UNIVERSIDADE FEDERAL DO PAMPA

CURSO DE DIREITO

MATHEUS DELTREGIA REYS

RESPONSABILIZAÇÃO CIVIL *IN RE IPSA* NA LEI GERAL DE PROTEÇÃO DE DADOS

SANTANA DO LIVRAMENTO

2021

MATHEUS DELTREGIA REYS

RESPONSABILIZAÇÃO CIVIL *IN RE IPSA* NA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado como requisito para obtenção de título de Bacharel em Direito pela Universidade Federal do Pampa – UNIPAMPA

Orientadora: Profa. Júlia Bagatini
Doutoranda

SANTANA DO LIVRAMENTO

2021

RESPONSABILIZAÇÃO CIVIL *IN RE IPSA* NA LEI GERAL DE PROTEÇÃO DE DADOS

MATHEUS DELTREGIA REYS

Aprovado em ___/___/___.

BANCA EXAMINADORA

_____

Professora Júlia Bagatini
Universidade Federal do Pampa

_____

Professor João Paulo Rocha de Miranda
Universidade Federal do Pampa

_____

Professora Alessandra Marconatto
Universidade Federal do Pampa

RESUMO

O presente trabalho tem por objetivo delimitar a pertinência e a abrangência da aplicação de indenização por danos morais *in re ipsa* ocasionados aos titulares de dados, os quais reiteradamente têm seu direito fundamental de privacidade violado por meio da coleta, armazenamento e compartilhamento excessivo e ilegal de dados pessoais. Isso gera como consequência vazamento de dados cada vez mais frequentes e com maiores consequências a diversos indivíduos. Busca-se analisar a responsabilização objetiva dos agentes de tratamento de dados, almejando-se compreender se é possível a ocorrência de danos morais *in re* ipsa quando da violação de dados sigilosos devido ao descumprimento dos deveres de segurança dos agentes de tratamento, ou se esses danos devem ser comprovados pelos titulares de danos que sofrem a lesão à privacidade. Partindo-se de uma análise doutrinária e jurisprudencial acerca do tema, a partir do estudo de bibliografias acerca do tema, além de decisões judicias recentes, foi possível entender que a responsabilização por danos morais *in re ipsa* não é entendido como regra geral, pois na maioria dos casos os titulares de dados devem provar que os vazamentos de dados lhes geraram um abalo psíquico que permite a caracterização de dano moral. Logo, se entende que a expectativa de danos morais em si, pelos titulares de dados, não possibilita necessariamente a responsabilização dos agentes de tratamento pelos danos surgidos em incidentes de segurança.

Palavras-Chave**:** Direito de Privacidade. Lei Geral de Proteção de Dados. Vazamento de Dados. Danos morais *in re ipsa*

ABSTRACT

The present works aims to delimit the pertinence and scope of the application of compensation moral damages *in re ipsa* to data owners, who repeatedly have their fundamental right of privacy violated through the excessive and ilegal gathering, storage and sharing of personal data, which results in increasingly frequent data leakage, with greater consequences for different individuals.The ai mis to analyze the objective liability of data processing agentes, aiming to understand whether it is possible for moral damages to occur *in re ipsa* when confidential data is breached due to non compliance with the securities of the processing agentes, on if these damages must be verified by the data owners who suffer the damage to privacy . Starting from a doctrinal and case law analysis on the subject, the work seeks to delimit the level of proctetion that data owners need in order to not have their data leaked, with the analysis of the adequacy of the application of moral damages *in re ipsa* to processing agentes that act illegally, not adopting security measures in order to prevent the occurrence of damage to data owners. Therefore, it is understood that the expectation of pain and suffering in itself, by data owners, does not necessarily allow the processing agentes to be held liable for damages arisen from security incidents.

Keywords: Right to privacy. General Data Protection Law. Data leakes. Moral damages *in re ipsa*

SUMÁRIO

1. INTRODUÇÃO..... 8
2. DIREITO FUNDAMENTAL À PRIVACIDADE E À AUTODETERMINAÇÃO INFORMATIVA..... 10
2.1 A privacidade no âmbito da Sociedade Informacional..... 10
2.2 O imperativo da vigilância.....12
2.3 O direito à autodeterminação informativa.....13
2.4 A aplicação dos princípios da Lei Geral de Proteção de Dados..... 15
3. RESPONSABILIDADE CIVIL OBJETIVA NO CÓDIGO CONSUMERISTA E NA LEI GERAL DE PROTEÇÃO DE DADOS..... 18
3.1 Noções gerais de responsabilidade civil objetiva..... 18
3.2 A responsabilidade pela má- prestação de serviços no Código Consumerista... 19
3.3 A responsabilidade dos agentes de tratamento por meio da aplicação da Lei Geral de Proteção de Dados..... 23
4. OS DANOS MORAIS *IN RE IPSA* NO CONTEXTO DE VAZAMENTO DE DADOS..... 28
4.1 Os danos morais e suas espécies..... 28
4.2 Violação de dados sigilosos..... 31
4.3 Aplicabilidade dos danos morais em decisões judiciais..... 36
4.4 Vazamento de dados e a aplicação de danos morais *in re ipsa* nas decisões do Tribunal de Justiça do Estado de São Paulo e na doutrina recente..... 39
5. CONCLUSÃO..... 43
6. REFERÊNCIAS.....

Ficha catalográfica elaborada automaticamente com os dados fornecidos pelo através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais).

Reys, Matheus Deltregia
Responsabilização Civil *in re ipsa* na Lei Geral de Proteção de Dados. – 2021
51 p.

Orientadora: Júlia Bagatini
Trabalho de Conclusão de Curso (Graduação) – Universidade Federal do Pampa – DIREITO, Campus de Santana do Livramento, 2021

1.Direito de Privacidade 2. Lei Geral de Proteção de Dados 3.Danos Morais *in re ipsa*. I. Reys, Matheus Deltregia II. Título.

AGRADECIMENTO

À Professora Dra. Júlia Bagatini pela orientação e apoio a fim de que eu realizasse o Trabalho de Conclusão de Curso

À minha família, por sempre me apoiarem e estimularem os meus estudos, a fim de que eu obtivesse um aprendizado não apenas para me qualificar formalmente, mas também para me tornar uma pessoa melhor e um cidadão mais responsável

Aos meus amigos que fiz durante o curso, ao longo desses últimos cinco anos

A todas as pessoas que, direta ou indiretamente, contribuíram para a realização deste trabalho.

1. INTRODUÇÃO

A discussão a respeito da aplicação de danos morais *in re ipsa* no contexto de vazamento de dados está atrelada fundamentalmente à importância que os dados pessoais assumiram na atual Sociedade Informacional, no contexto do capitalismo pós-industrial. Os dados pessoais são coletados, armazenados e compartilhados por diversas empresas, que dependem dessas informações para desenvolverem seus negócios e otimizarem seus lucros.

Os titulares de dados, por sua vez, muitas vezes equiparados a consumidores, necessitam fornecer com maior ou menor frequência os seus dados e, portanto, tem sua vulnerabilidade maximizada, caso os sujeitos que tratem seus dados não tomarem as precauções a fim de garantir a inviolabilidade desses, o que acarreta uma situação de potencial violação aos direitos de personalidade dos titulares de dados. A violação de dados sigilosos é mais frequente quando o próprio titular de dados não possui qualquer controle sobre suas informações pessoais, que circulam por banco de dados pela internet.

Com o advento da Lei Geral de Proteção de Dados, houve a regulamentação das atividades atreladas ao tratamento de dados, necessária a discussão das mudanças que esta Lei ocasionou no contexto de proteção de dados pessoais, a partir de elementos essenciais como a figura do consentimento, os princípios elencados na lei e a responsabilização civil que poderão sofrer os agentes de tratamento, caso agirem em desconformidade com a normativa supracitada.

É importante questionar, a partir de um amplo debate, de que maneira e em que grau as pessoas jurídicas de direito privado estão regulamentando suas atividades de tratamento de dados e de que maneira, a partir da vigência da Lei Geral de Proteção de Dados e das sanções administrativas presentes nesta lei, aquelas vão adotar medidas de *compliance* a fim de prevenir os danos ao direito de privacidade dos titulares de dados, que com maior frequência estão expostos a riscos de vazamentos de dados, devido à ineficácia das medidas de segurança adotadas pelos agentes de tratamento.

O presente trabalho pretende responder de que forma, a partir do advento da Lei Geral de Proteção de Dados, os agentes de tratamento serão responsabilizados, caso, no contexto de vazamento de dados, ocasionarem danos extrapatrimoniais aos titulares de dados. A princípio, surgem danos morais *in re ipsa* devido à violação do sigilo dos dados, pois é uma situação que afronta diretamente o direito fundamental da privacidade.

