



**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
FACULDADE DE DIREITO**

**A Responsabilidade Civil de Fornecedores de Tecnologia no Vazamento de
Dados: Desafios e Implicações no Direito Digital**

Karina Vidal Onófrío
Prof^a. Dr^a. Nathaly Campitelli Roque

SÃO PAULO
2024

KARINA VIDAL ONÓFRIO

RA00285683

**A Responsabilidade Civil de Fornecedores de Tecnologia no Vazamento de
Dados: Desafios e Implicações no Direito Digital**

Projeto de Monografia apresentado à Faculdade de Direito da Pontifícia Universidade Católica de São Paulo, pela graduanda Karina Vidal Onófrío, como Trabalho de Conclusão de Curso (TCC) sob orientação da Professora Doutora Nathaly Campitelli Roque.

SÃO PAULO

2024

Sistemas de Bibliotecas da Pontifícia Universidade Católica de São Paulo -
Ficha Catalográfica com dados fornecidos pelo autor

Vidal Onófrio, Karina
A Responsabilidade Civil de Fornecedores no Vazamento de
Dados: Desafios e Implicações no Direito Digital. / Karina
Vidal Onófrio. -- São Paulo: [s.n.], 2024.
p. ; cm.

Orientador: Nathaly Campitelli Roque.
Trabalho de Conclusão de Curso (Graduação) -- Pontifícia
Universidade Católica de São Paulo, Graduação em Direito,
2024.

1. Responsabilidade Civil. 2. LGPD. 3. Fornecedores. 4.
Indenização Civil.. I. Campitelli Roque, Nathaly . II.
Pontifícia Universidade Católica de São Paulo, Trabalho de
Conclusão de Curso para Graduação em Direito. III. Título.

CDD

AGRADECIMENTOS

Àqueles que estiveram comigo e que acompanharão a minha caminhada até meu sonho. O esforço sempre vence o talento.

RESUMO

Este trabalho tem por objeto analisar a responsabilidade civil de empresas de tecnologia no que diz respeito ao vazamento de dados dos usuários. O método utilizado foi a análise teórica e crítica de obras, de leis do nosso próprio ordenamento, e de julgados. A Análise do tema se faz relevante em uma sociedade *hiperconectada*, na qual a regulamentação das redes se mostra insuficientes para os problemas atuais. Sendo assim, inicialmente será dissertado sobre a nossa atual sociedade, código de defesa do consumidor, a responsabilidade civil, o dano moral e por fim, um julgado paradigma do Superior Tribunal de Justiça será analisado.

Palavras-Chave: Responsabilidade Civil. Fornecedor. Lei Geral de Proteção de Dados. Indenização Civil.

ABSTRACT

This study seeks to examine the civil liability of tech companies in the context of data breaches. We employed a theoretical and critical analysis of scholarly works, domestic legislation, and case law. This research is particularly timely in our hyperconnected world, where existing regulations often fall short of addressing the challenges posed by modern networks. To this end, we will first explore contemporary society, consumer protection laws, civil liability, and non-pecuniary damages. Finally, we will delve into a landmark decision by the Superior Court of Justice.

Keywords: Civil Liability. Supplier. General Data Protection Law (GDPR). Civil Indemnity.

SUMÁRIO

INTRODUÇÃO	12
1. CONTEXTUALIZAÇÃO NECESSÁRIA	13
2. DOS DADOS	17
2.1 Dados Pessoais	18
2.1.1 Aspecto Analítico do Dado Pessoal Como Direito Da Personalidade	22
2.1.2 Conceituação de Dado Pessoal.....	23
2.2 Dados Sensíveis	25
2.3 Vazamento Ou Publicação Indevida De Dados.....	26
3. RESPONSABILIDADE CIVIL NO ÂMBITO DA LEI GERAL DE PROTEÇÃO DE DADOS.....	30
3.1 Responsabilidade Civil Subjetiva e Objetiva	30
3.2 Responsabilidade Civil No Código de Defesa Do Consumidor	32
3.3 Responsabilidade Civil Na Lei Geral De Proteção De Dados	36
4. DANO MORAL DECORRENTE DE VAZAMENTO DE DADOS.....	38
4.1. A Frequência dos Vazamentos De Dados e a Fragilidade Das Medidas De Segurança	38
4.2 O Dano Moral Decorrente De Vazamento De Dados e o Dano <i>In Re Ipsa</i> .	38
4.2.1 Do Dano Moral	38
4.2.2 Dano Moral Indenizável e o Mero Aborrecimento	39
4.2.3 Dano Moral <i>In Re Ipsa</i>	41
4.2.4 Do Enquadramento No Vazamento De Dados.....	43
4.3 Culpa Exclusiva De Terceiro	44
4.4 A (Des)necessária Comprovação Do Dano Efetivo Na Busca Por Indenização	46
4.4.1 Análise Dos Pressupostos No Precedente Firmado No AREsp nº 2.130.619/SP	47
CONCLUSÃO.....	53

REFERÊNCIAS55

INTRODUÇÃO

A crescente digitalização da sociedade contemporânea, marcada pela intensificação das relações jurídicas estabelecidas no âmbito virtual, impõe novos desafios à ordem jurídica. Dentre esses desafios, destaca-se a necessidade de se estabelecer um arcabouço normativo capaz de tutelar os direitos fundamentais dos indivíduos em face dos riscos inerentes ao tratamento de dados pessoais, em especial no que concerne à sua privacidade.

Nesse contexto, a presente pesquisa tem como objetivo central analisar a responsabilidade civil das empresas de tecnologia, enquanto controladoras de dados, em caso de vazamento de informações pessoais dos usuários, aprofundando a discussão sobre a aplicabilidade da teoria da responsabilidade objetiva nesse peculiar contexto e a adequação da legislação brasileira para a tutela dos direitos individuais lesados.

A relevância do tema reside na necessidade de se conferir efetividade aos direitos fundamentais à privacidade e à proteção de dados, consagrados na Constituição Federal e recentemente positivados na Lei Geral de Proteção de Dados Pessoais (LGPD). A proliferação de incidentes de segurança cibernética e os consequentes vazamentos de dados pessoais têm gerado inúmeros prejuízos aos consumidores, exigindo uma resposta contundente do ordenamento jurídico.

Para tanto, foi realizada uma análise aprofundada da legislação brasileira pertinente, com destaque para o Código de Defesa do Consumidor e a LGPD, bem como da jurisprudência pátria. A pesquisa buscará identificar os elementos caracterizadores da responsabilidade civil objetiva das empresas de tecnologia, os requisitos para a configuração do dano moral decorrente do vazamento de dados e as possíveis defesas invocadas pelas empresas em tais situações.

1. CONTEXTUALIZAÇÃO NECESSÁRIA

A Lei de nº Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD) constituiu-se como resposta legislativa aos inúmeros avanços tecnológicos que, ao mesmo tempo em que impulsionaram o desenvolvimento, trouxeram consigo novos desafios no âmbito da segurança virtual, tanto para empresas quanto para usuários. Com a popularização do mundo digital e da internet, tornou-se imperativo garantir a proteção dos dados pessoais dos usuários e sua privacidade.

Nesse contexto, a doutrina conceitua a privacidade como um direito fundamental, consagrado na Constituição Federal brasileira, que assegura ao indivíduo o direito de viver sua própria vida em isolamento, sem intromissões indevidas, e de impedir que terceiros conheçam, divulguem ou utilizem indevidamente informações a seu respeito. A privacidade, portanto, representa um dos pilares da dignidade da pessoa humana e da autonomia individual.

Contudo, o advento da internet e das mídias sociais tem desafiado a efetividade desse direito fundamental, relativizando-o de forma disfarçada. A coleta, o tratamento e a compartilhamento de dados pessoais em larga escala, sem os devidos controles, expõem os indivíduos a riscos como a violação de sua intimidade, a discriminação e o uso indevido de suas informações.

A Constituição Federal, em consonância com o direito à privacidade, estabelece a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

A LGPD, por sua vez, materializa esses princípios constitucionais ao instituir um marco legal completo para a proteção de dados pessoais no âmbito nacional, impondo a empresas e órgãos públicos a adoção de medidas técnicas e administrativas para garantir a segurança e a privacidade das informações.

Em um mundo cada vez mais digital e interconectado, a LGPD se revela como um instrumento essencial para promover a confiança dos indivíduos no ambiente digital e para fomentar a inovação de forma responsável, assegurando que o desenvolvimento tecnológico ocorra em consonância com os direitos fundamentais.

A LGPD veio complementar o Marco Civil, Lei nº 12.965/2014, que instituiu um arcabouço normativo para as relações digitais no Brasil, estabelecendo regras mais específicas e detalhadas para a coleta, tratamento e armazenamento de dados

peçoais, com o objetivo de garantir a efetiva proteção dos direitos fundamentais dos indivíduos na era digital.

Neste sentido, considerando os princípios e direitos fundamentais presentes na Constituição, além das novas normas trazidas pela LGPD, doutrinadores como Teffé e Viola, aduzem:

Entende-se que o sistema desenvolvido tem como pilares centrais: a) amplo conceito de dado pessoal; b) necessidade de que qualquer tratamento de dados tenha uma base legal; c) rol taxativo de hipóteses legais para o tratamento de dados; d) caracterização detalhada do consentimento do titular e preocupação com sua manifestação; e) legítimo interesse como uma das hipóteses autorizativas e necessidade de realização de um teste de balanceamento de interesses para a sua regular aplicação; f) amplo rol de direitos do titular; e g) densa carga principiológica¹.

Sob esse viés, a LGPD não apenas estabelece diretrizes claras para o tratamento de dados pessoais, mas também visa promover a transparência, a privacidade e a segurança dos dados. De acordo com essa lei, as empresas são obrigadas a adotar medidas de segurança adequadas, a obter consentimento explícito dos usuários para coletar e utilizar seus dados, além de estabelecer políticas claras sobre o armazenamento e o compartilhamento dessas informações.

As obrigações imputadas aos gerenciadores de dados, fornecidos pelas pessoas, visam proteger os direitos de privacidade individuais. Essa responsabilidade, considerada solidária aos agentes envolvidos no tratamento dos dados dos usuários, incentiva as corporações a adotarem meios para assegurar a eficácia do dispositivo normativo. Com isso, algumas medidas de segurança, como a criptografia, a verificação de acesso e a autenticação, tornaram-se comuns nos sites e aplicativos de diversas empresas.

Portanto, em uma breve análise do Marco Civil e da LGPD, vê-se que ambas representam um marco importante em um mundo que deveria garantir que os dados pessoais daqueles que utilizam as redes de computadores fossem tratados com responsabilidade e respeito, de modo a prestigiar as empresas que atuam de forma ética e transparente no ambiente virtual.

¹ TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Tratamento de dados pessoais na LGPD: estudo sobre as bases legais*. *Civilistica.com*, [S. l.], v. 9, n. 1, p. 1-38, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>.

Nesse interim, ao entendermos que empresas fornecedoras de alguma tecnologia possuem o dever de agir de modo socialmente responsável, principalmente frente à proteção de dados pessoais, inicia-se a discussão sobre quando é possível aplicar a elas a responsabilidade civil, tendo em vista a violação da lei, e quais os limites para essa imputação.

Para que haja a responsabilização dessas empresas, com fulcro no instituto da responsabilidade civil no direito brasileiro, é necessária uma análise sobre o tratamento de dados dos usuários, a forma como ela deve ser feita e quais as consequências do não seguimento da lei, que por conseguinte geraria o dever de indenizar.

Nesse sentido, a LGPD estabeleceu uma regulação própria para a responsabilização civil por danos causados decorrente do mau tratamento dos dados nos arts. 42 a 45, que em resumo, determina que todo operador de atividade tecnológica, que faz o tratamento de dados pessoais, será obrigado a reparar qualquer dano material ou moral sofrido, quando decorrente de violação da legislação vigente, exceto se provar que: (1) O tratamento dos dados não era parte de suas atribuições; (2) Não houve violação legal; ou (3) O dano é consequente de culpa exclusiva do titular.

Nada obstante, a lei também considera alvo de responsabilização civil, o tratamento irregular dos dados pessoais, isto é, quando a atividade não está em conformidade com as diretrizes legais, ou quando não providenciar as medidas de segurança previstas de forma adequada:

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

- I. o modo pelo qual é realizado;
- II. o resultado e os riscos que razoavelmente dele se esperam;
- III. as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

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

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Dessa forma, não apenas o tratamento inadequado dos dados, mas também a ausência de requisitos táticos de segurança da informação, podem ser fundamentos para a imputação de responsabilidade civil

Ademais, a regulamentação trazida pela LGPD não esgota a discussão doutrinária sobre o enquadramento dessa responsabilidade, existindo duas outras abordagens principais:

- a) A Responsabilidade Objetiva: Nesse caso, a culpa não é o fator determinante para a responsabilização. Basta que ocorra o dano e que haja um nexo causal entre o ato ilícito (dano sofrido) e o agente responsável.
- b) A Responsabilidade Subjetiva: Aqui, é necessário comprovar a culpa do agente no evento danoso. Além do nexo causal, é preciso demonstrar que o agente agiu com negligência, imprudência ou imperícia.

Independentemente do enquadramento teórico da responsabilidade, é inegável que os dados pessoais devem ser protegidos. A violação da proteção de dados sensíveis e sigilosos representa um patamar ainda mais elevado de incumbência para os agentes responsáveis.

