIAIS ALVARO RODRIGUES JUNIOR - J. 11.03.2025)

Ambas tratam de situações em que houve o compartilhamento indevido de dados pessoais, mas não sensíveis, conforme a definição do artigo 5º, inciso II, LGPD. Em comum, os julgados reforçam o entendimento de que o simples vazamento de dados, por si só, não configura automaticamente o dever de indenizar por dano moral. Para que se reconheça a reparação civil, exige-se a demonstração de prejuízo concreto que decorra diretamente da exposição indevida das informações.

A comparação entre os casos evidencia um padrão decisório alinhado à jurisprudência do Superior Tribunal de Justiça (STJ), que distingue os dados comuns dos sensíveis e exige, nos primeiros, a comprovação de impacto real à honra, intimidade ou integridade do indivíduo para fins de responsabilização civil. O critério predominante não é apenas a ocorrência do vazamento, mas os efeitos que este gerou na vida do titular.

## 7 CONSIDERAÇÕES FINAIS

Esta pesquisa teve como objetivo investigar a problemática do vazamento de dados pessoais sob o prisma da responsabilidade civil no sistema jurídico brasileiro atual, principalmente após a implementação da Lei Geral de Proteção de Dados (LGPD).

Através de uma análise que uniu teoria e decisões judiciais, notou-se que, apesar da principal linha de pensamento doutrinária tender a ver os dados pessoais como uma extensão da individualidade e, por consequência, como bens jurídicos que demandam alta proteção, a prática dos tribunais, em especial com o acórdão

proferido no Agravo do Recurso Especial nº 2.130.619/SP, ainda se mostra menos abrangente e protecionista no que se refere à reparação por danos morais decorrentes do simples vazamento indevido de dados.

Autores como Danilo Doneda e Miriam Wimmer defendem uma proteção mais objetiva e preventiva das informações pessoais, ressaltando sua ligação essencial com a existência humana e a relevância de se reconhecer o dano moral automático, sobretudo quando se tratam de dados de natureza sensível.

Em contrapartida, o entendimento jurisprudencial verificado no julgamento do STJ e do TJPR diverge dessa linha de raciocínio ao exigir a demonstração real do prejuízo sofrido para que se conceda indenização por dano moral, principalmente quando os dados que foram expostos são considerados como "comuns".

Tal interpretação cria uma dificuldade prática à proteção eficaz dos donos dos dados, visto que, em diversas situações, os efeitos do vazamento só aparecem em um momento futuro ou se manifestam de maneira particular e difícil de comprovar.

Dessa forma, conclui-se que há um distanciamento entre a doutrina, que avança no sentido de uma defesa mais efetiva e indenizatória, e a jurisprudência, que assume uma postura menos punitiva. Esse contraste revela a necessidade de aperfeiçoamento da compreensão judicial sobre a proteção de dados pessoais, para que os princípios constitucionais da dignidade da pessoa humana e da privacidade possam ser plenamente concretizados no ambiente digital atual.

Finalmente, como resultado para a problemática, pode-se verificar que não é possível estabelecer parâmetros objetivos para construir o valor concreto de um dado pessoal, pois o cenário revelado pela jurisprudência, que é instável e incerto, depende integralmente do magistrado para reconhecer que houve prejuízo ao indivíduo, se há direito ou não. Portanto, mesmo que seja reconhecido o dano, a indenização vai variar conforme o grau do prejuízo.

## REFERÊNCIAS

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Diário Oficial da União, Brasília, DF. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)>. Acesso em: 22 nov. 2025.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619 - SP (2022/0152262-2)**. Relator: Ministro Francisco Falcão, 7 de março de 2023. Disponível em: <[https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num\\_registro=202201522622&dt\\_publicacao=10/03/2023](https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023)>. Data de acesso: 15 abr. de 2025.

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. Civillistica.com. Rio de Janeiro, a. 9, n. 3, 2020.

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

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico: Journal of Law, v. 12, n. 2, p. 91-108, 2011. Disponível em: <<https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>>. Acesso em: 20 maio de 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** Fundamentos da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Revista dos Tribunais, 2019

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso Pereira de. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Revista dos Tribunais (Thomson Reuters Brasil), 2019.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro, Volume 1:** Parte Geral. 10. ed. São Paulo : Saraiva, 2012. Disponível em: <<https://direitouninoveest.wordpress.com/wp-content/uploads/2016/03/direito-civil-brasileiro-2012-vol-1-parte-geral-carlos-roberto-gonc3a7alves.pdf>>. Acesso em: 18 nov. de 2024.

GUERRA, Alexandre Dartanhan de Mello; BENACCHIO, Marcelo. **Responsabilidade civil.** São Paulo: Escola Paulista da Magistratura, 2015. Disponível em: <<https://www.tjsp.jus.br/Download/EPM/Obras/ResponsabilidadeCivil.pdf>>. Acesso em: 20 nov. de 2024.

MINISTÉRIO PÚBLICO FEDERAL. **MPF requer da Serasa o pagamento de multa superior a R\$ 200 milhões por vazamento de dados pessoais.** Sala de Imprensa – São Paulo, 05 dez. 2023. Disponível em: <<https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/mpf-requer-da-serasa-o-pagamento-de-multa-superior-a-r-200-milhoes-por-vazamento-de-dados-pessoais.>>. Acesso em: 01 jun. 2025.

ROSENVALD, Nelson. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2020.

SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. **Marco civil da internet:** construção e aplicação. Editar, 2016. Disponível em: <[https://itsrio.org/wp-content/uploads/2017/02/marco\\_civil\\_construcao\\_aplicacao.pdf](https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf)>. Acesso em: 18 nov. de 2024.

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. **Apelação Cível nº 0032691-19.2022.8.16.0182,** Rel. Des. José Laurindo de Souza Netto, 4ª Câmara Cível, julgado em 16 maio 2023. Curitiba: TJPR, 2023. Disponível em: <<https://portal.tjpr.jus.br/jurisprudencia/j/2100000031358151/Ac%C3%B3rd%C3%A3o-0032691-19.2022.8.16.0182.>> Acesso em: 01 jun. 2025.

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. **Apelação Cível nº 0001835-32.2023.8.16.0184,** Rel. Des. Ruy Muggiati, 5ª Câmara Cível, julgado em 22 fev. 2024. Curitiba: TJPR, 2024. Disponível em: <<https://portal.tjpr.jus.br/jurisprudencia/j/2100000027994921/Ac%C3%B3rd%C3%A3o-0001835-32.2023.8.16.0184.>>. Acesso em: 01 jun. 2025.

VERONESE, Alexandre Bahia. **Direito fundamental à privacidade e proteção de dados pessoais.** In: PINHEIRO, Patrícia Peck; BIONI, Bruno Ricardo (orgs.). Tratado de Proteção de Dados Pessoais. São Paulo: Thomson Reuters Brasil, 2021.

WIMMER, Miriam. **Proteção de Dados Pessoais:** A Função e os Desafios da Regulação. São Paulo: Revista dos Tribunais, 2021.