O objetivo do trabalho é analisar a necessidade e a adequação da aplicação de danos morais *in re ipsa* no contexto de vazamento de dados, levando em conta a lesão ao direito fundamental da privacidade e a cláusula da dignidade. Assim, busca-se compreender se é possível presumir o prejuízo do titular quando do compartilhamento irregular de dados ou é necessário a comprovação do prejuízo desses em cada caso concreto.

Para a realização desse trabalho foi utilizado o método dedutivo e a técnica de pesquisa documental indireta, havendo a escolha de cinco decisões judiciais do Tribunal de Justiça de São Paulo, além de decisões do Superior Tribunal de Justiça, que trazem relevantes interfaces entre o Código Consumerista e a Lei Geral de Proteção de Dados. A escolha desse Tribunal em especial é devido a maior quantidade de empresas alocadas nesse Estado, o que, por conseguinte, verifica-se a maior quantidade de decisões judiciais que trabalham o tema proposto neste trabalho.

Entendeu-se, a partir da análise doutrinária e jurisprudencial, que pode-se considerar o dano moral *in re ipsa* em situações específicas, em que se presume uma conduta mais gravosa dos agentes de tratamento de dados ou no casos em que os incidentes de segurança envolvem dados sensíveis, os quais possuem maior risco de, quando compartilhados de forma irregular, gerarem consequências mais gravosas, como um tratamento discriminatório, que é considerado irregular.

Primeiramente, será delimitado a questão associada ao direito fundamental da privacidade na Sociedade Informacional, e a delimitação dos princípios elencados na Lei Geral de Proteção de Dados. Em seguida se demarcará as interfaces entre o Código Consumerista e a legislação de proteção de dados, em relação a responsabilidade civil objetiva dos agente de tratamento de dados/ fornecedores de serviços. Por último se especificará a aplicação dos danos morais *in re ipsa* no contexto de vazamento de dados, utilizando a doutrina recente e decisões judiciais do Tribunal de Justiça de São Paulo e do Superior Tribunal de Justiça

2. O DIREITO FUNDAMENTAL À PRIVACIDADE E A AUTODETERMINAÇÃO INFORMATIVA

A partir do direito fundamental à privacidade, expresso na Constituição Federal, e do contexto da denominada Sociedade Informacional, verificar-se-á os riscos dessa à tutela da privacidade dos indivíduos frente aos particulares e ao Estado. Delimitar-se-á a posição do consumidor frente ao Imperativo da Vigilância, e a necessidade da autodeterminação informativa por parte desse, a fim de que esse possa tutelar seus dados pessoais.

No final do capítulo será analisado importância da Lei Geral de Proteção de Dados para garantir o respeito ao direito fundamental da privacidade dos titulares de dados, e se elencará os princípios que fundamentam a Lei n° 13.853/2019, e aplicação desses com a finalidade de garantir o direito de autodeterminação informativa por parte dos titulares de dados.

2.1 A Privacidade no âmbito da Sociedade Informacional

O Direito fundamental à privacidade está atrelado a deveres essenciais, impostos a entidades privadas e públicas de toda a sociedade, relacionados à proteção da incolumidade psíquica e física dos cidadãos, que não podem ter suas informações pessoais devassadas, sob risco de se perder a sustentação dos valores de liberdade e igualdade de um Estado Constitucional Democrático de Direito.

Os deveres essenciais dessas instituições sociais são a de garantir a todos um núcleo fundamental de intimidade, que possibilita os cidadãos de desenvolverem livremente sua personalidade, minimizando e mitigando os riscos de incidentes que perturbem o sossego e a vida privada daqueles que querem desenvolver atividades das mais variadas possíveis, dentre elas atividades de consumo.

O direito à privacidade está atrelado a autonomia que um indivíduo tem em relação à informação sobre si e sua vida privada, a qual está tangenciada por múltiplas relações sócio jurídicas, dentre elas as relações de consumo. Dentro de uma sociedade pluralista, o titular do direito à privacidade deve possuir um espaço para desenvolver livremente a sua personalidade, pois uma democracia constitucional deve garantir uma sociedade livre e baseada na dignidade humana e na autodeterminação dos indivíduos (MENDES, 2008, p.25).

Um dos desafios maiores da sociedade atual é harmonizar o direito de privacidade com o desenvolvimento da tecnologia da informação, inclusive porque as tecnologias de informação irradiam-se rapidamente no seio das relações socioeconômicas. Há o que se denomina de Sociedade Informacional, a qual está baseada em um alto grau de desenvolvimento de tecnologias de informação e comunicação, que são fatores em um grande processo de transformação da base capitalista e também da base informacional. O capitalismo pós-industrial ("Economia Flexível") está alicerçado em organizações produtivas descentralizadas e flexíveis, em novos modelos de gerenciamento e de marketing, onde a informação, proveniente dos dados dos consumidores, é o núcleo essencial que possibilita a intensificação dos fluxos financeiros, gerando maior lucratividade para as empresas.

Pode-se dizer que a geração, o processamento e a difusão de informações, a partir do tratamento de dados, tornaram-se essenciais na vida em sociedade e cabe aos Estados, por meio de legislações e regulamentos, regular o tratamento de dados pessoais, ou seja, aqueles que repercutem no âmbito da liberdade e da privacidade dos cidadãos.

Os cidadãos consumidores necessitam, a fim de estabelecer suas relações de consumo com os fabricantes, disponibilizar uma série de informações pessoais, as quais formam os bancos de dados, verdadeiros perfis de consumidores, as quais destacam as tendências e hábitos de consumo dos indivíduos. Isto garante uma vantagem econômica a um consumidor, porém pode repercutir negativamente em sua privacidade, caso essa não for resguardada, em hipóteses que houver um tratamento inadequado desses dados, gerando vazamento de dados a terceiros, por exemplo.

A fim de se resguardar o direito fundamental à privacidade e garantir o livre desenvolvimento da personalidade das pessoas naturais (elementos chaves elencados no artigo 1° da Lei Geral de Proteção de Dados), é necessário aplicar as garantias e direitos fundamentais expressos na Carta Política, expressos em seu artigo 5°, incisos X e XII. Ambos incisos traduzem a necessidade de preservação da intimidade e da vida privada dos cidadãos, sendo que o segundo elenca a necessidade de manutenção de sigilo de comunicações telefônicas, e por meio de interpretação extensiva, aplica-se às comunicações por meio da internet. A Lei Geral de Proteção de Dados, em seu art. 17, destaca a necessidade da proteção do direito de personalidade:

> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Por conseguinte, a partir do direito fundamental de privacidade, presente na Carta Cidadã, e reiterado na Lei Geral de Proteção de Dados, é possível garantir ao titular de dados um espaço privado frente ao chamado “Big Data”, onde há, pelas pessoas jurídicas privadas, o uso de dados pessoais de forma irrestrita a fim de auferir lucro.

2.2 O Imperativo da Vigilância

O cidadão – consumidor, titular de dados pessoais, está à mercê de uma vigilância ininterrupta de empresas as quais fornecem produtos e serviços a partir dos dados pessoais fornecidos pelas pessoas naturais. A fim de se garantir a aplicação da tutela constitucional ao consumidor, é preciso constatar a natureza assimétrica entre o fabricante (empresário que busca captar, tratar e difundir dados pessoais com o fito de lucro) e o comerciante, que é vulnerável, pois muitas vezes não tem o conhecimento informacional e técnico acerca dos serviços que estão sendo prestados, que dependem do processamento e tratamento de dados pessoais, em relação aos quais os consumidores muitas vezes nem acesso possuem.

É importante que haja o reconhecimento do consumidor da vulnerabilidade no ciberespaço, a fim de proteger o consumidor em uma sociedade massificada e informatizada, o que se coaduna com o artigo 4°, inciso I do Código Consumerista, que identifica o reconhecimento da vulnerabilidade como um dos objetivos da Política Nacional das Relações de Consumo. O alicerce mais importante do Direito Consumerista é o Princípio da Vulnerabilidade, por meio do qual o Direito Brasileiro reconhece o consumidor não apenas como sujeito de direito, mas também como sujeito social que carece de uma tutela específica a fim de garantir o equilíbrio nas relações de consumo (TEIXEIRA, 2015, p. 442).

A vigilância sobre os dados pessoais dos indivíduos não apenas interfere na dimensão da liberdade/intimidade, mas também em relação a dimensão da igualdade, pois é possível que um tratamento inadequado dos dados gere uma rotulação discriminatória dos indivíduos, por meio de técnicas de *profiling* (segmentação de mercado). A formação de perfil de um consumidor, com seu consentimento, por si só não acarreta uma violação a seu direito de personalidade, sendo uma técnica de obtenção de informações a que pode facilitar e acelerar a relação de consumo. O problema surge quando não se tem o consentimento do indivíduo em relação ao dado que está sendo tratado, e muitas vezes os cruzamentos desses dados podem acarretar a formação de um perfil indesejado. Essa técnica de construção de perfis permite a

tomada de decisões importantes acerca dos consumidores e cidadãos em geral, afetando a vida das pessoas e influenciando o seu acesso a oportunidades sociais (MENDES, 2008, p.107).