Diante da divergência existente entre lei, doutrina e sua aplicação prática, configura-se um campo fértil para a presente pesquisa monográfica. Objetiva-se analisar a responsabilidade civil das empresas, o dever de indenizar e os motivos pelos quais, em determinadas situações, o dever de indenizar é afastado, mesmo diante do reconhecimento da responsabilidade civil.

2. DOS DADOS

Necessário, nesse momento e antes de especificamente entrar no assunto “dado pessoal”, trazer algumas considerações do que é considerado um dado. Um dado é “*um elemento ou base para a formação de um juízo*”², ou seja, é parte de um todo que permite a identificação de algo. Dessa forma, é possível entender que um dado é qualquer particularidade que indique alguma informação, individualizando-a.

O dado pode ser exposto de várias formas, seja através de suportes fixos, como o papel, ou através de suportes digitais, representados pela menor fração eletrônica, o *bit*. A caracterização desse tipo de informação acerca do dado é importante para os dias atuais, tendo em vista que a migração de sistemas analógicos e meios físicos estão com dias contados. A digitalização é a regra da nova geração, na medida em que os Tribunais^{3 4} e o Poder Executivo⁵ estão editando suas normas para total atuação digital.

Para Valdemar W. Setzer, o dado digital é uma sucessão matemática de símbolos quantificados ou quantificáveis⁶, o que permite deduzir que, assim, podem ser armazenados em um computador e por ele processados.

O dado é uma coisa distinta da informação. O dado, segundo Danilo Doneda, “*apresenta conotação um pouco mais primitiva e fragmentada [...]; uma espécie de pré-informação*”⁷ e a informação, por sua vez, “*alude a algo além da representação contida no dado, chegando ao limiar da cognição [...]*”⁸, ou seja, um dado é qualquer fragmento que, junto com outros dados, pode se tornar uma informação.

² OLINTO, ANTONIO. Minidicionário Antônio Olinto da língua portuguesa. Tradução de Ubiratan Rosa. São Paulo: Moderna, 1919. P. 240.

³ CONSELHO NACIONAL DE JUSTIÇA. Incentivos estimulam digitalização de processos na Justiça alagoana. CNJ, 21 setembro 2016. Disponível em: Acesso em: 16 de outubro de 2024

⁴ CONSELHO NACIONAL DE JUSTIÇA. Norma prevê digitalização de 100% dos processos da Justiça Eleitoral do DF. CNJ, 16 maio 2020. Disponível em: Acesso em: 17 outubro de 2024

⁵ BRASIL. DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015. BRASIL. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8539.htm>. Acesso em: outubro de 2024.

⁶ SETZER, VALDEMAR W. Dado, Informação, Conhecimento e Competência, São Paulo, maio 2015. Disponível em: <https://d1wqtxts1xzle7.cloudfront.net/44270487/ART_2_GEST.pdf?1459453402=&responsecontentdisposition=inline%3B+filename%3DDado_Informacao_Conhecimento_e_Cometenc.pdf&Expires=1594060757&Signature=bExxhJPnU947pfHVGQ8uqh7rqk~KsZJOAraqvSqPorc-A6TPKUYNEI~M4>.

⁷ DONEDA, DANILO. Informação e dados pessoais. In: DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. Cap. 2, p. 152.

⁸ *Idem*.

Portanto, o dado digital pode ser um texto, uma imagem, uma figura, filhos gravados e vídeos, tudo o que pode ser salvo em um banco de dados de um computador e mensurado através de seu processamento digital.

Em meio às normas sobre digitalização de meios e ao grande fluxo de informações que circulam na rede mundial de informática dentro do país, o legislador observa um campo até então sem regulamentação, ou seja, sem uma norma específica para tratar do tema. As informações já não se limitam apenas a dados aleatórios, matemáticos ou instrucionais. Atualmente, os dados circulam com dados pessoais, íntimos ou de proteção, resultando em insegurança tanto para o indivíduo quanto para o Estado, em caso de falha sem respaldo legal.

Foi assim que sobreveio o advento da Lei Geral de Proteção de Dados Pessoais, haja vista que uma Lei com esse escopo não carece de razões para sua aprovação. Conforme já mencionado por Márcio Cots e Ricardo Oliveira:

[...] Com o aumento exponencial de processamento de dados, inteligência artificial e o compartilhamento de informações, estava claro que a privacidade e a intimidade das pessoas estavam morrendo aos poucos, vítima de inúmeros mecanismos do mundo moderno, especialmente redes sociais, bancos de dados públicos, migração da informação que antes estava registrada em papel, agora disponível na internet e outros meios, livre garimpagem e enriquecimento de bancos de dados de todos os tipos, entre outros⁹.

A Lei abrange as informações que abordam o âmbito pessoal do dado, considerando a individualização da informação, ou seja, o dado como uma informação que possibilita a formação de um juízo pessoal do indivíduo. O que foi recolhido por um banco de dados específico e será processado para uso compartilhado, ou não, será, portanto, um dado pessoal.

Assim, é importante destacar a relevância do tema como um campo jurídico que merece maior atenção, considerando a possibilidade de uso econômico e possíveis eventos específicos.

2.1 Dados Pessoais

⁹ COTS, MÁRCIO; OLIVEIRA, RICARDO. Lei Geral de Proteção de Dados Pessoais Comentada. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 25.

A Lei é a origem imediata do Direito no Brasil, destacando sua superioridade em relação às demais fontes. Assim, a primeira análise do que é dado pessoal também deve se pautar pela legislação. A Lei Geral de Proteção de Dados Pessoais, em seu art. 5º, define o que é um dado pessoal.

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Como apresentado, a legislação caracteriza como dado pessoal qualquer informação que possa identificar um indivíduo ou que possa torná-lo conhecido. De acordo com Patrícia Peck Pinheiro, o dado pessoal vai além do nome, apelido, placas de veículos e outras informações diretas, abrangendo tudo o que está ligado à pessoa natural. Por exemplo, um evento ocorrido em sua vida pessoal pode ser capaz de diferenciar alguém de outros.

De acordo com a legislação, o responsável pelo dado é o proprietário do dado pessoal. Portanto, as informações fornecidas pelo proprietário do dado aos agentes econômicos que coletam os dados pessoais, ou às agências governamentais e entidades públicas, representam fragmentos que serão posteriormente comparados e formarão informações que serão interligadas.

Por exemplo, todos os usuários do *Waze* devem divulgar sua posição geográfica, utilizando seu sistema de GPS. Esta é uma exigência para que o aplicativo identifique os pontos congestionados na estrada e, assim, proporcione alternativas aos condutores com menor volume de tráfego. Para aproveitar a conveniência, o usuário consente que terceiros tenham acesso ao seu smartphone, através de um contrato digital.

Quando terceiros têm acesso a dados pessoais, frequentemente sensíveis, a legislação tem como meta salvaguardar os direitos fundamentais de liberdade, privacidade e o desenvolvimento livre da personalidade do indivíduo, além de outros propósitos como a segurança da privacidade, honra, direito de imagem e dignidade. *In verbis*, o artigo 1º da LGPD:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Conforme evidenciado, mesmo a Lei é direcionada a pessoas que coletam e processam dados pessoais, o objetivo final da norma é a proteção. Em outras palavras, o objetivo central da LGPD é proteger o indivíduo e, por isso, antes de se aprofundar no conceito de dados pessoais, é necessário fazer uma avaliação da vulnerabilidade do que está protegido.

Os serviços disponibilizados em aplicativos, sites e programas, anunciados como gratuitos, podem não ser exatamente o que aparentemente foram. Por trás dessa boa intenção, há um interesse econômico. A cobrança da importância que seria paga para utilização desses serviços é transferida para outros meios, como ocorre no oferecimento personalizado dentro do próprio serviço prestado pela rede social ou sítio eletrônico, o que se configura como um subterfúgio estratégico de vendas.

Além disso, também envolve uma alteração no uso da plataforma. Existe, de forma voluntária, a disponibilização de informações pessoais nos bancos de dados dessas companhias, em troca do uso de meios de comunicação ou serviço, ou que, de certa forma, configura um contrato de adesão. Apenas com o fornecimento dos dados pessoais e a utilização subsequente da plataforma, é possível negociar as cláusulas. Se você não optar por fornecer, não poderá utilizar o serviço.

Dessa forma, em posse de diversas informações dos usuários - esses que não são, em grande medida, conhecedores do potencial econômico destes elementos informativos-, as companhias realizam estudos socioeconômicos, psicológicos e perfis consumeristas, cruzando dados compartilhados, inclusive entre outras empresas, com a finalidade de realizar a venda de espaços de publicidade profundamente personalizados para cada um daqueles que desfrutam da rede social ou serviço, supostamente inclusivos e gratuitos.

Com o uso de perfis de consumo e socioeconômicos foram criados verdadeiros impérios que dominam o mercado digital e que são, neste momento, principal forma de divulgação de produtos no mundo, inclusive ditando regras para o *marketplace* ou *marketing digital*. Logo, deu-se início ao que já é intitulado como “o verdadeiro petróleo da era digital”¹⁰, ou seja, os dados pessoais colhidos são tratados como uma mercadoria de grande valor e rentabilidade. Patrícia Peck Pinheiro afirma que “[...] a

¹⁰ SARLET, GABRIELLE BEZERRA SALES; CALDEIRA, CRISTINA. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com*, Rio de Janeiro, p. 7, 2019. Disponível em: <<http://civilistica.com/o-consentimento-informado-e-a-protecao/>>. Acesso em: 19 setembro 2024.

*informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder*¹¹.

Esses dados, que são coletados e processados, podem ser avaliados como cada publicação que recebe "curtidas", e cada comentário publicado é registrado no Facebook. A participação ativa do usuário é o que determina o sucesso da plataforma. Essas interações possibilitam a ferramenta delinear um padrão minucioso sobre o usuário. Sob essa perspectiva, o comportamento na internet pode desvendar suas inclinações políticas, sua orientação sexual e outros gostos.

O Google procede da mesma maneira. A sua conta pessoal documenta os lugares que você visitou, as pesquisas feitas na internet e os vídeos que viram no YouTube. Mesmo fotos e e-mails removidos da caixa de entrada continuam nos servidores, gerando um relatório que equivale a milhões de páginas de texto, incluindo a possibilidade de recuperação desses dados¹².

No entanto, existe um participante, já considerado, nessas relações comerciais que é conhecido como 'titular', os detentores dos dados pessoais recolhidos. Este, que se encontra em uma situação mais delicada nesta relação, devido à necessidade de usar o serviço e às obrigações de aceitar os termos de uso, contratuais e legais.

Não é incomum que o proprietário forneça suas informações para obter um pequeno desconto na aquisição de um produto ou para usar um serviço que é anunciado como 'sem custo'. Com base nessa premissa, considera-se que esse titular é uma parte em desvantagem na relação, evidenciando a necessidade de proteção desigual por parte da ordem jurídica para garantir a equidade do Direito.

Ressalta-se que o indivíduo que fazia o uso da rede de internet, antes da promulgação da LGPD, não estava totalmente descoberto pela legislação nacional, uma vez que havia uma legislação vigente que regulava, e ainda regula, as interações que se realizam por meio do mundo online, ou seja, através da conexão de internet, não sendo o caso dos dados estáticos que são armazenados em bancos de dados.

O Marco Civil da Internet estabelece os direitos e obrigações mútuas à interação daqueles que navegam na internet. No entanto, como mencionado anteriormente, a regulamentação dos dados que tratam das interações entre aqueles que coletam e armazenam informações online e offline era crucial para o progresso sustentável da

¹¹ PINHEIRO, PATRÍCIA PECK. Proteção de dados pessoais - comentários à Lei n. 13.709/2018 (LGPD). 1. ed. São Paulo: Saraiva educação, 2018, p. 50)

¹² Informações disponíveis na aba "Dados e Privacidade" do Google.

sociedade. Em outras palavras, os dados estáticos devem ser protegidos por lei, incluindo os bancos de dados.

2.1.1 Aspecto Analítico do Dado Pessoal Como Direito Da Personalidade

O conceito de direito da personalidade, tal como foi compreendido no século XVII, se distanciou da noção de que os direitos eram decorrentes de uma força divina e passaram a ser interpretados de maneira diferente na ciência jurídica, por meio de um processo de laicidade. Portanto, o ser humano possui direitos inatos e derivados de sua própria natureza, uma visão que se alinha ao jusnaturalismo. Principalmente após a Segunda Guerra Mundial, com a proclamação dos direitos universais pela Organização das Nações Unidas, aumentou ainda mais a preocupação de que o direito garanta os interesses existenciais do indivíduo.

O Código Civil de 2002, com projeto de Orlando Gomes, trouxe os direitos da personalidade, logo no segundo capítulo, em seu art. 11. A medida demonstra nítida preocupação com os direitos da personalidade, realizando uma releitura do Código anterior (1916), com um foco na proteção da pessoa humana, efeito que pode ser denominado “*despatrimonialização*” do direito¹³.

O objetivo indicado no projeto do Código Civil de 2002 estabelece uma cláusula geral de proteção, tutela e promoção da pessoa humana, conforme deduz-se do enunciado 274 da IV Jornada de Direito Civil, cuja principal consequência é a flexibilidade da proteção.

Neste momento, a lista de direitos da personalidade se torna flexível, uma vez que os direitos definidos pelo artigo 11, há um número indeterminado, permitindo a criação de novos direitos de acordo com a mudança da sociedade. Dessa maneira, o direito à proteção de dados pessoais se insere na lista de direitos da personalidade, sobrevivendo uma tutela dinâmica e aberta para promoção da pessoa humana.