O imperativo da vigilância está presente no contexto da Economia Flexível, em que ocorre a customização da produção, o que possibilita maiores oportunidades de negócios para os empresários juntamente com uma redução de riscos em suas atividades econômicas, pois a informação sobre o consumidor é o elemento chave nessa nova ótica.

Surge, por conseguinte, o denominado "consumidor de vidro", que tem suas informações e hábitos de consumo devassados. As empresas saem ganhando, pela dimensão de custos e de concorrência, porém há uma ameaça ao equilíbrio de mercado e à liberdade e igualdade dos consumidores, caso o fluxo de dados for utilizado para limitar indevidamente o acesso dos consumidores a serviços e produtos e classifica-los de forma discriminatória (MENDES, 2008, p.85).

2.3 O Direito à Autodeterminação Informativa

A fim de se possibilitar e legitimar o acesso dos cidadãos – consumidores aos seus dados, em um contexto de descentralização de múltiplos bancos de dados, é necessário se garantir a autodeterminação informativa desses, um dos elementos basilares da Lei Geral de Proteção de Dados.

O Direito de Autodeterminação Informativa é uma garantia fundamental aos cidadãos, de modo que possibilita o indivíduo ter um controle sobre as informações pessoais sobre si, que são objeto de coleta, tratamento e compartilhamento na forma de dados. É um direito de liberdade dada aos indivíduos, que os possibilita a escolher com quem pretendem compartilhar sua privacidade, partindo-se do pressuposto que o indivíduo pode vetar qualquer ingerência não consentida em relação a dados pessoais que quer manter em sigilo (RUARO, 2020, p. 5).

Do direito de privacidade informacional (autodeterminação informativa) decorre a necessidade de que haja o prévio consentimento à coleta e ao tratamento de dados pessoais. Pode-se afirmar que:

> A autodeterminação informativa resguarda o titular dos dados contra a utilização indevida de suas informações, coibindo discriminações e controles sociais calcados em bancos de dados que não são de conhecimento do titular tudo como corolário ao princípio da dignidade da pessoa humana (RUARO,2020, p.10).

A autodeterminação informativa tem como elemento essencial o consentimento, que de acordo com o artigo 9° da Lei Geral de Proteção de Dados, será válido caso informar de forma clara e precisa quais são os dados objetos da coleta, a forma pelos quais esses serão tratados, a finalidade do tratamento, com quem serão compartilhados, além da identificação dos agentes de tratamento e as responsabilidades desses em relação ao desempenho de suas funções associada ao tratamento dos dados. Por conseguinte, não são poucos os requisitos para que o consentimento seja válido e regular, sendo que o parágrafo 4° da mesma Lei deixa explícito que o consentimento será nulo, caso não se referir a finalidades específicas.

No direito consumerista o direito à autodeterminação informativa é essencial a fim de reequilibrar a relação desigual de consumo, possibilitando ao consumidor o direito de ter o conhecimento prévio e atualizado sobre o serviço ou o produto que vai consumir. Está expresso no art. 6°, inciso III, do Código Consumerista, o dever de informação por parte do fornecedor (decorre do princípio da boa-fé objetiva). A informação deve ser fornecida de forma clara, adequada e suficiente, cumprindo com sua finalidade de esclarecer o consumidor, a fim de esse consentir com a relação de consumo que surgirá.

O direito básico à informação do consumidor é um dos pilares da proteção ao consumidor brasileiro, pois tem como finalidade promover o equilíbrio relacional entre consumidores e fornecedores, ao assegurar a existência de uma equidade informacional entre as partes (MIRAGEM, 2016, p. 216).

A fim de haver a proteção das informações pessoais do consumidor em um banco de dados, o próprio Código de Defesa do Consumidor, no artigo 43 (muito antes da Lei n°13.708/2018), indica que se deve garantir, de forma facilitada, o acesso dos consumidores sobre seus dados em cadastro e que esses dados deveriam estar escritos de forma clara e simplificada, havendo um prazo máximo de cinco anos para a manutenção de informações negativas sobre os consumidores, havendo a eliminação desses dados posteriormente.

> Art. 43 CDC O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
>
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
>
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
>
> § 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Por sua vez, a Lei Geral de Proteção de dados traz de forma muito enfática o direito de acesso do titular (art. 18) aos seus dados pessoais, e principalmente sobre a figura do consentimento, que de acordo com o art. 5°, inciso XII da Lei supracitada, deve ser livre (sem vício de consentimento), informada (precisão e atualização das informações) e inequívoca (clareza, de forma simplificada).

O consentimento, dependendo da finalidade específica do tratamento, pode ser prévio ou posterior, sendo que nesse último caso a existência do tratamento deve ser comunicado, por escrito, ao titular de dados. O § 6° do art. 7 ° da mesma Lei indica que, mesmo havendo dispensa de consentimento, deve haver, por parte dos agentes de tratamento, observância dos Princípios elencados por esta Lei e dos direitos do titular. Há a possibilidade expressa de o titular de dados peticionar a qualquer tempo, por meio de um procedimento simples e gratuito, pela revogação do tratamento de seus dados (art. 8 °, § 5° da Lei 13.708/2018).

2.4 A Aplicação dos Princípios da Lei Geral de Dados

Com o advento da Lei Geral de Proteção de Dados, passou-se a regulamentar as atividades de tratamento de dados pessoais. Dados pessoais estão relacionados à informações privadas de pessoa natural. Por sua vez as atividades de tratamento de dados podem ser entendidas como:

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

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

Ao se discutir a aplicação de princípios da Lei Geral de Proteção de Dados e o direito de autodeterminação informativa é importante salientar que há duas figuras essenciais que compõem a atividade de tratamento de dados, as quais são os titulares de dados e os agentes de tratamento de dados, que são o controlador e o operador, tudo de acordo com o art. 5°, incisos V e IX, da Lei Geral de Proteção de Dados.

O art. 6° da Lei Geral de Proteção de Dados elenca os princípios que correspondem a direitos de titulares de dados pessoais. A aplicação desses princípios é essencial, a fim de garantir elementos-chave como liberdade e igualdade, os quais devem convergir para que o direito de privacidade se concretize ao tratamento de dados pessoais. Destacar-se-ão algum dos princípios elencados no rol a seguir:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas 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 difusão;

> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Em relação ao princípio de finalidade, o titular de dados tem o direito de possuir informações claras e precisas que indiquem quais dados estão sendo coletados e quais as finalidades específicas desse tratamento, além de indicar quais as medidas utilizadas para se assegurar o cumprimento desse princípio. As finalidades de qualquer tratamento de dados pessoais devem ser legítimas e específicas, sendo que, havendo a mudança de finalidade, o titular de dados deverá ser informado dessa de forma célere, a fim de atualizar o consentimento à atividade desenvolvida (art. 9°, § 2° da Lei Geral de Proteção de Dados). Pode-se afirmar que:

> [...] a partir da promulgação da LGPD, não é mais possível o tratamento de dados pessoais com finalidades genéricas ou indeterminadas. O tratamento deverá ser feito com fins específicos, legítimos, explícitos e informados, devendo as empresas explicar para que usarão cada um dos dados pessoais. (FLUMIGNAN; FLUMIGNAN, 2020, p.128).

A partir do princípio de Adequação, pode-se infirmar que só a partir desse o tratamento estará conforme com as finalidades informadas ao titular de dados. Em relação ao princípio da Necessidade, intrinsecamente relacionado ao último, este implicará maior responsabilidade para o agente de tratamento de dados, que deverá coletar e armazenar o mínimo necessário de informações para a realização de suas finalidades. Ou seja, deverá se coletar apenas dados necessários e proporcionais às finalidades requeridas do tratamento.

Por sua vez, o Princípio de Transparência de Dados possibilita o direito do titular de obter informações claras e atualizadas sobre o tratamento de dados, além de garantir o livre acesso aos agentes de tratamento, o que proporciona os direitos de retificação e revogação desses dados. Com base nesse princípio pode-se dizer que o compartilhamento de dados não pode ser oculto, ou seja, depende da obtenção de consentimento prévio e preciso.

O princípio da Segurança denota a necessidade de assegurar normas protetoras que possibilitem um tratamento de dados que seja compatível com os direitos dos titulares de dados, evitando um tratamento irregular, assim como a prevenção de riscos inerentes à atividade (MIRAGEM, 2016, p.12). Deve haver, portanto, a utilização de medidas de segurança e de boas práticas (*compliance*), que estão, por sua vez, definidas ao longo do capítulo VII da LGPD.

Quanto a aplicação do princípio de prevenção no tratamento de dados pessoais, os agentes de tratamento têm o dever de atuar de forma cuidadosa e preventiva, minimizando o máximo possível os riscos de violação dos dados pessoais, que possam acarretar danos à privacidade dos titulares de dados.

Por último, há o princípio de Responsabilização e Prestação de Contas. É importante que os agentes de tratamento comprovem a eficácia das medidas preventivas adotadas, a fim de demonstrar a boa-fé negocial. Caso haja, por sua vez, eventuais danos aos titulares de dados, estes deverão ser indenizados, com base na assunção da responsabilidade dos agentes de tratamento.

Acerca desse princípio, indica Flumignan e Flumignan (2020, pág. 138):

> Percebe-se, assim, que quem efetuar o tratamento de dados pessoais deverá prestar contas, demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados, bem como efetuar o tratamento em consonância com o consentimento dado pelo titular, sob pena de responsabilização caso haja algum dano decorrente de sua atuação

Por conseguinte, a partir do direito fundamental de privacidade, presente na Carta Cidadã, e reiterado na Lei Geral de Proteção de Dados, é possível garantir ao titular de dados um espaço de privacidade frente ao que pode ser denominado de “Big Data”, onde há, pelas pessoas jurídicas privadas, o uso de dados pessoais de forma irrestrita, importando em muitas situações na invasão da privacidade dos titulares de dados.

3. RESPONSABILIDADE CIVIL OBJETIVA NO CÓDIGO CONSUMERISTA E NA LEI GERAL DE PROTEÇÃO DE DADOS

A responsabilidade civil será verificada a partir dos elementos que a constituem, enfatizando a responsabilização em que se presume a culpa. Destaca-se a responsabilidade civil objetiva solidária presente no Código Consumerista, na hipótese de falha de prestação de serviços. A partir disso se estabelecem paralelos, por meio da técnica de diálogo das fontes, entre o Código Consumerista e a Lei Geral de Proteção de Dados, explicitando-se a adequação e a necessidade de se aplicar a responsabilização civil objetiva e solidária no âmbito da legislação de proteção de dados, a partir do que se dispõe entre os artigos 42 e 45 dessa Lei.

3.1 Noções Gerais de Responsabilidade Civil Objetiva

Antes de evidenciar as interfaces (similitudes e diferenças) entre a responsabilidade acarretada pela prática de ato ilícito (art. 186 CC) ou abuso de direito (art.187 CC) que ocasionam a violação do direito de privacidade dos consumidores/titulares de dados, é necessário buscar definir o que se entende por responsabilidade civil, especificamente a objetiva, onde há presunção de culpa. A responsabilidade civil surge em face do descumprimento de uma obrigação, pela desconformidade com uma regra contratual, ou por um indivíduo ter deixado de observar um preceito normativo que regula a vida (TARTUCE, 2018, p.313).

Por sua vez, a responsabilidade civil objetiva está atrelada a uma responsabilização que independe da prova de culpa de um sujeito, mas depende do surgimento do dano e da observância do nexo causal entre a conduta ilícita do sujeito (ou exercício irregular do direito) e o dano, que resulta da violação do direito de alguém. Importante destacar que a responsabilidade civil, de forma geral, depende da prova do dano, o que possibilita o surgimento do dever de reparação daquele que comete a conduta/ato ilícito (art. 927 do Código Civil).

A reponsabilidade civil objetiva decorre de uma necessidade sócio histórica de se responsabilizar um agente que desenvolve uma atividade que gera riscos a toda a coletividade, algo que portanto está de acordo com a função social dos contratos e da constitucionalização do Direito Civil, que leva em conta princípios como o de isonomia (art. 5°, *caput*, da Constituição Federal) e o de dignidade humana (art. 1°, inciso III, CF). Necessário, portanto, destacar um dispositivo do Código Civil:

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

Deve-se destacar que a responsabilidade civil objetiva, de acordo com a análise do parágrafo único do art. 927 do Código Civil, surge da ideia do risco de atividade de alguém (o risco-proveito do empreendedor, como no caso do fornecedor de bens de consumo). O risco é algo que deve ser suportado por aquele que desenvolve a atividade com ânimo lucrativo, sendo que o prejuízo gerado a outra parte deve ser reparado, já que o risco é inerente. As atividades desenvolvidas que, por sua natureza, acarretem riscos aos terceiros, geram o dever de reparar

os danos dela advindos, sem a necessidade de comprovação de culpa por parte do autor do ato (WOLKOFF, 2010, p.16).

3.2 A responsabilização pela má-prestação de serviços no Código Consumerista

A responsabilidade civil objetiva está presente no Código Consumerista, inclusive com a finalidade de garantir a isonomia entre os fornecedores e consumidores, devido a desigualdade fática, econômica e informacional existentes entre as partes. Pode-se afirmar que:

> O art. 6°, VI, da Lei 8078/1990 consagra o princípio de reparação integral de danos, pelo qual tem direito o consumidor ao ressarcimento integral pelos prejuízos materiais, morais e estéticos causados pelo fornecimento de produtos, prestação de serviços ou má-informação a eles relacionados [...] (TARTUCE, 2018, p. 532).

O artigo 14 do Código Consumerista, ao lado do art. 12 da mesma Lei, definem a responsabilidade por fato do produto ou do serviço, que é uma responsabilidade objetiva e solidária dos fornecedores (exceto os profissionais liberais, em que a responsabilidade depende de prova de culpa). Destaca-se o art. 14 do Código de Defesa do Consumidor:

> **Art. 14**. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
>
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
>
> I - o modo de seu fornecimento;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;
>
> III - a época em que foi fornecido.
>
> § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.
>
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
>
> I - que, tendo prestado o serviço, o defeito inexiste;
>
> II - a culpa exclusiva do consumidor ou de terceiros.
>
> § 4° A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.

A responsabilidade por fato de serviço surge, portanto, da infringência, pelo fornecedor, do dever de segurança em relação ao serviço que este fornece. Difere da responsabilidade por vício do serviço, a qual está relacionada com uma inadequação do serviço em si, por este ser não corresponder à legítima expectativa do consumidor quanto à sua utilização. Quanto ao fato de serviço, esse ultrapassa, portanto, a inadequação do serviço, tendo um potencial de maximizar riscos à sua incolumidade ou de terceiros.

Com relação à responsabilização pelo fato do serviço, o fornecedor deve suportar o risco (risco-criado ou riscos que razoavelmente se esperam), surgindo o dever de reparação quando o consumidor tem violado sua expectativa de fruir o serviço de forma integral. Essa responsabilidade apenas será excluída nas hipóteses do parágrafo 3° do art. 14 do Código Consumerista, em que o fornecedor de serviços prova, por meio de seu conjunto de conhecimentos técnicos e informacionais, que os defeitos são inexistentes, ou, que se presentes, surgiram devido a fatos supervenientes, devido a culpa exclusiva (não concorrente) do consumidor ou de terceiros.

Caso haja a possibilidade se o serviço apresentar uma nocividade/risco maior ao consumidor, deve ser lhe garantido, pelo fornecedor, a proteção da vida, saúde e segurança (art. 6°, inciso I do Código Consumerista). Por sua vez, é possível que os danos causados pelos defeitos dos serviços afetam terceiros, os quais são partes legítimas para ingressar com ação de reparação de danos, como se entende a partir do art. 17 do CDC, o qual equipara aos consumidores todas as vítimas do evento danoso (COSTA, 2007, p. 15). Aqui está presente a necessária tutela de direitos difusos e coletivos dos consumidores (art. 6°, inciso VI, Código Consumerista), havendo a necessidade de prevenção e reparação em relação a acidentes de consumo, que podem gerar danos com múltiplas vítimas.

Em relação ao dever de informação por parte do fornecedor, pode-se dizer que é um núcleo essencial à proteção da boa-fé objetiva, além de possibilitar uma maior harmonização da relação de consumo (princípio do equilíbrio contratual), considerando a vulnerabilidade ínsita do consumidor. As informações devem ser prestadas com veracidade, clareza e adequação à finalidade de esclarecer o consumidor. De acordo com Miragem (2016, p.216):

> [...] Em uma relação contratual, o conteúdo da informação adequada deve abranger essencialmente: a) as condições da contratação; b) as características dos produtos ou serviços objetos da relação de consumo; c) eventuais consequências e riscos da contratação. Na ausência de contrato, o dever de informar assume caráter mais difuso, mas nem por isso menos preciso.

Evidencia-se, por conseguinte, um dever de informação por parte do fornecedor, constituindo-se um direito subjetivo do consumidor, o que efetivamente se coaduna com o princípio da boa-fé objetiva aplicada nas relações contratuais (associada aos deveres anexos de lealdade, probidade e transparência). Isso possibilita a proteção da confiança dos consumidores dentro de uma relação caracterizada pela vulnerabilidade desse, o que é essencial para haver a proteção dos direitos da personalidade humana, realçando a importância da aplicação do princípio da dignidade humana.