A própria Lei Geral de Proteção de Dados Pessoais se encarregou de dispor expressamente acerca do respeito à pessoa humana e seus bens extrapatrimoniais, consoante seu art. 1º, apesar da passível interpretação conforme os direitos individuais da Constituição Federal e dos direitos da personalidade no Código Civil.

¹³ GOMES, ORLANDO. Memória justificativa do anteprojeto de reforma do código civil. Rio de Janeiro: Departamento de Imprensa Nacional, 1963. p. 35.

Um dado classificado como pessoal identifica uma parte ou aparência do seu proprietário. Do ponto de vista analítico, o dado pessoal atua como uma nova categoria de identidade. Para garantir a proteção da identificação projetada, os detentores têm o direito de que a personalidade dessas informações corresponda à realidade. Portanto, a proteção do direito não se restringe apenas ao direito à privacidade, mas abrange um conjunto de direitos que são categorizados como direitos da personalidade.

Com base no que foi apresentado, a definição de proteção de dados pessoais não se limita ao simples desdobramento de um dos direitos da personalidade, mas representa uma inovação na legislação brasileira. Portanto, um direito independente, concebido para cumprir uma função mais complexa do que apenas a privacidade, conforme já indicado.

2.1.2 Conceituação de Dado Pessoal

O conceito de dado pessoal é, muito provavelmente, um dos objetos de maiores disputas e discussões na comunidade acadêmica e de profissionais que se debruçam sobre a proteção de dados pessoais. De partida, o próprio termo sofre variação; não obstante a noção de dado pessoal ser adotada na legislação de diversos países, encontra-se também os termos informação pessoal¹⁴ e informação pessoalmente identificável.

A diferença lexical, no entanto, não se traduz necessariamente numa distinção de significado. Da consulta à literatura especializada, percebe-se que os vocábulos “informação” e “dado”, não raro, se apresentam sobrepostos ou idênticos¹⁵. Vincenzo Zeno-Zencovich, por exemplo, ao expor o que ele designa de natureza poliédrica da informação, destaca que, numa acepção conteudista, “*por informação se entende*

¹⁴ Na legislação pátria encontra-se essa nomenclatura no art. 4º, IV, da Lei n. 12.527/2011. A mesma opção foi feita pela legislação canadense que regula entidades privadas que tratam informações pessoais –Personal Information Protection and Electronic Documents Act (PIPEDA)–ea lei do Estado norte-americano da Califórnia, na recente California Consumer Privacy Act, de 2018.

¹⁵ MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 55

*qualquer dado representativo da realidade que é mantida por um sujeito ou comunicado por um sujeito a outro*¹⁶.

Contudo, essa equivalência tem sido afastada por expressiva parcela dos estudiosos da teoria da informação e suas diversas interfaces. Nesse sentido já se observou que “o dado” apresenta conotação um pouco mais primitiva e fragmentada. Este, para Raymond Wacks¹⁷, a título de exemplificação, consiste numa informação em estado potencial, antes de ser transmitida; o dado estaria associado a uma espécie de “pré-informação”, anterior à interpretação e ao processo de elaboração.

A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar para o seu receptor. Sem aludir ao significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, apontando à redução de um estado de incerteza.

Dito isto, entender o conceito legal de dado pessoal é crucial para a interpretação do escopo normativo de diversas leis de proteção de dados atualmente em vigor globalmente.

Nesse cenário, a LGPD fundamenta sua definição de dado pessoal em seu texto, especialmente no artigo 5º, inciso I. Essa definição de dado pessoal apresenta uma situação crucial na proteção de dados, uma vez que restringe a própria proteção legal em questão. Portanto, ao examinar a redação da Lei, nota-se que ela abrange duas perspectivas, que, conforme Bruno Ricardo Bioni destaca, incluem a esfera expansionista e a esfera reducionista.

Neste contexto, a sistematização acontece devido ao texto do artigo 5º, inciso I, da Lei de proteção, que emprega as palavras “identificada” e “identificável” para se referir à informação recolhida. Se a informação não puder ser identificada, a proteção é ampliada, expansiva. Se a informação for confiável, determinada, a proteção é simplificada.

¹⁶ ZENO-ZENCOVICH, Vincenzo. *Informazione (profili civilistici)*. In: *Digesto –Sezione Civile*. v. IX. Torino: UTET, 1993. p. 3. Tradução livre de: “per informazione si intende qualsiasi dato rappresentativo della realtà che viene conservato da un soggetto oppure comunicato da un soggetto ad un altro”.

¹⁷ WACKS, Raymond. *Personal Information: Privacy and the Law*. Oxford: Oxford University Press, 1989. p. 25. Vide, também, MENDES, Laura Schertel. *Habeas datae autodeterminação informativa: os dois lados da mesma moeda*. *Direitos Fundamentais & Justiça*, v. 12, n. 39, p. 185–216, 2018, p. 200; ALBERS, Marion. *A complexidade da proteção de dados*. *Direitos Fundamentais & Justiça*, v. 10, n. 35, p. 19–45, 2016, p. 30-32.

Para compreender a distinção entre o que é identificável e o identificado, podemos utilizar um exemplo simples: em uma tabela, existem colunas e linhas, conhecidas como atributos. A ligação desses atributos entre si possibilita a identificação precisa de uma pessoa. Na situação sugerida, todos os dados são pessoais, a diferença reside no tipo de dado definido. Como a LGPD indicou explicitamente que dados identificáveis poderiam ser considerados dados pessoais, a teoria escolhida foi a expansionista.

Contudo, é importante ressaltar que a LGPD também propõe outro tipo de informação pessoal, que se choca com a escolha da Lei pela teoria expansionista: o dado anônimo. Este, por sua vez, é aquele que não permitiria a identificação direta do indivíduo.

2.2 Dados Sensíveis

Para fins de regulação das atividades de tratamento de dados, a Lei Geral de Proteção de Dados Brasileira, categoriza e tutela de forma diferenciada os dados pessoais e os dados pessoais sensíveis.

Enquanto dados pessoais são compostos por informações relacionadas a pessoa natural identificada ou identificável (artigo 5º, I), dados pessoais sensíveis refere-se à *“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”* (art. 5º, II).

Por essa razão, a regulamentação da coleta, utilização, processamento e compartilhamento de dados pela Lei Geral de Proteção de Dados é crucial. Essas atividades devem ser conduzidas de maneira a cumprir os princípios definidos na lei referida. Em particular, no caso de dados sensíveis, deve-se priorizar o uso que honre o princípio da igualdade e evite qualquer discriminação, em conformidade, inclusive, com os princípios norteadores da LGPD.

Por exemplo, observe-se um conjunto mais limitado de situações que autorizam o tratamento de dados sensíveis, conforme previsto no artigo 11 da LGPD. É crucial que o consentimento, além de livre, seja esclarecido, específico e direcionado a um propósito semelhante, seja destacado, ou, como é comumente dito, avaliado de maneira "granular".

A estratégia empregada para estabelecer e restringir as hipóteses que possibilitariam o tratamento requer uma comunicação antecipada aos interessados sobre o uso que será feito das informações obtidas. Para algumas categorias de dados particularmente sensíveis, estabelece-se que o único propósito permitido é o interesse do indivíduo em questão.

É importante ressaltar que, conforme o parágrafo 1 do artigo 11 da mesma Lei, se qualquer tratamento feito com dados pessoais não sensível puder revelar dados sensíveis e potencialmente causar danos ao titular, o regime jurídico específico será aplicado, a menos que outra norma estabeleça de forma diferente.

A tutela jurídica de dados pessoais como um corolário do direito à privacidade (ou do direito à identidade) nos leva a considerar que a autodeterminação informativa, ou o poder de controle sobre os próprios dados, deve ser a tônica quando buscamos a proteção específica dos dados sensíveis, especialmente se tais dados podem gerar tratamentos desiguais.

Ademais, no que diz respeito ao aspecto constitucional, desde a promulgação da Emenda Constitucional 115, em 10 de fevereiro de 2022, a proteção de dados pessoais é um direito essencial na Constituição Federal do Brasil. O inciso LXXIX do artigo 5º da Constituição garante o direito à segurança dos dados pessoais, inclusive em ambientes digitais.

A segurança de dados pessoais, resultante da cláusula geral de proteção à pessoa humana e ao direito à privacidade, é uma exigência fundamental para a democracia. O processamento de dados pessoais de várias naturezas tem crescido exponencialmente, principalmente com o surgimento de tecnologias avançadas de inteligência artificial, que empregam algoritmos complexos e possibilitam o aprendizado de máquinas (*machine learning*).

2.3 Vazamento Ou Publicação Indevida De Dados

Tanto a LGPD quanto o Marco Civil da Internet visam proteger a pessoa natural, a parte mais frágil da relação. Portanto, estabelecem princípios e garantias para proteger o consentimento legítimo do usuário ao contratar qualquer empresa ou compartilhar seus dados com quem quer que seja.

A diferença entre as Leis é que o Marco Civil da Internet tem uma abordagem mais geral nas relações e voltado para o prisma da conectividade, e a Lei Geral de

Proteção de Dados se aplica nos casos em que “o objetivo seja a oferta ou o fornecimento de bens ou serviços”¹⁸, ou seja, com fins econômicos.

Nesta perspectiva, as leis mencionadas estabelecem um ambiente regulatório para os agentes referenciais. No entanto, é importante ressaltar que, embora as leis se concentrem nas relações entre o coletor de dados e os proprietários desses, outros participantes na relação podem usar os dados, registros e toda a estrutura de mapeamento elaborada pelos especialistas no tratamento de dados para alcançar seus objetivos. O Poder Judiciário é uma das situações que a LGPD e o Marco Civil da Internet permitem.

O Brasil já conta com número razoável de julgados em que o Poder Judiciário, dentro do âmbito processual, requisita informações de dados pessoais para resolução de demandas cíveis e criminais. Isto é, o modelo probatório do processo judicial brasileiro está mudando, assim como as relações da sociedade. Uma decisão judicial penal pode ser fundamentada em indícios coletados diretamente do ambiente virtual.

A aplicação desses dados, já amplamente utilizada nos tribunais brasileiros, fornece uma nova visão na obtenção de informações para a instrução probatória do processo. A capacidade de solicitar perfis de consumo, análise socioeconômica, perfis de atividade ou estudos personalizados de cada banco de dados pode representar uma oportunidade para a mudança do método probatório.

Portanto, é indiscutível o constante fluxo de informações que ocorre todos os dias entre entidades governamentais, entidades sob controle do Estado e empresas privadas. Portanto, existe um grande interesse nos dados pessoais dos indivíduos bloqueados por entidades públicas e privadas que não podem ser acessados sem que ocorra um vazamento desses dados, seja ele acidental ou não.

A Constituição da República Federativa do Brasil de 1988 também faz referência à proteção de dados pessoais em seu artigo 5º, inciso XII, garantindo, em essência, a inviolabilidade do sigilo de correspondência, comunicações telegráficas, de dados e comunicações telefônicas, com uma única exceção. Em situações em que uma ordem judicial, conforme a legislação, autoriza a quebra do sigilo para condução de investigações criminais ou processos criminais.

A Lei Geral de Proteção de Dados Pessoais prevê em seu artigo 7º, inciso VI, e no artigo 11, inciso II, alínea ‘d’, a possibilidade de utilização de dados pessoais em

¹⁸ PINHEIRO, PATRÍCIA PECK. Proteção de dados pessoais - comentários à Lei n. 13.709/2018 (LGPD). 1. ed. São Paulo: Saraiva educação, 2018, p. 57.

diversos momentos. Em um destes é a utilização de dados para o regular exercício de direitos em processos judiciais:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) 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);

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...) II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: (...) d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem).

Além disso, o Marco Civil da Internet traz um dispositivo que permite também a quebra do sigilo de dados com fundamento de utilização dos dados em conjunto probatório em processos cíveis e penais, com autorização judicial, cabendo ao juízo manter o sigilo dos dados¹⁹.

Em tais situações, a permissão legal para o uso de dados é concedida de forma distinta solicitada ao indivíduo no formulário de "aceito os termos" das entidades que coletam dados pessoais. Podemos mencionar uma relação não contratual com o Estado. No entanto, caso ocorra uma falha na proteção desses dados ou uma invasão forçada dos sistemas, a lei deve proteger o indivíduo e seu direito.

Por esse motivo, a Lei Geral de Proteção de Dados Pessoais afirma em seus artigos 46 e 48, além do 52, §7º, condutas que servirão de base para a atuação do tratamento de dados, uma espécie de lista de procedimentos a serem seguidos para assegurar a segurança do titular²⁰.

¹⁹ Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

²⁰ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

É importante destacar que a legislação estabelece que uma entidade nacional será encarregada de supervisionar os controladores dos dados pessoais recolhidos para fins econômicos. Nestas situações de vazamento ou divulgação não autorizada, a autoridade encarregada de agir para corrigir e responsabilizar as reclamações ao sistema de segurança e a violação de direitos pessoais.

No entanto, a lei indica que o gestor de dados pessoais será penalizado, seja no âmbito administrativo ou na esfera subjetiva possível do Judiciário, sem especificar claramente a teoria utilizada - se objetiva ou subjetiva - para solucionar situações tanto para indivíduos quanto para dados que estão incluídos sob a posse do Estado.