A fim de que o consumidor tenha o que se denomina de consentimento esclarecido, é imprescindível que haja a aplicação do princípio da transparência (art. 4°, *caput,* Código Consumerista), decorrente da boa-fé objetiva, sendo que a relação contratual deve ser estar clara para ambas as partes, o que significa a necessidade de descrição e informação correta sobre o produto ou o serviço a ser prestado (GARCIA, 2020, p. 7). Pode se afirmar ainda que, em decorrência do princípio da informação, o legislador garantiu ao consumidor o direito de ser informado, de maneira ostensiva e adequada, sobre os riscos do produto que esse vai adquirir. Havendo falha na informação dirigida ao consumidor, o produto/serviço será considerado defeituoso e, se causar qualquer tipo de dano ao consumidor, poderá ser pleiteado indenização frente ao fornecedor (GARCIA, 2020, p. 11).

Constata-se, portanto, que o dever de informação está associado a prevenção de danos individuais, coletivos ou difusos que possam surgir dos defeitos dos produtos ou serviços. A prevenção não surge a penas para evitar a realização de danos, mas para possibilitar a adoção de medidas que desestimulem efetivamente a ofensa dos direitos consumeristas pelos fornecedores, dando exemplo inclusive aos demais agentes econômicos para que não reproduzam tal comportamento (MIRAGEM, 2016, p.222).

As informações prestadas pelo fornecedor, no ato da oferta/proposta, vinculam esse a oferta que for veiculada ao consumidor, além de integrar o contrato que vier a ser estabelecido (art. 30 do Código Consumerista). O artigo 35 da mesma Lei apresentam as consequências da violação do dever de informar por parte do fornecedor, sendo que a rescisão contratual gerará automaticamente perdas e danos.

> Art. 35 Se o fornecedor de produtos ou serviços recusar cumprimento à oferta, apresentação ou publicidade, o consumidor poderá, alternativamente e à sua livre escolha:
>
> I - exigir o cumprimento forçado da obrigação, nos termos da oferta, apresentação ou publicidade;

> II - aceitar outro produto ou prestação de serviço equivalente;
>
> III - rescindir o contrato, com direito à restituição de quantia eventualmente antecipada, monetariamente atualizada, e a perdas e danos.

Além do mais, em relação ao contrato fornecido ao consumidor (caracterizado vai de regra como um contrato de adesão), haverá a ineficácia das disposições contratuais que não forem adequadamente informadas (art. 46 do Código Consumerista), o que possibilitará a resolução do contrato ou até a sua manutenção. Inclusive o defeito informacional poderá acarretar o surgimento de uma cláusula abusiva no contrato, o que implicará na sua nulidade (art. 54 do Código Consumerista). Hodiernamente é muito comum o uso de contratos de adesão no comércio eletrônico, pois o consumidor a partir de um clique (consentimento) aceita os termos contratuais estabelecidos pelo fornecedor. Caso o fornecedor não cumprir o seu dever de informação, especificando de forma clara as cláusulas contratuais, não há possibilidade de o consumidor dar o seu consentimento livre e motivado.

O direito à facilitação à defesa é essencial na relação consumerista, pois essa está calcada na desigualdade informacional, técnica e econômica entre as partes, inclusive dentro do contexto de defesa de suas pretensões, pois os fornecedores dispõem de mais recursos financeiros para defenderem seus interesses. Por conseguinte, é muito importante que o ônus da prova não seja um dever concentrado nas mãos do consumidor, o que denota a importância da inversão do ônus da prova na relação consumerista, pois está fortalece consideravelmente o acesso à justiça por parte do consumidor. A inversão do ônus da prova, por sua vez, está condicionada, à verificação pelo juiz, da hipossuficiência do consumidor ou da verossimilhança das alegações (art. 6°, VIII, do Código de Defesa do Consumidor).

Há a existência de requisitos não-cumulativos para que o Juiz, em cada caso concreto, reconheça ou não a existência do direito à inversão do ônus da prova ao consumidor. Em relação ao requisito da hipossuficiência, pode-se dizer que esta, diferentemente da vulnerabilidade, que é reconhecida a todo consumidor, pode ser enunciada como uma circunstância concreta, de desigualdade cm relação à outra parte, e que no processo se revela pela falta de condições econômicas da defesa, a fim de demonstrar e provar adequadamente a sua pretensão (MIRAGEM, 2016, p. 229).

3.3 A responsabilização dos agentes de tratamento por meio da aplicação da Lei Geral de Prestação de Dados

Ao analisar a Lei Geral de Proteção de Dados, pode-se notar certas interfaces com relação ao Código Consumerista, como em relação à aplicação de princípios constitucionais ao reconhecimento da situação de vulnerabilidade do consumidor de dados na Sociedade Informacional e também, destaca-se, em relação ao regime de responsabilidade civil objetiva e solidária. Deve-se frisar que há também entendimento pela responsabilidade subjetiva quando do vazamento de dados pessoais.

Na análise da responsabilidade dos agentes de tratamento em relação aos dados pessoais dos titulares de dados, deve-se levar em conta que a atividade de tratamento e processamento de dados tem como característica inerente o risco, já que se forem feitas de forma irregular (contra os preceitos descritos na Lei Geral de Proteção de Dados), podem acarretar vazamentos de dados dos titulares de dados. Existe noção, portanto, de quem devem aplicadas uma série de boas práticas de tratamento a fim de garantir a segurança de dados (art. 50 da Lei Geral de Proteção de Dados), evitando assim, incidentes de seguranças.

Deve-se destacar que, na atividade de tratamento de dados pessoais, é necessário a aplicação dos princípios elencados no art. 6°, a fim de manter a transparência e o equilíbrio contratual entre o controlador/operador de dados (fornecedor) e o titular de dados (consumidor), o que, de fato possibilita minimizar o risco-atividade (risco-proveito) dessa atividade cada vez mais predominante na Sociedade Informacional. Deve haver, portanto, por parte dos agentes de tratamento de dados, legítimo interesse vinculado ao exercício de finalidades legítimas, que se dá, na maior parte dos casos, com a presença de consentimento por parte dos titulares de dados.

Pode-se dizer que aquele que realiza o procedimento relacionado ao tratamento de dados tem o dever de definir em termos claros e precisos a participação e a localização dos dados pessoais, a fim de que o titular, em dadas situações de litígios judiciais (envolvendo danos morais e materiais), consiga definir exatamente onde ocorreu o tratamento indevido de seus dados pessoais (DIVINO; LIMA,2020, p. 12).

Em relação à responsabilidade civil ocorrida devida ao tratamento irregular de dados, deve-se aplicar o princípio da reparação integral de danos (art. 6°, VII, Código Consumerista), realizando um importante diálogo de fontes com o Código Consumerista, a fim de salvaguardar o direito de privacidade dos titulares de dados. Pode-se afirmar que:

> {...} o controlador ou o operador que, em razão do exercício da atividade de tratamento de dados, causar ao titular dos dados, dano moral, individual ou coletivo, violando o GPDR brasileiro, será obrigado a repará-lo. Neste prisma a legislação brasileira reconhece a possibilidade da existência de danos coletivos pelos atos ilícitos causados pelo controlador ou operador. Exemplifica-se como o vazamento de dados pessoais que deveriam ser tutelados por instituições financeiras (DIVINO; LIMA, 2020, p. 14).

A aproximação entre a Lei Geral de Proteção de Dados e o Código Consumerista é evidenciado no rol dos direitos do titular de dados, que ao peticionar aos agentes de tratamento, a fim de ter acesso aos dados (confirmação da existência de tratamento de dados, retificação de dados desatualizados, anonimização, bloqueio e eliminação de dados tratados em desconformidade com a legislação de proteção de dados, etc.), pode exercer esses direitos perante os organismos de defesa do consumidor (art. 18, § 8° da Lei Geral de Proteção de Dados).

Em relação à responsabilidade civil na Lei Geral de Proteção de Dados, é importante ressaltar que as normas dessa Lei não serão necessariamente aplicadas em todos os casos que envolvam responsabilização civil, podendo, a depender da relação jurídica apresentada, ceder espaço a normas específicas, como o CDC, o que, inclusive, é expressamente reconhecido pela Lei Geral de Proteção de Dados em seu art. 45 (CAPANEMA, 2020, p. 2).

O art. 42 da Lei Geral de Proteção de Dados pode ser definido como uma cláusula geral da responsabilidade civil, onde os titulares de dados deverão ser reparados (tutela individual ou coletiva) por danos morais e materiais que surjam devido ao tratamento de dados, que esteja em desconformidade com esta Lei. Essas ocorrem quando os controladores e operadores (agentes de tratamento), por meio de suas atividades, violarem as normas e princípios dessa Lei, que pode ocorrer, por exemplo, quando o consentimento do titular de dados, mesmo que livre e informado, não esteja relacionado a alguma finalidade específica (art. 8°, § 4° da Lei n° 13.708/2018).

A fim de se assegurar ao titular de dados uma efetiva indenização, deverá o operador responder de forma solidária pelos danos causados pelo tratamento, quando agir de forma contrária ao que está disposto na Lei 13.709/2018 ou quando não seguir corretamente as instruções do controlador, desde que essas sejam lícitas. As hipóteses de solidariedade elencadas no art. 42, § 1° da Lei supracitada estarão apenas afastadas quando presentes as hipóteses de exclusão de responsabilidade (art.43 da Lei Geral de Proteção de Dados).

A Lei Geral de Proteção de Dados não elenca a responsabilidade civil do encarregado, que poderá surgir, no entanto, caso essa função for exercida por pessoa natural ou jurídica do controlador e do operador em uma relação consumerista. Neste caso, por haver a presença de uma cadeia de produção, o encarregado poderá ser responsabilizado de forma solidária pelo dano causado (CAPANEMA, 2020, p.4).

Há a presença, dentro do espectro da responsabilidade civil (extracontratual), do direito de inversão do ônus da prova, a partir de critérios similares com os presentes no Código Consumerista. Há a presença de requisitos alternativos, que são: verossimilhança das alegações, existência da hipossuficiência (uso do critério jurídico/probatório e não econômico) e existência de situações em que a produção da prova seja muito onerosa ao titular de dados (art.42, § 3°, Lei Geral de Proteção de Dados).

O parágrafo 2° do mesmo artigo indica a possibilidade de reparação de danos coletivos ou difusos, por meio da aplicação da tutela coletiva, evidenciando a aplicação do microssistema consumerista, quando envolvem direitos difusos, coletivos e individuais homogêneos. Caso se verifique danos a interesses sociais e individuais indisponíveis, é conveniente e necessário o ingresso do Ministério Público como agente de defesa da ordem jurídica (DIVINO; LIMA, 2020, p.15).

É importante ressaltar a possibilidade de direito de regresso de um dos operadores ou controladores de dados que indenizaram o dano ao titular de dados. Quanto ao direito de regresso (sub-rogação) pode-se dizer:

> (...) se verificada uma culpa pequena ou mínima diante de um extenso dano cometido por um concurso de agentes, aquele que vier a compensar ou reparar o dano deverá agir em regresso aos demais na medida de sua culpabilidade. Portanto, entende-se que deve analisar os graus de culpa (se leve, média, grave ou gravíssima) dos agentes envolvidos (DIVINO e DE LIMA, 2020, p.15).

Em relação ao tipo de responsabilidade civil dos agentes privados (fornecedores) existente na Lei Geral de Proteção de Dados, essa deve ser objetiva, pois uma legislação protetiva dessa importância não pode renegar a evolução no âmbito da responsabilidade civil numa sociedade massificada, em que os riscos produzidos pelos agentes privados/fornecedores são socializados pelos cidadãos, os quais precisam ter os seus direitos fundamentais tutelados contra a crescente de riscos nas atividades cada vez mais informatizadas. Destaque-se que há posições dissonantes que advogam pela aplicação da responsabilidade civil subjetiva, no âmbito da legislação de proteção de dados.

Antes mesmo da configuração da tecnologia da internet, que pode ser denominada de 4° Revolução industrial, havia a aplicação da responsabilização objetiva e solidária no âmbito das relações de consumo. Portanto, aplicar ao sistema de proteção de dados pessoais a responsabilização civil subjetiva iria configurar um contexto que apenas maximizaria as lesões aos direitos de personalidade.

O art. 43 da Lei Geral de Proteção de Dados evidencia uma série de hipóteses em que haverá exclusão de responsabilidade, não geradas pela ausência de riscos por parte das atividades dos agentes de tratamento (o que é inclusive impossível, mesmo com a adoção de medidas preventivas que salvaguardem a segurança das atividades de tratamento), mas sim por situações em que os controladores e operadores confirmem não ter envolvimento com o tratamento de determinados dados pessoais que foram violados/vazados (inciso I), em contextos onde se configure culpa exclusiva da vítima e de terceiros, como na disponibilização pela vítima de uma senha para um terceiro (inciso III) ou ainda quando houver vazamento/violação de dados, mas não houver, por parte dos agentes de tratamento, violação à legislação da proteção de dados (inciso II).

Quanto ao art. 44, trata-se da definição do que denomina de tratamento irregular de dados, que pode ser definida como uma cláusula aberta que traz duas situações de antijuridicidade, que são a desconformidade com a legislação de proteção de dados e a não observância de deveres de segurança. Veja-se:

> 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.

Verifica-se, a partir do art. 44 supracitado, a necessidade de responsabilização objetiva dos agentes de tratamento por atos ilícitos (que envolve remoção do ato ilícito e indenização ao titular de dados) quando esses não observarem os deveres inerentes de segurança (art. 46 da Lei Geral de Proteção de Dados), não adotando as medidas protetivas que mitiguem

com a maior eficácia possível os incidentes de segurança, como no caso de vazamentos de dados pessoais. Observa-se que deve haver um parâmetro de razoabilidade, pois para se definir se há ou não inobservância dos deveres de segurança deve-se atentar a resultados e riscos razoavelmente esperados, além do modo utilizado para tratar os dados pessoais. A partir disso, pode-se dizer havendo a correta utilização de técnicas adotadas exige-se um peso maior nos outros critérios postos para verificar a violação aos deveres de segurança.

Considerando-se o tratamento irregular de danos (art. 44 da Lei Geral de Proteção de Dados) pode-se dizer que:

> Caso o serviço esteja irregular (no termo da LGPD) porque dissonante dos critérios dos três incisos, o dano decorrente da mera prestação será indenizável pelo agente de tratamento. Nesse caso, o dever de indenizar não terá origem em anomalia do tratamento de dados, mas em violação dos parâmetros de segurança razoável dispostos em lei (OLIVEIRA, 2020, p.7).

Logo, o direito de reparação do titular está atrelado a uma falha no serviço prestado pelos agentes de tratamento. Havendo um desvio quanto à expectativa legítima do titular de dados, em decorrência da inobservância de parâmetros de segurança, surgirá para os agentes de tratamento o dever de reparação.

4. OS DANOS MORAIS *IN RE IPSA* NO CONTEXTO DE VAZAMENTO DE DADOS

A análise dar-se-á, neste capítulo, pela definição de danos morais, as espécies de lesão extrapatrimonial e a forma como esses são quantificados em cada caso concreto, devido a característica de subjetividade. Após isso, conceituar-se-á o vazamento de dados e de que forma esse resulta em danos ao direito fundamental de privacidade do titular de dados. Por fim analisar-se-ão decisões judiciais do Tribunal de Justiça de São Paulo, expondo três das seis decisões analisadas no período de 2020/2021, referentes à aplicação de dano moral.

4.1 Os danos morais e suas espécies

Antes de discorrer sobre os vazamentos de dados e os danos morais que possam surgir neste contexto é necessário definir o que são os danos morais. Deve se ressaltar que estes se dão no contexto de responsabilização civil (art. 927 do Código Civil) e possuem autonomia

frente aos danos materiais, importante conquista que se deu a partir da Constituição Federal, a partir da leitura do art. 5°:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> (...)
>
> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;

Sem dúvida, é necessária a independência do dano extrapatrimonial em relação ao dano patrimonial, pois este último reflete nas consequências quando há a perda de patrimônio, relativo a danos emergentes e lucros cessantes. Já no dano moral (que pode ser direto ou indireto; individual ou coletivo) há um reflexo direto no "patrimônio moral" do indivíduo, pois surge a partir de lesões ao direito de personalidade, como os de direito à imagem, privacidade, honra, etc. O dano moral pode ser evidenciado quando há uma lesão a dimensão psicológica (abalo psicológico e não meramente dissabor cotidiano), à imagem do indivíduo no meio social, constrangimento moral, o que pode levar à depressão e a outros problemas de cunho emocional.

A fim de garantir da tutela da personalidade, não é possível nem desejável haver a constituição de um rol exaustivo de danos morais através da repercussão desses na esfera íntima, psíquica e física, dos indivíduos. Busca-se reparar esses danos a personalidade (liberdade, intimidade, honra, decoro etc.) através de tutelas preventivas e específicas (obrigações de fazer e de não fazer) necessárias para proteção dos direitos da personalidade, almejando impedir a consumação do dano moral, desfazendo ou mitigando o resultado advindo da conduta ilícita e evitando o agravamento e a reiteração desses danos morais (MONTEIRO FILHO; ZANETTA,2016, p. 10).

A fim de se garantir a reparação do dano moral, é necessário verificar que o desfalque de patrimônio que vai se gerar ao ofensor possui a função punitiva/sancionadora, além da função compensatória, a fim de minimizar os danos afligidos à esfera íntima do ofendido. É evidente que a reparação do dano moral não tem como consequência o retorno à situação anterior (*status quo ante)*, mas possibilita uma compensação pecuniária à vítima ou mesmo a família, no caso de um dano moral indireto (ou em ricochete).