Por todas essas razões, parece haver uma vulnerabilidade aparente dos direitos de personalidade em relação ao tratamento de dados pessoais pelo Estado e a eventual vazamento e/ou divulgação não autorizada de informações pessoais. A LGPD obriga os indivíduos de direito privado e público a serem penalizados pela autoridade de controle de dados, exigida pela própria legislação, mas não garante ao titular a proteção de seu direito subjetivo.

Nesse contexto, nos capítulos subsequentes, convidamos discutir a responsabilidade civil do Estado em situações de risco social envolvendo dados pessoais em seu poder.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional.

§7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.

3. RESPONSABILIDADE CIVIL NO ÂMBITO DA LEI GERAL DE PROTEÇÃO DE DADOS

3.1 Responsabilidade Civil Subjetiva e Objetiva

A responsabilidade civil visa restaurar o equilíbrio moral ou patrimonial rovocado pelo autor de um dano, em razão de um prejuízo acarretado à vítima do dano. Desta forma, possui a finalidade de restaurar o equilíbrio e a harmonia por meio da reparação do dano.²¹

A responsabilidade civil pode ser objetiva ou subjetiva, a depender da necessidade de comprovação de culpa do autor do dano. Flávio Tartuce explica que a regra geral do Direito Civil brasileiro é a da teoria da culpa, “*segundo a qual haverá obrigação de indenizar somente se houver culpa genérica do agente*”²², cabendo ao autor da demanda comprovar a existência da culpa, conforme o art. 373, I, do Código de Processo Civil.

Trata-se da chamada responsabilidade subjetiva, segundo a qual o elemento da culpa é um pressuposto da responsabilidade civil, sendo que, não havendo culpa, não há que se falar em responsabilidade.

A responsabilidade subjetiva está prevista no art. 927 do Código Civil, o qual dispõe que aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo. Ato ilícito, por sua vez, é definido no art. 186 do Código Civil como “*aquele que, por ação ou omissão voluntária, negligência ou imperícia, violar direito e causar dano a outrem, ainda que exclusivamente moral*”.

O parágrafo único do artigo 927 do Código Civil também estabelece que a obrigação de reparar o dano, independentemente da existência de culpa, se aplicará nas situações previstas em lei ou quando a ação do causador do dano, por sua própria natureza, representar um perigo para os direitos alheios. Portanto, deduz-se que a norma geral definida no Código Civil é a teoria da culpa, com a responsabilidade objetiva sendo aplicável de forma excepcional, apenas nos casos explicitamente previstos na legislação.

²¹ GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro: Responsabilidade Civil*. vol..4. 15 ed. São Paulo: Saraiva Educação, 2020, p. 20.

²² TARTUCE, Flávio. *Responsabilidade Civil*. 3 ed. Rio de Janeiro: Forense, 2021, p. 259.

Além disso, é importante destacar que a responsabilidade subjetiva tem como objetivo responsabilizar quem sofreu um dano através de uma ação culposa, que pode ser voluntária ou involuntária. Ela deve ser compreendida em sua totalidade, incluindo tanto o dolo quanto a culpa em sentido lato.

Neste sentido, Segundo Arnaldo Rizzardo, não há responsabilidade quando o agente agiu com a devida cautela ou não podia prever o dano, sendo a culpa um pressuposto da responsabilidade subjetiva:

Pela teoria da responsabilidade subjetiva, só é imputável, a título de culpa, aquele que praticou o fato culposos possível de ser evitado. Não há responsabilidade quando o agente não pretendeu e nem podia prever, tendo agido com a necessária cautela. Não se pode, de maneira alguma, ir além do ato ilícito para firmar a responsabilidade subjetiva, contrariamente ao que alguns pretendem, com superficialidade, a ponto de ver em tudo o que acontece a obrigação de indenizar, sustentando que, verificado o dano, nasce tal obrigação, sem indagar da culpa do lesado, e impondo, como único pressuposto, o nexo causal entre o fato e o dano²³.

Desta forma, a totalidade de elementos que fundam a responsabilidade subjetiva são: i) a ação ou omissão do agente; (ii) que a ação ou omissão do agente seja culposa; (iii) o nexo causal entre a conduta do agente e o dano; e (iv) o dano²⁴. A culpa em sentido amplo é, portanto, um dos elementos essenciais para a incidência da responsabilidade subjetiva, podendo ser expressada por meio de uma conduta voluntária ou involuntária.

A responsabilidade objetiva, por outro lado, é aquela que se baseia na teoria do risco, levando-se em conta o perigo da atividade do autor do dano por sua natureza ou pela natureza dos meios empregados²⁵. Neste sentido, segundo a teoria do risco, aqueles que exercem uma atividade que possui o risco de causar dano a outrem, respondem de forma objetiva pelos danos causados, pois assumiram o risco de gerar danos em razão da atividade exercida.

Em relação ao risco, que pode ser definido como o risco ou a possibilidade de dano, entende-se que, caso a atividade realizada por um agente cause um risco a terceiros, este deverá reparar o prejuízo causado pela sua ação. Como será detalhado

²³ RIZZARDO, Arnaldo. *Responsabilidade Civil*. 8 ed. Rio de Janeiro: Forense, 2019, p. 26.

²⁴ *Ibidem.*, p. 33-34.

²⁵ VENOSA, Silvio de Salvo. *Direito Civil: Obrigações e Responsabilidade Civil*. vol. 2, 21 ed. São Paulo: Atlas, 2021, p. 366.

posteriormente, trata-se do risco que é gerado ao consumidor, o elemento mais suscetível na relação de consumo.

Em relação ao tratamento de dados pessoais, pode -se afirmar que o proprietário dos dados pessoais, cujos dados estão sob a responsabilidade do responsável pelo tratamento, é o mais frágil da relação jurídica. Nesse sentido, a própria Lei Geral de Proteção de Dados, em seu artigo 42, § 2º, admite que, em situações de hipossuficiência do titular, o magistrado pode inverter a obrigação de provar. Portanto, o profissional de tratamento de dados, ao realizar tal tarefa, assume o risco de causar danos a esses dados pessoais que estão sendo processados.

Como já mencionado, o parágrafo único do artigo 927 do Código Civil estabelece as disposições em que a responsabilidade objetiva é aplicável, sejam elas nas situações previstas na lei ou quando a atividade for realizada. Em relação ao tratamento de dados, pode-se afirmar que a atividade envolve um risco, possibilitando a aplicação do disposto no art. 927, parágrafo único, do Código Civil.

Os pressupostos da responsabilidade objetiva são os mesmos da responsabilidade subjetiva, com exceção da culpa. Neste sentido, explica Caio Mario da Silva Pereira²⁶ que a responsabilidade objetiva resulta do dano e da autoria do evento danoso:

A doutrina objetiva, ao invés de exigir que a responsabilidade civil seja a resultante dos elementos tradicionais (culpa, dano, vínculo de causalidade entre uma e outro) assenta na equação binária cujos polos são o dano e a autoria do evento danoso. Sem cogitar da imputabilidade ou investigar a antijuridicidade do fato danoso, o que importa para assegurar o ressarcimento é a verificação se ocorreu o evento e se dele emanou o prejuízo. Em tal ocorrendo, o autor do fato causador do dano é o responsável.

Portanto, de acordo com a teoria do risco, a mera presença do dano, a relação causal e a autoria são suficientes para responsabilizar o agente. Adicionalmente, de acordo com o artigo 927 e seu parágrafo único do Código Civil, a responsabilidade civil é aplicável em duas situações: quando exigida por lei ou quando o indivíduo realiza uma atividade que possa colocar em risco o direito alheio. Assim, a responsabilidade objetiva é fundamentada no risco e no prejuízo.

5.2 Responsabilidade Civil No Código de Defesa Do Consumidor

²⁶ PEREIRA, Caio Mario da Silva. *Responsabilidade Civil*. 12 ed. Rio de Janeiro: Forense, 2018, p. 346.

O Código de Defesa do Consumidor estabelece regras de segurança e defesa do consumidor, entendido como a pessoa física ou jurídica que adquire um produto ou serviço como destinatário final, conforme previsto no artigo 2º do código. O fornecedor, que é definido no artigo 3º da lei como uma pessoa física ou jurídica que realiza atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou venda de produtos ou serviços, ocupa a outra extremidade da relação jurídica.

A proteção do consumidor está fundada na sua vulnerabilidade perante o mercado de consumo, o que é reconhecido pela Política Nacional das Relações de Consumo, nos termos do art. 4º, I, do Código de Defesa do Consumidor. Referida política tem a finalidade de atender as necessidades e interesses dos consumidores. Segundo Silvio Venosa²⁷, o Código de Defesa do Consumidor municiou o consumidor frente à supremacia econômica do fornecedor:

O Código de Defesa do Consumidor procurou municiar o consumidor, vulnerável na relação de consumo, com instrumentos eficazes, outorgando-lhe superioridade jurídica em relação ao fornecedor que, em tese, possui supremacia econômica.

A previsão da responsabilidade objetiva, uma das ferramentas previstas no Código de Defesa do Consumidor, tem como objetivo proteger o consumidor diante da superioridade técnica e econômica do fornecedor. O artigo 12 do Código de Defesa do Consumidor estabelece que os fabricantes, produtores, construtores e importadores são responsáveis, sem considerar a culpa, pelos prejuízos dos prejuízos causados aos consumidores devido a falhas em seus produtos.

Da mesma forma, o art. 14 do código prevê que o fornecedor de serviços responde pela reparação dos danos causados aos consumidores por defeito na prestação de serviços, independentemente da culpa. O parágrafo único do mencionado artigo, a seu turno, define que o serviço defeituoso é aquele que não fornece a segurança que o consumidor dele pode esperar.

Trata-se da responsabilidade pelo fato do serviço, o que ocorre quando há um defeito na prestação de serviços que pode comprometer a segurança do consumidor. Assim, o Código de Defesa do Consumidor previu a responsabilidade objetiva para os fornecedores de produtos e serviços no âmbito das relações de consumo.

²⁷ VENOSA, Silvio de Salvo. op. cit., p. 556.

É importante ressaltar que o Código de Defesa do Consumidor também estabelece a responsabilidade decorrente de defeito no produto ou serviço, conforme previsto nos artigos 18 e 20, respectivamente. A diferença fundamental entre o fato do serviço e o vínculo do serviço é que o primeiro está ligado à proteção do cliente, causando danos que ultrapassam os limites do serviço fornecido, enquanto o segundo está ligado a um dano intrínseco ao serviço.

Naturalmente, a responsabilidade objetiva prevista no Código de Defesa do Consumidor está diretamente relacionada à teoria do risco, pois presume-se que a atividade exercida pelos fornecedores possui um risco inerente de causar dano aos consumidores, que são vulneráveis e hipossuficiências dentro da relação de consumo.

Tão relevante é a proteção do consumidor e a reparação de danos no âmbito das relações de consumo, que um dos direitos básicos do consumidor é a prevenção e reparação de danos materiais, morais, individuais, coletivos e difusos ocasionados em relações de consumo, conforme inciso VI do art. 6º do código.

Sendo assim, em seu art. 81, o Código de Defesa do Consumidor define que “*a defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo*”. Ainda, o parágrafo único do referido artigo dispõe sobre as hipóteses em que a defesa coletiva dos direitos de consumidores poderá ser exercida, o que poderá ocorrer quando (i) tratar-se de interesses ou direitos difusos de indivíduos indeterminados ligados por uma circunstância de fato; (ii) interesses ou direitos coletivos de que seja titular um grupo, categoria ou classe de pessoas ligadas entre si ou com a parte contrária; e (iii) tratar-se de interesses ou direitos individuais homogêneos decorrentes de uma origem comum.

Em relação ao vazamento de informações pessoais no âmbito do direito do consumidor, é possível afirmar que o vazamento de informações representa uma falha no serviço fornecido, resultando na responsabilidade objetiva pelo fato do serviço, conforme previsto no artigo 14 do Código de Defesa do Consumidor. Isso acontece porque uma falha no serviço coloca em risco a segurança do proprietário dos dados, que pode ter seus dados usados de forma ilícita ou ilegal. Além disso, as repercussões do vazamento de informações pessoais protegem os serviços prestados, pois podem levar a danos materiais ou morais ao titular.

Ainda, afirma Gabriel Araújo²⁸ que, ocorrendo um vazamento de dados pessoais e não tendo sido tomadas as medidas previstas na Lei Geral de Proteção de Dados, sendo comprovado o dano gerado em violação ao direito do consumidor, aplica-se a responsabilidade objetiva ao agente de tratamento de dados, nos termos previstos no Código de Defesa do Consumidor.

Tal afirmativa tem fundamento no art. 45 da Lei Geral de Proteção de Dados, que prevê que os casos de violação do direito do titular nas relações de consumo são sujeitas às regras de responsabilidade previstas na legislação pertinente, ou seja, no Código de Defesa do Consumidor.

Sendo assim, a regulamentação da responsabilidade civil na lei de proteção de dados pessoais não impede a aplicação da responsabilidade exigida no Código de Defesa do Consumidor, caso se configure uma relação de consumo. Como já mencionado, o artigo 45 da Lei Geral de Proteção de Dados estabelece que, em situações de violação do direito do titular durante uma relação de consumo, as normas de responsabilidade condicionais no Código de Defesa do Consumidor permanecem aplicáveis.

Neste mesmo sentido, Walter Aranha Capanema, ao comentar sobre a responsabilidade civil na Lei Geral de Proteção de Dados, ressalta que as normas da Lei Geral de Proteção de Dados não são aplicáveis em todos os casos envolvendo responsabilidade civil, pois haverá espaço para normas específicas como o Código de Defesa do Consumidor, a depender da relação jurídica²⁹.

Portanto, de acordo com o Código de Defesa do Consumidor, o fornecedor tem uma responsabilidade objetiva pelos prejuízos causados aos consumidores. Se houver dano e uma relação causal, o fornecedor será obrigado a reparar o prejuízo, independentemente da existência de culpa. Isso ocorre porque, ao introduzir produtos e serviços no mercado de consumo, o fornecedor assume a possibilidade de causar prejuízos aos seus clientes, que são frágeis na relação jurídica.

Em relação aos dados pessoais, quando se estabelece uma relação de consumo, pode-se aplicar a responsabilidade civil objetiva, fundamentada no Código de Defesa do Consumidor, por infração à privacidade do consumidor.

²⁸ SOUTO, Gabriel Araújo. Vazamento de dados no setor privado brasileiro: a gestão do risco como parâmetro para a responsabilidade empresarial. *Revista de Direito e as Novas Tecnologias*, vol. 7/2020, Abr-Jun/2020, DTR\2020\7817.

²⁹ CAPANEMA, Walter Aranha. A Responsabilidade Civil na Lei Geral de Proteção de Dados. *Cadernos Jurídicos*, São Paulo, ano 21, n° 53, p. 163-170, Jan-Mar/2020.

3.3 Responsabilidade Civil Na Lei Geral De Proteção De Dados

O artigo 42 da Lei Geral de Proteção de Dados estabelece a responsabilidade e o pagamento de danos causados pelo controlador ou operador que, ao tratar dados pessoais, cause prejuízo a terceiros, seja moral, financeiro, individual ou coletivo, infringindo a lei.

Ademais, o parágrafo único do artigo 44 da lei estabelece a responsabilidade do controlador ou do operador pelos prejuízos resultantes da violação da segurança dos dados, caso cause o dano ao não implementar as medidas de segurança condicionais na legislação. Portanto, a responsabilidade civil surge quando há infração à legislação ou violação das normas técnicas relacionadas à proteção de dados.

Como mencionado anteriormente, o controlador é o indivíduo ou entidade responsável pelas decisões relacionadas ao tratamento de dados pessoais, sendo aquele que recebe as informações pessoais do titular e obtém sua assinatura. Por outro lado, o operador atua como o responsável pelo processamento de dados pessoais em nome do controlador.

Considerando que são esses os agentes de tratamento de dados pessoais, a Lei Geral de Proteção de Dados estabeleceu que o operador responde solidariamente pelos danos causados quando descumprir a legislação ou quando não tiver seguido as instruções do controlador, equiparando-se a ele. Além disso, o controlador responde solidariamente quando estiver diretamente envolvido no tratamento de dados do qual decorreu danos ao titular.

A Lei Geral de Proteção de Dados também define, em seu artigo 43, as indicações nas quais os responsáveis pelo tratamento de dados não serão responsabilizados pelos prejuízos causados. Estes são os casos em que os agentes indicados comprovaram que (i) não executaram o tratamento de dados que os chefes foram designados; (ii) mesmo tendo realizado o tratamento de dados, não infringiram a lei; ou (iii) o dano resultar exclusivamente da culpa do titular ou de terceiros.

Portanto, a interpretação do artigo 43 sugere que os agentes respondam de forma objetiva, deixando de responder apenas em situações específicas.

Além disso, de forma similar ao Código de Defesa do Consumidor, a Lei Geral de Proteção de Dados admite a inversão do ônus da prova no processo civil quando o titular dos dados pessoais for hipossuficiente para fins de produção de prova, a sua alegação for verossímil ou quando a produção de prova pelo titular for excessivamente

onerosa, conforme o § 2º do art. 42 da Lei Geral de Proteção de Dados.

Conforme estudado no tópico anterior, não há dúvidas de que, havendo o reconhecimento de uma relação de consumo, aplica-se a responsabilidade objetiva, nos termos do Código de Defesa do Consumidor. Contudo, é possível verificar que a responsabilidade civil prevista na Lei Geral de Proteção de Dados assemelha-se àquela da legislação consumerista.

Embora a matéria não seja pacificada na jurisprudência, entende-se por ora que a responsabilidade civil prevista na Lei Geral de Proteção de Dados é da modalidade objetiva, seja porque o titular dos dados pessoais ocupa posição de vulnerabilidade e hipossuficiência perante o agente de tratamento de dados, seja porque a atividade de tratamento de dados possui um risco inerente que é assumido pela empresa, enquadrando-se no parágrafo único do art. 927 do Código Civil.

Ainda, entende-se que vazamento de dados pessoais poderia configurar um dano moral *in re ipsa*, uma vez que a divulgação de dados pessoais envolve a violação de direitos da personalidade e da proteção de dados pessoais, que assumiu *status* de direito fundamental.

Há, ainda, notável semelhança nos dispositivos da Lei Geral de Proteção de Dados e do Código de Defesa do Consumidor, na medida em que a Lei Geral de Proteção de Dados reconhece a vulnerabilidade dos titulares de dados pessoais em relação aos agentes de tratamento de dados, prevê a possibilidade de inversão do ônus da prova, a solidariedade entre o controlador e o operador, e prevê as hipóteses de exclusão de responsabilidade possibilidade de inverteção do ônus da prova.

4. DANO MORAL DECORRENTE DE VAZAMENTO DE DADOS

4.1. A Frequência dos Vazamentos De Dados e a Fragilidade Das Medidas De Segurança

O incidente de segurança que envolve dados pessoais é um fato inegável à sociedade da informação, podendo ser visto como um risco inescapável e causado à prática de tratamento de dados.

É importante lembrar que, mesmo com a definição de normas de segurança para a proteção de dados pessoais, não podemos descartar a possibilidade de que ações mal-intencionadas de terceiros possam violar os sistemas de segurança, resultando no vazamento indevido de informações dos proprietários.

As medidas de segurança são inovadoras de maneira reativa para interromper um ataque e fechar brechas para evitar sua reprodução. Apesar do esforço em antecipar um ataque futuro para dificultar a ação dos cibercriminosos, esses testes são incessantes e desconhecidos até o momento em que acontecem.

Ademais, assim que uma forma de ataque é solucionada, os *cibercriminosos* já colocaram em prática um novo *modus operandi*, restando clara a fragilidade das medidas de segurança.

4.2 O Dano Moral Decorrente De Vazamento De Dados e o Dano *In Re Ipsa*

4.2.1 Do Dano Moral

Inicialmente, é crucial enfatizar que o dano moral é um tipo de dano do tipo extrapatrimonial, já que segundo ensinam Pablo Stolze Gagliano e Rodolfo Pamplona Filho³⁰:

[...] o dano moral consiste na lesão de direitos cujo conteúdo não é pecuniário, nem comercialmente redutível a dinheiro. Em outras palavras, podemos afirmar que o dano moral é aquele que lesiona a esfera personalíssima da pessoa (seus direitos da personalidade).

Alguns autores consideram o dano moral como residual, isto é, algo que não se enquadra em outras categorias, como o dano estético, existencial ou à imagem. No entanto, quando se trata de um dano extrapatrimonial, seria classificado como dano

³⁰ GAGLIANO, Pablo Stolze e FILHO, Rodolfo Pamplona Filho. Novo curso de direito civil: responsabilidade civil, vol. III, 9ª ed., São Paulo: Saraiva, 2011, p. 97.

moral.

Na realidade, esta escritora acredita que o dano moral pode abranger todas as formas de danos extrapatrimoniais, incluindo as mencionadas acima, entre outras. Contudo, a principal diferença entre as subespécies é a determinação do valor da compensação para cada categoria de dano moral.

4.2.2 Dano Moral Indenizável e o Mero Aborrecimento

O dano moral é um prejuízo que impacta a psique da vítima, manifestando-se através de desgosto e angústia. Pode ser entendido não somente como uma infração aos direitos da personalidade, mas também como uma lesão a um interesse existencial real que merece proteção jurídica.

Nesse sentido é o Enunciado 444 do Conselho da Justiça Federal, emitido na V Jornada de Direito Civil: "*o dano moral indenizável não pressupõe necessariamente a verificação de sentimentos humanos desagradáveis como dor ou sofrimento*".

Portanto, não que diz respeito ao dano moral, o objetivo é salvaguardar características que ultrapassam o aspecto financeiro, prevenindo a coisificação do indivíduo através da proteção de sua integridade física, mental, moral e intelectual. Além de investigar a presença desses efeitos, é necessário determinar se os eventos envolvidos infringem os interesses existenciais da vítima, evidenciados nas lesões sofridas e suas consequências, que resultaram em distúrbios que ultrapassaram a normalidade.

Logo, o que define o dano moral como indenizável são os efeitos ou desdobramentos da lesão, e não o próprio dano. Há situações em que, mesmo existindo o dano moral, ele não será indenizado, como ocorre nos casos de exclusões de responsabilidade civil.

O prejuízo moral reparável surge da violação dos direitos da personalidade da vítima, incluindo sua integridade mental, intelectual, moral e física. Portanto, é necessário mais fazer que apenas constrangimento ou frustração, sendo necessária a identificação de um desconforto extremamente significativo que possa violar a dignidade humana.

Por outro lado, o denominado "mero incômodo" é aquele que não infringe direitos de personalidade ou existenciais do indivíduo afetado. O prejuízo pode até ter ocorrido, porém não é reembolsável, pois não afetou a integridade física, mental,

moral e intelectual da vítima.

Além disso, o simples descontentamento diz respeito a situação é desafiador e irritante que são comuns no dia a dia, mas que não provocam prejuízos consideráveis à esfera emocional, psicológica ou à negociação de um indivíduo. Normalmente, esses imprevistos não geram direito a compensação financeira.

Alguns exemplos de situações que geralmente se enquadram como mero aborrecimento incluem: meros atrasos em voos, transportes públicos ou atendimento em estabelecimentos comerciais, desde que não resultem em perdas substanciais; erros triviais ou pequenos em serviços, como uma pizza entregue com um ingrediente errado, mero descumprimento contratual, desde que não causem prejuízos significativos; ou, inconveniências comuns como barulhos de vizinhos, pequenos congestionamentos de trânsito e outros aborrecimentos normais da vida em sociedade.

A distinção entre dano moral reparável e simples incômodo é fundamental para o funcionamento justo e eficiente do sistema de justiça. Embora o dano moral envolva a violação de direitos pessoais e a exija a comprovação da lesão, relação causal e culpa ou dolo, o simples incômodo se refere à supervisão competitiva, porém comum, que não justificam a compensação por meio de compensação financeira.

Segundo ensina o Douo Sérgio Carvalhier Filho³¹ ao tratar do dano moral:

Se dano moral é agressão a dignidade humana, não basta para configurá-lo qualquer contrariedade. (...) Nessa linha de princípio, só deve ser reputado como dano moral a dor, vexame, sofrimento ou humilhação que, fugindo à normalidade, interfira intensamente no comportamento psicológico do indivíduo, causando-lhe aflições, angústia e desequilíbrio em seu bem-estar. Mero dissabor, aborrecimento, mágoa, irritação ou sensibilidade exacerbada estão fora da órbita do dano moral, porquanto além de fazerem parte da normalidade do nosso dia-a-dia, no trabalho, no trânsito, entre amigos e até no ambiente familiar, tais situações não são intensas e duradouras, a ponto de romper o equilíbrio psicológico do indivíduo.

Portanto, para que um dano moral seja caracterizado como indenizável, além da comprovação da dor, é necessário evidenciar os requisitos da responsabilidade civil.

É crucial que os participantes e o sistema jurídico compreendam a diferença entre esses conceitos para prevenir o excesso de processos judiciais e garantir que a

³¹ Farias, Cristiano Chaves de; Rosenvald, Nelson; Netto, Felipe Peixoto Braga. Curso de direito civil: responsabilidade civil, 4ª ed. rev. e atual., Salvador: JusPodivm, 2017, p. 297.

responsabilidade civil seja resolvida de maneira equitativa e proporcional. Isso contribui para a proteção dos direitos básicos dos indivíduos e mantém um equilíbrio entre a liberdade de ação e a defesa contra abusos na convivência social. Além de prevenir a banalização do pedido de indenização por dano moral.

O Superior Tribunal de Justiça (STJ), ao se manifestar sobre a caracterização do dano moral indenizável no AgInt nos EDcl no AREsp 1.713.267/SP, cujo relator foi o Ministro Raul Araújo, firmou entendimento de que:

Para que fique configurado o dever de indenização por danos morais, é necessário que o ato ilícito tenha violado direito de personalidade, provocando dor, sofrimento, abalo psicológico ou humilhação consideráveis à pessoa. Precedentes (Quarta Turma, julgado em 24/10/22, DJe de 28/10/22).

O próprio CSTJ ao negar conhecimento ao AREsp 2.408.593, do qual foi relator o Ministro Moura Ribeiro, manteve o entendimento do Tribunal Estadual sobre a caracterização de mero aborrecimento, nos seguintes termos:

[...] Soberano na apreciação das provas dos autos, o Tribunal de origem concluiu que o atraso na entrega do produto adquirido pela autora não ultrapassou a esfera do mero aborrecimento e, portanto, não ocasionou danos morais reparáveis (DJe de 19/9/23).

4.2.3 Dano Moral *In Re Ipsa*

A expressão jurídica "*dano moral in re ipsa*" refere-se a um tipo de dano moral que é presumido ou evidente com base nas situações do caso, dispensando a apresentação de evidências adicionais das consequências dos prejuízos sofridos. Esta frase é comumente empregada em situações em que a gravidade do evento ou da ação ilícita é tão evidente que a ofensa à dignidade ou à integridade mental da vítima é clara e inquestionável.

Em resumo, quando se reivindica um dano moral *in re ipsa*, a mera ocorrência do evento ou do comportamento já é vista como evidência suficiente de que a vítima foi prejudicada em sua dignidade, confiança, integridade psicológica, integridade existencial ou outros direitos pessoais inalienáveis. Isso acontece porque a seriedade do cenário é tão clara que não é preciso fornecer provas adicionais para confirmar o dano moral.

Trata-se de uma presunção de natureza judicial, então, lapidar neste sentido os ensinamentos de Eduardo Cambi e Renê Francisco Hellman³² de que:

Demonstrada a prova do fato lesivo, não há a necessidade de se comprovar o dano moral, porque ele é tido como lesão à personalidade, à honra da pessoa, revelando-se, muitas vezes, de difícil demonstração, por atingir reflexos estritamente íntimos.

Assim, basta a prova do fato lesivo para que se presuma o dano moral.

A Corte do STJ, em várias situações, entendeu estar configurado o dano moral in re ipsa, e a título de exemplo se pode citar: protesto indevido (REsp 1.432.324/SP, Rel. Ministro Paulo de Tarso Sanseverino, Terceira Turma, julgado em 18/12/14, DJe de 4/2/15); corpo estranho em produto alimentício (AgInt no REsp 1.517.591/MG, Rel. Ministro João Otávio de Noronha, Quarta Turma, julgado em 6/3/23, DJe de 9/3/23); danos físicos (REsp 1.306.167/RS, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 3/12/13, DJe de 5/3/14); morte de parente (AgInt no REsp 1165102/RJ, Rel. Ministro Raul Araújo, Quarta Turma, julgado em 17/11/16, DJe 07/12/16); recusa indevida do plano de saúde de realizar tratamento prescrito por médico (AgInt no AREsp 1573618/GO, Rel. Ministro Luis Felipe Salomão, Quarta Turma, julgado em 22/06/2020, DJe 30/06/2020); publicação não autorizada de imagem (AgInt no AgInt no AREsp 1546407/SP, Rel. Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 18/05/2020, DJe 26/5/20); falha da prestação de serviço essencial (AgInt no AREsp 771.013/RS, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 13/10/20, DJe 16/10/20).

No mais, não é possível aplicar a presunção para todas as situações que aparentem a existência de dano moral, isto porque, conforme entendimento expendido pelo STJ, quando do julgamento do REsp 1.653.413/RJ, de relatoria do Ministro Marco Aurélio Belizze:

A caracterização do dano moral in re ipsa não pode ser elasticizada a ponto de afastar a necessidade de sua efetiva demonstração em qualquer situação. Isso porque ao assim proceder se estaria a percorrer o caminho diametralmente oposto ao sentido da despatrimonialização do direito civil, transformando em caráter meramente patrimonial os danos extrapatrimoniais e fomentando a já bastante conhecida 'indústria do dano moral. (Terceira Turma, julgado em 5/6/18, DJe 8/6/18).

³² O dano moral in re ipsa e sua dimensão probatória na jurisprudência do STJ, Revista de Processo, vol. 291, Ano 44, São Paulo: Ed. RT. 2019, p. 317

No que diz respeito ao dano moral, a norma é a comprovação do prejuízo para a correta avaliação do montante da indenização, que deve ser proporcional às lesões sofridas, e não apenas à severidade da ação do infrator. O juiz determinará o limite entre o simples incômodo da vida da sociedade e o ato de dano que originou a compensação financeira.

Ademais, o próprio STJ, corroborando com este entendimento já se manifestou em diversos julgamentos, como elucidam trechos dos escólios selecionados, dentre outros:

A omissão de socorro, por si, não configura hipótese de dano moral *in re ipsa*.
4. Recurso especial provido para julgar improcedente o pedido de indenização por danos morais" (REsp 1.512.001/SP, relator Ministro Antonio Carlos Ferreira, Quarta Turma, julgado em 27/4/21, DJe de 30/4/21); "Para a pessoa jurídica, o dano moral não se configura *in re ipsa*, por se tratar de fenômeno muito distinto daquele relacionado à pessoa natural. É, contudo, possível a utilização de presunções e regras de experiência no julgamento" (REsp n. 1.564.955/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 6/2/18, DJe de 15/2/18); "O atraso, por parte de instituição financeira, na baixa de gravame de alienação fiduciária no registro de veículo não caracteriza, por si só, dano moral *in re ipsa*" (REsp n. 1.881.453/RS, relator Ministro Marco Aurélio Bellizze, Segunda Seção, julgado em 30/11/21, DJe de 7/12/21); "Não caracteriza dano moral *in re ipsa* os danos decorrentes de acidentes de veículos automotores sem vítimas, os quais normalmente se resolvem por meio de reparação de danos patrimoniais. 4. A condenação à compensação de danos morais, nesses casos, depende de comprovação de circunstâncias peculiares que demonstrem o extrapolamento da esfera exclusivamente patrimonial, o que demanda exame de fatos e provas. (REsp 1.653.413/RJ, relator Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 5/6/18, DJe de 8/6/18).

4.2.4 Do Enquadramento No Vazamento De Dados

Neste trabalho, não se sustenta a necessidade de que haja efetiva comprovação da dor ou sofrimento, até mesmo porque tais sentimentos não configuram elemento hábil à definição ontológica do dano moral, mas, tão somente, eventual consequência de lesão à personalidade.

Em se tratando de pleito indenizatório por danos morais, o que prescinde de comprovação, em realidade, são os efeitos psicológicos ocasionados à parte supostamente lesionada. Nesse passo, inviável o acolhimento da pretensão indenizatória deduzida, mormente por não configurar o caso hipótese de dano *in re ipsa*.

A obrigação de reparação, no contexto do vazamento de dados, não deve ser

aceita sem a comprovação do dano e do vínculo causal entre a ação e o evento prejudicial, pois isso implicaria uma descaracterização do propósito e dos componentes da responsabilidade civil.

O seguinte trecho das instruções que corroboram o entendimento pretoriano com o que se propõe agora. Em termos:

INDENIZATÓRIA. DANOS MORAIS. DIVULGAÇÃO INDEVIDA DOS DADOS CADASTRAIS EM GRUPO DE E-MAIL DE ALUNOS. AUSÊNCIA DE DEMONSTRAÇÃO DE QUALQUER ATO QUE PUDESSE IMPORTAR EM OFENSA AO DIREITO DE PERSONALIDADE DA AUTORA. SENTENÇA DE IMPROCEDÊNCIA MANTIDA. A divulgação dos dados cadastrais da autora e de outros alunos não é negada pela recorrida. Ao contrário, assumiu está a responsabilidade por eventuais danos que pudessem ocorrer. Caso em que não se cogita de dano moral na modalidade in re ipsa, havendo necessidade de comprovação, o que inócorre no caso concreto. A divulgação dos dados pessoais da autora, sem conotação pejorativa e por erro de uma funcionária da ré, não tem em sua essência o condão de caracterizar, por si só o dano moral. Ademais, a recorrida tomou todas as medidas cabíveis para minorar as chances de danos aos alunos que tiveram seus dados divulgados indevidamente, ingressando, inclusive com demanda judicial, menos de uma semana após a descoberta da divulgação, para anotar no SPC/SERASA, ao lado do CPF de cada um dos alunos, o vazamento sucedido, a fim de evitar fraudes com a utilização dos dados. Sentença de improcedência confirmada. RECURSO DESPROVIDO.

(TJRS. Recurso Cível nº 71003906021, Primeira Turma Recursal Cível, Relator Pedro Luiz Pozza, julgado em 13/09/2012 – grifou-se.)

Como é amplamente conhecido, as situações onde o sistema jurídico brasileiro permite a responsabilização sem a necessidade de comprovação do dano, ou seja, in re ipsa, são abordagens à regra.

No entanto, é importante destacar que a hipótese agora proposta não se enquadra em uma dessas situações específicas. Para dizer a verdade, levando em conta as especificidades do assunto em discussão, a única conclusão possível é que o vazamento de dados cadastrais, sem qualquer impacto específico, não causa dano moral, uma vez que não viola a dignidade humana.

Far-se-ia necessária, portanto, a prova da lesão efetiva para ocorrência dos danos morais, em que pese seja dispensada a comprovação das consequências da lesão sobre a sensibilidade da vítima.

4.3 Culpa Exclusiva De Terceiro

O artigo 43 da LGPD aborda as excludentes de responsabilidade dos

encarregados de tratamento, prevendo explicitamente, em seu inciso III, a isenção de responsabilidade quando o prejuízo for causado exclusivamente pelo proprietário dos dados ou por terceiros.

Frequentemente, os incidentes de vazamento de informações relacionados a um ataque sofrido por um terceiro mal-intencionado, conhecido como hacker . Contudo, apesar da visão comum de um hacker, ele não é necessariamente um criminoso que opera ilegalmente na internet.

Na lição de Liliana Minardi Paesani, muitos hackers têm por função atuar na correção de falhas de segurança em sistemas, com vistas a otimizar e melhorar a qualidade dos serviços prestados. Tal função é fundamental para garantir que apenas as pessoas que legitimamente possuem credenciais de acesso a determinado sistema, possam acessar determinadas contas criadas nas plataformas dos provedores de hospedagem³³.

Por outro lado, quando um hacker utiliza seus conhecimentos com o objetivo de infringir a lei, alcunha-se o mesmo como cracker, sendo os verdadeiros agentes causadores do ilícito.

No entanto, um dos maiores obstáculos na proteção dos titulares de dados na era digital é uma tarefa difícil de determinar com exatidão quem causou o dano, especialmente devido à natureza difusa e transnacional dos ataques cibernéticos. Como esses crimes cibernéticos geralmente não são identificados, as ações judiciais tendem a ser dirigidas contra aqueles que detém a guarda dos dados.

Em sendo assim, acaso uma empresa venha a ser alvo de um incidente de segurança que venha a acarretar um vazamento de dados, é necessário que esta, após a descoberta do ataque, não encubra o ocorrido, mas, sim, aja de forma escorreita e de boa-fé, comunicando toda sua base de usuários acerca do ocorrido, atuando de forma transparente e propositiva, reduzindo e mitigando, assim, qualquer responsabilidade.

Nesse sentido, ensina Roberto Senise Lisboa, citado por Marcel Leonardi³⁴:

Caso se demonstre a culpa exclusiva de terceiros, como se verifica na hipótese do hacker a provedora poderá se beneficiar dessa excludente de

³³ PAESANI, Liliana Minardi. Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil. 7. ed. São Paulo: Atlas, 2014. p. 22

³⁴ LEONARDI, Marcel. Responsabilidade Civil dos Provedores de Serviços de Internet. São Paulo: Juarez de Oliveira, 2005. p 70.

responsabilidade, recaindo o dever de indenização por danos morais em desfavor do real violador (artigo, II da Lei nº 8.078/1990).

Diante de todo o exposto, dúvidas não há quanto à impossibilidade de responsabilização de uma empresa pelo vazamento de dados quando o mesmo ocorre em virtude de ataque cibernético, hipótese na qual resta caracterizada culpa exclusiva de terceiro que reuniu esforços para que o prejuízo ocorresse, restando, portanto, configurada hipótese de fortuito externo.

4.4 A (Des)necessária Comprovação Do Dano Efetivo Na Busca Por Indenização

Apesar do conteúdo abordado neste estudo, em 2023, a Segunda Turma do Superior Tribunal de Justiça (“STJ”), por meio do Agravo em Recurso Especial (“AREsp”) 2.130.619, negou indenização por danos morais em casos de vazamento de dados sensíveis, estabelecendo um marco significativo na interferência do Brasil.

Na presente ação de reparação civil, o autor, na qualidade de usuário de plataforma digital, alegou, em síntese, que sofreu um ilícito civil consistente no vazamento de dados pessoais sensíveis, quais sejam: nome completo, data de nascimento, endereço residencial e número do documento de identificação. Sustentou, ainda, que tais informações foram indevidamente acessadas por terceiros e, em seguida, comercializadas, expondo-o a um risco concreto de fraudes e importunações, em violação ao seu direito à privacidade e à segurança.

O pedido inicial foi julgado improcedente em primeira instância, entretanto, o Tribunal de Justiça do Estado de São Paulo, em sede de apelação, reformou a sentença, reconhecendo a ocorrência de falha na prestação de serviços por parte da ré, empresa responsável pela plataforma digital, em virtude do vazamento dos dados pessoais do autor, configurando, assim, ato ilícito passível de indenização.

O caso chegou ao STJ, por meio de AREsp, restando determinada a exigência da demonstração do dano moral real, difere de outras interpretações que aceitaram o vazamento em si como o bastante para caracterizar o dano, evidenciando a discrepância contínua da legislação na aplicação da lei.

Quando falamos de comprovação de um direito subjetivo, enfrentamos desafios ainda maiores, tais como: i) a própria natureza intangível e subjetiva do dano, vez que se trata de um sofrimento íntimo, difícil de mensurar e provar; ii) a dificuldade em quantificar o dano, em vista que a avaliação do valor da indenização

por dano moral é complexa e também subjetiva; iii) a necessidade de perícias especializadas, para que se consiga comprovar a extensão do dano e o nexo causal entre o vazamento e o prejuízo.

Portanto, a exigência de comprovação do dano moral em situações de vazamento de dados, apesar de complicada, pois se busca sempre resguardar grandes corporações, que frequentemente impulsionam a economia do país, acaba por complicar o acesso à justiça dos proprietários dos dados afetados. A natureza subjetiva e intangível do dano moral, juntamente com a complexidade da prova, exige uma avaliação intrincada por parte dos profissionais do direito.

Assim, defende-se, inclusive neste estudo, a implementação de um regime de responsabilidade objetiva para os casos de vazamento de dados, com a inversão do ônus da prova.

A caracterização de dano moral *in re ipsa*, devido à severidade da violação e à complexidade de estabelecer a relação causal, juntamente com o reforço da tutela coletiva através de ações civis públicas, são ações essenciais para a proteção dos direitos dos proprietários de dados, particularmente em situações de vazamentos em larga escala.

4.4.1 Análise Dos Pressupostos No Precedente Firmado No AREsp nº 2.130.619/SP

Não obstante, passemos à análise do precedente do STJ no AREsp n. 2.130.619/SP estruturado com base em duas premissas fundamentais, quais sejam: (i) o art. 5º, II, da LGPD, traria um “*rol taxativo daquilo que seriam os dados sensíveis*”; e (ii) os dados pessoais comuns, fornecidos em qualquer tipo de cadastro, não seriam “*acobertados por sigilo, e o conhecimento por terceiro em nada violaria o direito de personalidade*”, de modo que “*diferente seria, se, de fato, estivéssemos diante do vazamento de dados pessoais sensíveis, que dizem a respeito à intimidade da pessoa natural*”, dando a entender haveria uma possibilidade de reconhecimento de um dano moral *in re ipsa*, se o vazamento incidisse sobre dados sensíveis, um conceito que estaria especificamente descrito na legislação.

Em uma breve análise do caso em comento, tratou-se de ação de reparação de danos morais, ajuizada por Maria Edite de Souza, em decorrência de um vazamento de dados ocorrido nas bases tecnológicas da empresa Eletropaulo Metropolitana

Eletricidade de São Paulo (ENEL), uma sociedade anônima. Conforme se extrai dos autos processuais, os dados pessoais vazados não eram sensíveis em uma análise à luz da Lei Geral de Proteção de Dados Pessoais (LGPD). Os dados vazados, conforme consta do relatório do Agravo em Recurso Especial nº 2.130.619.

A requerente fundamentou sua ação de reparação em dois principais pontos: a) os dados vazados lhe expuseram ao risco de fraudes; b) os dados vazados lhe expuseram ao risco de importunações. Ademais, pleiteou-se R\$15.000,00 (quinze mil reais) a título de danos morais, haja vista que o vazamento lhe deixou vulnerável a fraudes e importunações.

Na primeira instância a ação de reparação não teve procedência, sendo movido recurso de apelação.

Em acórdão concedeu-se danos morais de R\$5.000,00, com juros moratórios desde a citação e a correção monetária desde o arbitramento. A empresa, assim, ajuizou embargos de declaração, com alegações de que a decisão colegiada estava omissa em analisar normas jurídicas da Lei Geral de Proteção de Dados Pessoais. Os embargos de declaração foram acolhidos, porém o mérito do colegiado se manteve.

A empresa, então, interpôs o Recurso Especial. A fundamentação jurídica foi no sentido de que tal caso não poderia ser observado apenas à luz do Código de Defesa do Consumidor, devendo os dispositivos jurídicos da LGPD serem observados. Aduziu que o vazamento dos dados pessoais não foi culpa da empresa, mas sim um fato de terceiro, inclusive havia medidas de segurança informática para evitar tais tipos de incidentes. Assim, pleiteou a exclusão da responsabilidade, alegando violação, principalmente, aos artigos 944 e 186 do Código Civil.

Não teve contrarrazões ao Recurso Especial e o mesmo foi negado, motivo pelo qual a empresa ajuizou agravo em Recurso Especial, sendo de nº 2.130.619 –SP.

A decisão colegiada desse agravo está ementada da seguinte forma:

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.

(STJ - AREsp: 2130619 SP 2022/0152262-2, Data de Julgamento: 07/03/2023, T2 - SEGUNDA TURMA, Data de Publicação: DJe 10/03/2023)

Ocorre que, *data máxima vênia*, o entendimento expresso por unanimidade pela Segunda Turma difere significativamente da posição estabelecida na doutrina especializada. Essa afirmação se baseia em quatro motivos principais, como salientado por Lúcia Maria Teixeira³⁵.

Inicialmente. A doutrina e a jurisprudência estão cada vez mais reconhecendo o direito à proteção de dados como um novo direito da personalidade, fundamentado no princípio da dignidade humana e no direito ao desenvolvimento livre da personalidade. Nesse sentido, Danilo Doneda, em obra essencial sobre o assunto, conclui que, *“por força do regime privilegiado de vinculação entre a informação pessoal e a pessoa à qual ela se refere — como representação direta de sua personalidade —, tal informação deve ser entendida, portanto, como uma extensão da sua personalidade”*³⁶.

³⁵ FERREIRA, Lucia Maria Teixeira; GARCIA, Matheus. Responsabilidade civil por vazamento de dados pessoais: análise da decisão proferida no AREsp n. 2.130.619/SP. *Civilistica.com*, Rio de Janeiro, v. 13, n. 2, p. 1–31, 2024. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/1038>. Acesso em: 21 out. 2024.

³⁶ DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 148.

Concomitantemente, Bruno Ricardo Bioni é categórico ao dizer que “os dados que influem na projeção de uma pessoa e na sua esfera relacional adéquam-se conceitualmente como um novo direito da personalidade”³⁷. A propósito, cumpre observar que a própria LGPD, especificamente nos artigos 1º, caput, e 2º, VII, pela primeira vez na legislação brasileira, propoe uma previsão explícita do direito ao desenvolvimento livre da personalidade.

Além disso, é importante destacar que os direitos fundamentais, sob uma perspectiva subjetiva, têm eficácia tanto na relação entre o indivíduo e o Estado quanto nas interações entre os indivíduos.

Em segundo lugar. A linha que distingue um dado pessoal classificado como “comum” de um classificado como “sensível” não é clara e ultrapassa as relações relacionadas no artigo 5º, inciso II, da LGPD. É importante registrar que, no âmbito do processamento eletrônico de dados, não há mais dados sem importância.

Como bem destacado por Laura Schertel Mendes, “*decisivo para a concepção do direito à autodeterminação informativa é o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados*”, de modo que “*o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados tratados*”³⁸.

No terceiro lugar. Conforme a literatura especializada, o conceito de dados pessoais sensíveis é um exemplo. Conforme previsto no artigo 5º, inciso I, da LGPD, o dado pessoal sensível é definido como 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*”.

Por fim, em relação à violação de um direito fundamental, o dano moral ocorre in re ipsa, ou seja, surge inescapável do próprio ao lesivo. Conforme observado, o direito básico à proteção de dados pessoais, através das diversas posições legais deduzidas de seu conteúdo, visa fornecer ao indivíduo o controle efetivo sobre suas próprias informações. Portanto, se a perda do controle informacional for comprovada

³⁷ BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, 58

³⁸ MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. Revista Pensar, Vol. 25, n. 4, 2020, p. 11.

através do tratamento impróprio dos dados pessoais, configura-se a violação do direito.

Além disso, tal como ocorre na proteção conferida à imagem³⁹, necessário admitir que, em situações de tratamento impróprio de dados pessoais, a responsabilidade de componentes surge do uso indevido de um direito personalíssimo, não sendo legal solicitar ao titular a comprovação da ocorrência de danos ou prejuízos.

Com base nos argumentos apresentados, observa-se que a decisão tomada pela Segunda Turma do STJ no julgamento do AREsp número. 2.130.619/SP retoma o paradigma, atualmente ultrapassado, de que os dados pessoais não foram protegidos de forma independente pelo sistema jurídico, mas apenas a transmissão desses dados, protegidos pelo conceito de sigilo.

Na situação atual, os dados pessoais evoluíram de um recurso restrito e de pouca relevância legal para ganharem, inclusive, um valor específico do ponto de vista legal, possuindo agora, proteção jurídica independente. Conforme referência com frequência, os dados pessoais surgiram como o motor da nova economia da informação. Assim, a proteção dessas informações é fundamental para a proteção dos direitos dos cidadãos e para a manutenção do conceito de cidadania.

Portanto, como amplamente discutido neste estudo, deve-se admitir que, no caso de vazamento de dados pessoais, o dano moral surge *in re ipsa*, ou seja, da própria divulgação dos dados. Basta a detecção de um ato ilegal para efetivar o direito à indenização⁴⁰.

A violação do interesse juridicamente protegido - a perda do controle do fluxo de informações - é o suficiente para caracterizar o prejuízo, que ocorre no momento em que os dados pessoais são divulgados, tornando-se acessíveis a terceiros. Essa perda pode se somar a outros, inclusive de ordem material, que podem surgir da mesma ação danosa, como o uso de dados para fraudes entre outros delitos.

Dentro dessa perspectiva, é possível afirmar que, em uma sociedade baseada

³⁹ STJ, 2ª T., REsp 1.292.141/SP, Rel.ª Min.ª Nancy Andrighi, j. em 04.12. 2012.

⁴⁰ CARPENA, Heloisa. Os vazamentos de dados pessoais e a reparação dos danos coletivos à luz do CDC. In: SCHREIBER, Anderson; MARTINS, Guilherme Magalhães; CARPENA, Heloisa (coord.). Direitos fundamentais e sociedade tecnológica. Indaiatuba SP: Editora Foco, 2022, p. 23; FRAZÃO, Ana; CARVALHO, Angelo Prata; MILANEZ, Giovanna Curso de proteção de dados pessoais: fundamentos da LGPD. Rio de Janeiro: Forense, 2022, p. 441.

em dados, um incidente de segurança originado por culpa exclusiva de terceiros (por exemplo, um ataque hacker), apesar de ser deliberado e geralmente imprevisível, pode, dependendo das circunstâncias específicas, estar relacionado à própria ação do agente. Isso se insere entre os riscos que devem ser suportados por quem, no exercício de sua autonomia privada, em situações específicas.

Nessa direção, cabe ao intérprete examinar o nível de risco associado ao processamento de dados pessoais, juntamente com a adoção de uma conduta diligente pelo agente de tratamento, para, então, classificar o incidente de segurança como um evento fortuito interno ou externo. A LGPD corrobora essa orientação ao estabelecer que, ao aplicar os princípios de segurança e prevenção, o gestor deve considerar a estrutura, a escala e a quantidade de suas operações, além da sensibilidade dos dados manipulados e da probabilidade e severidade dos danos aos titulares dos dados (art. 50, § 2º, caput).

CONCLUSÃO

Atualmente, os dados pessoais se transformaram em verdadeiros ativos econômicos. No entanto, embora o progresso tecnológico e o tratamento de dados pessoais tenham melhorado a relação entre as empresas e seus clientes, também se inspirou um aumento expressivo nas infrações aos direitos de privacidade, devido à transferência de informações pessoais entre empresas, ameaçando os interesses pessoais dos proprietários desses dados, como a sua privacidade e a sua privacidade.

Além disso, a segurança dos dados pessoais tornou-se um direito essencial, seja através de uma decisão do Supremo Tribunal Federal ou pela aprovação de uma Proposta de Emenda Constitucional nesse sentido.

Incidentes de vazamento de dados pessoais ocorrem com a exposição de dados pessoais, cujos titulares podem se tornar vítimas de fraudes, de invasão de contas pessoais na internet, de roubo de identidade, dentre outros usos indevidos cometidos por terceiros. Isto porque, os invasores podem utilizar indevidamente esses dados, afetando a segurança daqueles que confiam os seus dados aos fornecedores.

Este estudo teve como objetivo analisar os mecanismos de responsabilização das empresas em caso de vazamento de dados pessoais, conforme previsto na Lei Geral de Proteção de Dados e no Código de Defesa do Consumidor, e avaliar a eficácia dessas disposições.

Neste contexto, foram envolvidos os princípios e conceitos da Lei Geral de Proteção de Dados e do Código de Defesa do Consumidor. Depois, examinamos as deliberações administrativas possíveis, com a participação conjunta da ANPD e das entidades de proteção ao consumidor.

Esses órgãos têm a capacidade de supervisionar e aplicar as decisões apropriadas aos transgressores da legislação sobre tratamento de dados pessoais e relações de consumo, dentro de suas respectivas competências, sem que isso resulte em um *bis in idem*.

Em seguida, analisou-se a responsabilidade civil aplicável aos agentes de tratamento de dados, por meio de um cotejamento entre o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados.

Ao passo em que existem autores que defendem que a Lei Geral de Proteção de Dados estabeleceu a responsabilidade na modalidade subjetiva, entende-se que a responsabilidade aplicável é a objetiva, em razão (i) da vulnerabilidade do titular frente

aos agentes de tratamento de dados; (ii) das semelhanças entre as disposições da Lei Geral de Proteção de Dados e do Código de Defesa do Consumidor; e (iii) do fato de a atividade daquele que exerce o tratamento de dados pessoais envolver um risco, enquadrando-se no parágrafo único do art. 927 do Código Civil.

Isto pois, a própria Lei Geral de Proteção de Dados reconhece a vulnerabilidade dos titulares de dados pessoais em relação aos agentes de tratamento de dados, ao prever a possibilidade de inversão do ônus da prova, a solidariedade entre o controlador e o operador, e ao prever as hipóteses de exclusão de responsabilidade.

Ainda, entende-se que o vazamento de dados pessoais configura um dano moral *in re ipsa*, uma vez que a divulgação de dados pessoais envolve a violação de direitos da personalidade e do direito fundamental à proteção de dados pessoais.

Contudo, os poucos julgados já proferidos pelo Tribunal de Justiça do Estado de São Paulo demonstram que a responsabilidade decorrente de vazamento de dados pessoais é uma questão ainda a ser consolidada na jurisprudência, principalmente pelos Tribunais Superiores.

Em razão da exposição de dados de milhões de indivíduos, faz-se necessária a utilização da tutela coletiva, e do instituto do dano *in re ipsa*, prevista tanto na Lei Geral de Proteção de Dados, quanto no Código de Defesa do Consumidor. A ação civil pública pode ser proposta pelos legitimados previstos no Código de Defesa do Consumidor e na Lei da Ação Civil Pública.

Esta avaliação evidencia que o vazamento ilegal de informações pessoais representa uma grave infração aos direitos fundamentais, resultando em danos de peças difíceis. O sistema jurídico do Brasil, especialmente a Lei Geral de Proteção de Dados e o Código de Defesa do Consumidor, estabelece mecanismos de responsabilidade objetiva para os responsáveis pelo tratamento de dados.

É crucial, portanto, a colaboração entre legisladores, entidades de proteção ao consumidor, e a Autoridade Nacional de Proteção de Dados para a execução de políticas públicas efetivas e a criação de um ambiente digital seguro e de confiança.

REFERÊNCIAS

ANPD. *ANPD está apurando no caso do vazamento de dados de mais de 220 milhões de pessoas*. Gov.br, [s.l.], 29 jan. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas>. Acesso em: 26 de set. 2024.

AGÊNCIA SENADO. *Senado inclui proteção de dados pessoais como direito fundamental na Constituição*. Senado Notícias, [s.l.], 20 out. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao>. Acesso em: 25 de outubro de 2024.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: A função e os limites do consentimento*. 2 ed. Rio de Janeiro: Forense, 2020. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788530988777/pages/recent>. Acesso em: 22 out. 2024.

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, Rio de Janeiro, a. 9, n.3, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662>. Acesso em: 22 out. 2024.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 de maio de 2024.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a Proteção de Dados Pessoais. Diário Oficial da União, Brasília-DF, 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 fev. 2024.

CAPANEMA, Walter Aranha. *A Responsabilidade Civil na Lei Geral de Proteção de Dados*. Cadernos Jurídicos, São Paulo, ano 21, n° 53, p. 163-170, Jan-Mar/2020.

CAVALIERI FILHO, Sergio. *Programa de Responsabilidade Civil*. 14 ed. São Paulo: Atlas, 2020. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788597025422/>. Acesso em: 22 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA. Incentivos estimulam digitalização de processos na Justiça alagoana. CNJ, 21 setembro 2016. Disponível em: Acesso em: 16 de outubro de 2024.

CONSELHO NACIONAL DE JUSTIÇA. Norma prevê digitalização de 100% dos processos da Justiça Eleitoral do DF. CNJ, 16 maio 2020. Disponível em: Acesso em: 17 outubro de 2024.

COTS, MÁRCIO; OLIVEIRA, RICARDO. *Lei Geral de Proteção de Dados Pessoais Comentada*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 25

DONEDA, DANILO. Informação e dados pessoais. In: DONEDA, D. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. Cap. 2.

FERRARESI, Eurico. *Ação Popular, Ação Civil Pública e Mandado de Segurança: instrumentos processuais coletivos*. 1 ed. Rio de Janeiro: Forense, 2019. Disponível em: <https://app.minhabiblioteca.com.br/#/books/978-85-309-5596-0/cfi/0!/4/2@100:0.00> Acesso em: 01 outubro. 2024.

FERREIRA, Lucia Maria Teixeira; GARCIA, Matheus. Responsabilidade civil por vazamento de dados pessoais: análise da decisão proferida no AREsp n. 2.130.619/SP. *Civilistica.com*, Rio de Janeiro, v. 13, n. 2, p. 1–31, 2024. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/1038>. Acesso em: 21 out. 2024.

GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro: Responsabilidade Civil. vol..4*. 15 ed. São Paulo: Saraiva Educação, 2020. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788553615957/>. Acesso em: 22 out. 2024.

GUERRA, Guilherme. *Dados de 533 milhões de usuários do Facebook estão expostos na internet*. Link Estadão, São Paulo, 03 abr. 2021. Disponível em: <https://link.estadao.com.br/noticias/empresas,dados-de-533-milhoes-de-usuarios-do-facebook-estao-expostos-na-internet,70003669377>. Acesso em: 10 maio 2024.

GOMES, ORLANDO. Memória justificativa do anteprojeto de reforma do código civil. Rio de Janeiro: Departamento de Imprensa Nacional, 1963.

JANKAVSKI, André. *Vazamento de dados: empresas não se protegem porque não querem, diz CEO da PSafe*. CNN, São Paulo, 13 mar. 2021. Disponível em: <https://www.cnnbrasil.com.br/business/2021/03/13/vazamento-de-dados-empresas-nao-se-protegem-porque-nao-querem-diz-ceo-da-psafe>. Acesso em: 10 maio 2024.

KHOURI, Paulo R. Roque A. *Direito do Consumidor: Contratos, responsabilidade civil e defesa do consumidor em juízo*. 7 ed. São Paulo: Atlas, 2021.

LEONARDI, Marcel. Responsabilidade Civil dos Provedores de Serviços de Internet. São Paulo: Juarez de Oliveira, 2005.

LIMA, Cíntia Rosa Pereira de (Coord). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Grupo Almedina (Portugal), 2020. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788584935796/pageid/156>. Acesso em: 22 out. 2024.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord). *LGPD: Lei Geral de Proteção de Dados Comentada*. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 415.

MENDES, Laura Schertel. O Direito Básico de Consumidor à Proteção de Dados Pessoais. *Revista de Direito do Consumidor*, vol., 95/2014, p. 53-75, Set-Out/2014, DTR\2014\10481.

MIGALHAS. *Associação processa Facebook por vazamento de dados de usuários brasileiros*. Migalhas, [s.l.], 20 de abril de 2021. Disponível em:

<https://www.migalhas.com.br/quentes/278853/associacao-processa-facebook-por-vazamento-de-dados-de-usuarios-brasileiros>. Acesso em: 11 de setembro. 2024.

MIRAGEM, Bruno. *A Lei Geral de Proteção (Lei n° 13.709/2018) e o Direito do Consumidor*. Revista dos Tribunais. [s.l.], v. 1009, 2019. Disponível em: <https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>. Acesso em: 22 setembro 2024.

MORAES, Alexandre de. *Direito Constitucional*. 37 ed. São Paulo: Atlas, 2021. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788597027648/>. Acesso em: 22 out. 2024.

MULHOLLAND, Caitlin. *A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?* Migalhas. 30 jun. 2024. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-ofundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais-culpaou-risco>. Acesso em: 18/05/2024.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. *Responsabilidade Civil na LGPD: Problemas e Soluções*, CONPEDI LAW REVIEW, v. 6, n. 1, p. 158-174, Jan- Dez/2020. Disponível em: <https://www.indexlaw.org/index.php/conpedireview/article/view/7024>. Acesso em: 22 setembro 2024.

OLINTO, ANTONIO. *Minidicionário Antônio Olinto da língua portuguesa*. Tradução de Ubiratan Rosa. São Paulo: Moderna, 1919.

PADILHA, Rodrigo. *Direito Constitucional*. 6 ed. São Paulo: Método, 2020. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788530988319/cfi/6/10!/4/2/4@0:0>. Acesso em: 01 out. 2024.

PANEK, Ling Cristina Tung. *Lei geral de proteção de dados n° 13.709/2018: uma análise dos principais aspectos e do conceito privacidade na sociedade informal*.

2019. 33 p. Monografia (Graduação em Direito) – Universidade Federal do Paraná, Curitiba, 2019.

PESTANA, Marcio. *Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais)*. Consultor Jurídico. Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 18/05/2024

PEREIRA, Caio Mario da Silva. *Responsabilidade Civil*. 12 ed. Rio de Janeiro: Forense, 2018. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788530980320/>. Acesso em: 22 out. 2024.

PINHEIRO, Patrícia Peck. *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (LGPD)*. São Paulo: Saraiva, 2021. Disponível em: [https://app.minhabiblioteca.com.br/reader/books/9786555595123/epubcfi/6/44\[%3Bvnd.vst.id.ref%3Dmiolo17.xhtml!\]/4/2/2/1:0\[%2CREF\]](https://app.minhabiblioteca.com.br/reader/books/9786555595123/epubcfi/6/44[%3Bvnd.vst.id.ref%3Dmiolo17.xhtml!]/4/2/2/1:0[%2CREF]). Acesso em: 22 out. 2024.

PROCON-SP, Assessoria de Comunicação. Serasa complementar resposta sobre vazamento de dados. *PROCON-SP*, 06 abr. 2021. Disponível em: <https://www.procon.sp.gov.br/serasa-complementa-resposta-sobre-vazamento-de-dados/>. Acesso em: 26 de set. 2024.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40–81, 2018.

RIZZARDO, Arnaldo. *Responsabilidade Civil*. 8 ed. Rio de Janeiro: Forense, 2019, p. 26.

SCHMITT, Cristiano Heineck. *Responsabilidade Civil*. Porto Alegre: Verbo Jurídico, 2010.

SETZER, VALDEMAR W. Dado, Informação, Conhecimento e Competência, São Paulo, maio 2015. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/44270487/ART_2_GEST.pdf?1459453402=&re

[sponsecontentdisposition=inline%3B+filename%3DDado+Informacao+Conhecimento+e+Competenc.pdf&Expires=1594060757&Signature=bExxhJPnU947pfHVGQ8ugh7rqk~KsZJOAraqvSqPorc-A6TPKUYNEI~M4.](#)

SARLET, GABRIELLE BEZERRA SALES; CALDEIRA, CRISTINA. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com*, Rio de Janeiro, p. 7, 2019. Disponível em: <<http://civilistica.com/o-consentimento-informado-e-a-protecao/>>. Acesso em: 19 setembro 2024.

SOUTO, Gabriel Araújo. Vazamento de dados no setor privado brasileiro: a gestão do risco como parâmetro para a responsabilidade empresarial. *Revista de Direito e as Novas Tecnologias*, vol. 7/2020, Abr-Jun/2020, DTR\2020\7817.

TARTUCE, Flávio. *Manual de Direito do Consumidor: direito material e processual, volume único*. 10 ed. Rio de Janeiro: Forense, 2021. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786559640270/cfi/6/10!/4/2/4/2@0:0>. Acesso em: 07 out. 2024.

TARTUCE, Flávio. *Responsabilidade Civil*. 3 ed. Rio de Janeiro: Forense, 2021. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786559640959/>. Acesso em: 22 out. 2024.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. 2 ed. São Paulo: Thomson Reuters Brasil, 2020.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Tratamento de dados pessoais na LGPD: estudo sobre as bases legais*. *Civilistica.com*, [S. l.], v. 9, n. 1, p. 1-38, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em: 27 fev. 2024.

TEFFÉ, Chiara de; MAGRANI, Eduardo; VIOLA, Mario. *5 pontos sobre a importância de uma autoridade nacional de proteção de dados*. ITS Rio. 6 nov. 2018. Disponível em: <https://itsriodejaneiro.medium.com/5-pontos-sobre-a-import%C3%A2ncia-de-uma-autoridade-nacional-de-prote%C3%A7%C3%A3o-de-dados-4cf8137cf59e>)

Acesso em: 18/05/2024

THEODORO Jr., Humberto. *Direitos do Consumidor*. 10 ed. Rio de Janeiro: Forense, 2021. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788530992941/>.

Acesso em: 22 out. 2024.

VENOSA, Silvio de Salvo. *Direito Civil: Obrigações e Responsabilidade Civil*. vol. 2, 21 ed. São Paulo: Atlas, 2021. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788597026696>. Acesso em: 22 out. 2024.

VENTURA, Felipe. *Vazamento do Facebook expõe 533 milhões de usuários, incluindo brasileiros*. *Tecnoblog*, [s.l.], 05 abr. 2021. Disponível em: <https://tecnoblog.net/428248/vazamento-do-facebook-expoe-533-milhoes-de-usuarios-incluindo-brasileiros/>. Acesso em: 10 maio 2024.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. 2007. 297 p. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2007.

WARREN, Samuel; BRANDEIS, Louis. “*The Right to Privacy*”. *Harvard Law Review*, Vol. VI, n° 5, 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents. Acesso em: 22 out. 2024.

WACKS, Raymond. *Personal Information: Privacy and the Law*. Oxford: Oxford University Press, 1989. p. 25. Vide, também, MENDES, Laura Schertel. *Habeas datae autodeterminação informativa: os dois lados da mesma moeda*. *Direitos Fundamentais & Justiça*, v. 12, n. 39, p. 185–216, 2018, p. 200; ALBERS, Marion. A

complexidade da proteção de dados. *Direitos Fundamentais & Justiça*, v. 10, n. 35, p. 19–45, 2016, p. 30-32.

ZENO-ZENCOVICH, Vincenzo. Informação (profili civilistici). In: *Digesto –Sezione Civile*. v. IX. Torino: UTET, 1993. p. 3. Tradução livre de: “per informazione si intende qualsiasi dato rappresentativo della realtà che viene conservato da un soggetto oppure comunicato da un soggetto ad un altro”.