Os danos morais são fundamentados a partir da lesão aos bens jurídicos associados à dignidade da pessoa humana (direito constitucional subjetivo, essência de todos os direitos personalíssimos), e não a partir das consequências psíquicas e afetivas do dano, que são a dor e o padecimento. Pode-se dizer que:

> Em sentido impróprio, o dano moral constitui qualquer lesão aos direitos da personalidade, como, por exemplo, à liberdade, à opção sexual, à opção religiosa, entre outros. Trata-se do dano moral em sentido amplo ou *latu sensu*, que não necessita de prova de sofrimento em si para a sua caracterização(...) (TARTUCE, 2018, p.420).

Em relação à fixação de danos morais, a maioria dos entendimentos doutrinários e jurisprudenciais advogam pelo método bifásico de fixação de indenização. Com base nisto, a fim de se alcançar o valor adequado a cada caso, deve-se na primeira fase arbitrar um valor básico, de acordo com a jurisprudência sobre o evento danoso (valores comumente arbitrados), e por sua vez, na segunda fase, alcança-se o *quantum* definitivo, ajustando-se o valor básico alcançado na primeira fase às peculiaridades do caso concreto, em que são relevadas a gravidade do ato em si (a extensão do dano), a responsabilidade do agente, a culpa concorrente da vítima, além das condições socioeconômicas e socioculturais das partes (COSTA, 2007).

Em relação a estipulação/arbitramento do valor do dano moral, destaca-se que que os critérios estipulados na segunda fase de fixação do *quantum* do dano moral estão relacionadas aos artigos 944 e 945 do Código Civil. Em relação ao primeiro esse estabelece que a indenização, proporcional à extensão do dano, terá uma redução equitativa em relação ao seu valor, caso se mostre desproporcional o grau de culpa em relação ao dano sofrido pela vítima. O artigo 45 do Código Civil estabelece, por usa vez, a culpa concorrente, em que a havendo um grau de culpa também por parte da vítima, essa será levado em conta para a fixação da indenização, que terá parte de seu ônus também suportado pela vítima. Veja-se:

> Art. 945. Se a vítima tiver concorrido culposamente para o evento danoso, a sua indenização será fixada tendo-se em conta a gravidade de sua culpa em confronto com a do autor do dano.

Destaque-se que há o dano moral em que é necessário se provar, pelo autor da demanda, a existência de dano. Esse é denominado de dano moral subjetivo, enquanto o dano moral

subjetivo/presumido, também nomeado de dano moral *in re ipsa*, se refere àquele em que não é necessária a comprovação do dano, pois este é presumido.

Quanto ao dano moral *in re ipsa*, esse se configura em situações, já pacificados pela jurisprudência como protesto indevido de títulos, envio de nome de pessoa natural ou jurídica a cadastro de inadimplentes, perda de órgão ou parte do corpo e uso indevido de imagem. Afirma Tartuce (p. 421) que "ultimamente, a tendência jurisprudencial é de ampliar os casos envolvendo a desnecessidade de prova de dano moral, diante do princípio de proteção da dignidade da pessoa humana (...)".

Há danos morais que não são necessariamente individuais, pois atingem a esfera íntima de todo uma coletividade, determinada ou não, gerando lesões ao mesmo tempo a vários direitos da personalidade. Há portanto, uma tutela coletiva aos danos morais coletivos, podendo haver a aplicação do Código de Defesa do Consumidor e da Lei da Ação Pública. Importante assentar que não é mais razoável a configuração de danos morais considerando apenas os indivíduos em si, pois não são os únicos a sofrerem abalos morais, pois os prejuízos à imagem e moral coletivas geram danos muito expressivos na coletividade. Por conseguinte o dano extrapatrimonial coletivo pode ser aferido independentemente da prova de dor ou abalo psicológico sofridos pelos indivíduos.

4.2 Violação de dados sigilosos

Em relação ao vazamento de dados (violação de dados pessoais), este é conceituado como incidente de segurança. São incidentes que que se multiplicam cada vez mais, apesar do novo paradigma de adoção de boas práticas (práticas para garantir a segurança da informação) pelas empresas, podendo ser incidentes acidentais ou intencionais, que por sua vez, demonstram fragilidade do sistema de computadores. Segundo Freitas (2020, p.12) pode-se afirmar que:

> A violação de dados – também conhecida como vazamento de dados, vazamento de informações, perda de dados ou derrame de dados – é um incidente de segurança onde dados contendo todo tipo de informações confidenciais é visto, roubado ou utilizado por terceiros não autorizados. Como já afirmado a violação de dados poderá ocorrer de forma acidental ou intencional, interna ou externamente às empresas, e deverá ser apurado por meio de ferramentas, processos e treinamentos; constatando-se, na apuração, que houve violação ou vazamento intencional, o incidente será tratado como fraude

Hodiernamente estão sendo anunciados na mídia uma série de megavazamentos de dados, que expõem a identidade de muitos usuários. Nesse ano de 2021, pacotes de dados com informações pessoais de mais de 223 milhões de brasileiros foram vazados, com a finalidade de serem vendidos por criminosos. Há muitas ameaças em relação à segurança dos dados pessoais, devido a invasões de terceiros não-autorizados a banco de dados, o que evidencia que as empresas não estão adotando medidas preventivas suficientes e que o Estado não está conseguindo tutelar os direitos fundamentais, através de uma fiscalização eficiente.

Com o advento da Lei Geral de Proteção de Dados, passou-se do nível de proteção de dados por meio de autorregulamentação das empresas para um regulamento específico, que destacou a necessidade de se garantir a proteção de dados pessoais, a partir de um tratamento de dados que esteja conforme aos direitos dos usuários e aos princípios elencados pela legislação de proteção de dados. É necessário, portanto, que as empresas se adequem à normativa de proteção de dados, por meio de uma atuação preventiva (compliance), que permita que os agentes de tratamento tenham conhecimento sobre os fluxos de dados, a fim de os gerenciá-los e garantir que o tratamento desses dados pessoais esteja em conformidade com a legislação de proteção de dados.

É importante, por meio de políticas de privacidade (de governança, adoção de boas práticas) que as empresas adotem uma cultura organizacional que se adeque às finalidades legítimas dos tratamentos de dados, gerenciando os riscos que possam gerar incidentes de segurança, e que possibilitem que haja uma devida prestação de contas dos fluxos de dados que estão sendo tratados.

A Lei Geral de Proteção de Dados prevê a necessidade de criação de mecanismos capazes a aptos com o fito de demonstrar a preocupação dos agentes de tratamento de dados com a adoção de medidas adequadas para tratar os dados em seu poder. A adoção reiterada e demonstrada de mecanismos e procedimentos internos aptos a minimizar o dano e seus efeitos adversos, voltados ao tratamento de segurança de dados, a adoção de políticas de governança e a pronta adoção de medidas corretivas devem ser levadas em consideração na definição e aplicação de sanções às empresas (LOPES; CEZARINO, 2021).

Analisando-se o art. 50 da Lei Geral de Proteção de Dados, vê-se a necessidade da adoção de boas práticas, com a finalidade de garantir medidas de segurança, padrões técnicos de qualidade, obrigações específicas para os diversos envolvidos no tratamento, além de garantir a comunicação dos agentes de tratamento de dados com os titulares, através de petições

e reclamações. Os agentes de tratamento deverão levar em conta, ao estabelecer regras de governança, a natureza, finalidade, benefícios advindos do tratamento de dados do titular, além da análise da probabilidade e da gravidade dos riscos.

Importante destacar que havendo compartilhamento de dados a terceiros ou alterações quanto à forma, duração e finalidade ou acerca de informações em relação ao uso compartilhado dos dados pelo controlador (art.9° da Lei Geral de Proteção de Dados), deverá o controlador informar de forma adequada e eficiente os titulares de dados acerca desses novos usos de dados. Inclusive, de acordo com o art. 9° da Lei supracitada, caso houver essas alterações quanto a natureza e finalidade dos dados, poderá o titular de dados revogar o seu consentimento anterior, tendo como consequência o término do tratamento de dados, que deverá resultar na eliminação de dados.

Além da adoção dessas medidas preventivas é necessário destacar as medidas de reparação e prestação de contas quando ocorre a violação dos dados sigilosos dos usuários/titulares de dados. Os agentes de dados precisam ser efetivamente transparentes quando há a ocorrência de um incidente de segurança, que possa gerar risco ou dano relevante aos titulares de dados. Veja-se:

> 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.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.

> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Constata-se que havendo a ocorrência de incidente de segurança, a comunicação feita pelos controladores e operadores de dados deve ser imediata e feita de forma eficiente. Os destinatários dessa comunicação serão os titulares de dados e a Autoridade Nacional de Proteção de Dados. Essa tem a função primordial de criação de regulamentos a partir da Lei Geral de Proteção de Dados, fiscalização das atividades de tratamento realizadas pelas empresas privadas e públicas, aplicação de sanções quando ocorrerem tratamentos indevidos, promoção da conscientização da população acerca da necessidade de proteção dos dados pessoais, entre outras. A Autoridade Nacional de Proteção de Dados não deve apenas as funções de zelar e ser símbolo da privacidade e proteção dos dados pessoais, mas também atuar ativamente na regulamentação e fiscalização relativas à lei (MACIEL; GUEIROS, 2021).

A fim de haver a reversão ou mitigação dos danos provocados pelos incidentes de segurança aos titulares de dados, é necessário que se informe a natureza dos dados, os titulares envolvidos, riscos atrelados ao incidente de segurança, medidas técnicas e de segurança adotadas pra coibir os vazamentos de dados. Ademais devem estar expressas as medidas que devem ser adotadas pelos agentes de tratamento para reverter ou mitigar os danos à privacidade dos titulares de dados. Caso a Autoridade Nacional de Proteção de Dados entenda que não houve um correto procedimento para minimizar ou neutralizar os efeitos deletérios dos incidentes de segurança, haverá a aplicação das sanções administrativas expressas no artigo 52 da legislação de proteção de dados.

Em relação a essas sanções administrativas, essas vão desde advertência, aplicação de multa simples (que pode chegar até 2% do faturamento da pessoa jurídica de direito privado) ou diária, até penas mais severas, como eliminação de dados pessoais a que se refere infração, chegando até a proibição parcial ou total da pessoa jurídica de exercer atividades de tratamento de dados

A fim de minimizar a quantidade de incidentes de segurança e de evitar a aplicação de sanções administrativas, as empresas devem empregar uma série de medidas preventivas e de prestações de conta, a fim de evitar o máximo possível o vazamento de dados. Caso esses ocorram as medidas empregadas para comunicar a ocorrência ao titular e, para reverter ou

mitigar a violação aos dados pessoais, devem ser céleres e adequadas com o fim consignado, a fim de efetivar a tutela do direito de privacidade do titular de dados.

Da ocorrência de vazamento de dados, podem surgir danos materiais, levando prejuízos ao patrimônio do ofendido, assim como danos morais, pois há a ocorrência de lesão a direitos de personalidade devido a prática de atos ilícitos pelos agentes de tratamento. Esses por sua vez, muitas vezes não agem em conformidade com a Lei, não adotando as técnicas e medidas de segurança adequadas e atualizadas, o que facilita o acesso não autorizado de terceiros (prática comum dos hackers) a esses dados, que muitas vezem usurpam esses dados a fim de cometer fraudes contra os titulares de dados.

Os usuários de dados precisam ter muita precaução com o uso de seus dados, sendo que inclusive a culpa exclusiva da vítima exclui a responsabilidade dos agentes de tratamento. No entanto os agentes de tratamento devem suportar os riscos da atividade desenvolvida, e por isso, devem adotar todas as medidas possíveis, a fim de não serem responsabilizados, o que independe da verificação da culpa. Caso se verifique que esses cederam o uso dos dados do titular de dados a terceiros sem consentimento específico daquele, e havendo o vazamento de dados, é possível que surjam danos materiais e morais, além, é claro, da aplicação de sanções administrativas.

Na hipótese de vazamento de dados, a responsabilização civil objetiva solidária dos agentes de tratamento depende de fatores como a forma como se deu a violação da informação e do tipo de dado vazado. No primeiro caso deve-se analisar se houve, pelo agente de tratamento ou por um preposto desse, um compartilhamento de dados pessoais sem o consentimento específico do titular de dados ou se houve a invasão de um banco de dados por um hacker. Em relação ao tipo de dado vazado, esse pode ser um dado relacionado a identificação pessoal do usuário ou relacionado à etnia, orientação sexual ou religiosa, problema de saúde. Esses são dados sensíveis (art. 5°, inciso II, da Lei Geral de Proteção de dados), os quais se tratados de forma ilícita geram consequências mais graves aos titulares de dados, pois esses dados tem um maior potencial discriminatório, que prejudique seriamente a vida de um indivíduo afetado.

Havendo um dano decorrente de vazamento de dados pessoais passa a ser necessário a sua quantificação, o que é de difícil verificação em abstrato. Portanto, eventuais requerimentos de indenizações de danos materiais e morais terão que cuidadosamente observar as características dos casos concretos e da jurisprudência, aplicando-as a partir de suas funções reparatórias e punitivas (MODESTO; SILVA, 2020).

Ocorrendo um vazamento de dados, e sendo formulado pelo titular de dados vazadas uma ação contra os agentes de tratamento, devem os juízes primeiramente se ater aos pedidos formulados pelo titular de dados, a fim de julgarem ação por meio de uma sentença de mérito de procedência ou improcedência. É possível a aplicação de obrigações de fazer ou não fazer (tutelas mandamentais) e de aplicação de regras de responsabilidade civil nos artigos 42 a 45 da Lei Geral de Proteção de Dados e em outras leis, como o Código Consumerista.

A ocorrência de incidentes de segurança está relacionada, de forma geral, com falhas na prestação de serviços dos agentes de tratamento de dados. É evidenciado que esses devem levar em conta medidas preventivas a fim de minimizarem os riscos de vazamentos de dados e além disso, caso impossível não prevenir os danos aos titulares de dados, esses devem ter a garantia, sob pena de aplicação das sanções administrativas, de serem comunicados em curto prazo, além de terem seus danos revertidos ou, no mínimo, mitigados.

4.3 APLICABILIDADE DOS DANOS MORAIS EM DECISÕES JUDICIAIS

Em relação à aplicação de danos morais no contexto de vazamento de dados, observa-se na jurisprudência recente, a alusão frequente ao Código Consumerista e aos artigos 42 a 45 da legislação de proteção dos dados (tratamento irregular de dados). Além disso há uma clara divisão dos julgados que entendem pela aplicação de danos morais *in re ipsa* e outros que salientam que a reparação por dano moral depende da comprovação de dano ao consumidor.

Essa divisão supracitada se dá porque a Lei Geral de Proteção de Dados não é suficientemente clara acerca da responsabilização dos agentes de tratamento pelo tratamento irregular de dados, como no caso da ocorrência de incidentes de segurança. Apesar do entendimento majoritário acerca da responsabilidade objetiva dos agentes de tratamento, a aplicação ou não de danos morais depende, além da análise das excludentes de responsabilidade, da ponderação, no caso concreto, pela existência ou não de um abalo moral sofrido pelas vítimas, decorrente do vazamento de seus dados pessoais, através do compartilhamento indevido entre banco de dados (terceiros não autorizados), havendo o uso dos dados violados na perpetração de fraudes por terceiros.

Importante haver uma interface entre a legislação da proteção de dados com o Código Consumerista, pois há neste a utilização de tutelas individual e coletiva para a proteção do consumidor, que é vulnerável, além da aplicação da inversão do ônus da prova. Em relação à

aplicação de dano moral presumido nas relações consumeristas pode-se pegar como exemplo a inscrição indevida do nome da pessoa em cadastro de inadimplentes. De acordo com o entendimento do Superior Tribunal de Justiça, a inscrição indevida de dados pessoais em cadastros negativos (cadastros de proteção ao crédito) geram automaticamente danos morais, pois nesse caso se presume o abalo moral sofrido pela vítima.

Em relação ao uso indevido de imagem, sem autorização do titular deve-se aplicar a Súmula 403 do Superior Tribunal de Justiça, consoante a qual "independe de prova de prejuízo a indenização pela publicação não autorizada da imagem de pessoa com fins econômicos ou comerciais". O mesmo Superior Tribunal de Justiça entende pela aplicação do dano moral *in re ipsa* no caso de lesão a valores fundamentais protegidos pela Constituição Federal, devido à aplicação do princípio da dignidade humana. Veja-se:

> DIREITO CIVIL. RECURSO ESPECIAL. AÇÃO DE COMPENSAÇÃO POR DANOS MORAIS. ACIDENTE EM OBRAS DO RODOANEL MÁRIO COVAS. NECESSIDADE DEDESOCUPAÇÃO TEMPORÁRIA DE RESIDÊNCIAS. DANO MORAL IN RE IPSA. 1. Dispensa-se a comprovação de dor e sofrimento, sempre que demonstrada a ocorrência de ofensa injusta à dignidade da pessoa humana. 2. A violação de direitos individuais relacionados à moradia, bem como da legítima expectativa de segurança dos recorrentes, caracteriza dano moral in re ipsa a ser compensado. 3. Por não se enquadrar como excludente de responsabilidade, nos termos do art. 1.519 do CC/16, o estado de necessidade, embora não exclua o dever de indenizar, fundamenta a fixação das indenizações segundo o critério da proporcionalidade. 4. Indenização por danos morais fixada em R$ 500,00 (quinhentos reais) por dia de efetivo afastamento do lar, valor a ser corrigido monetariamente, a contar dessa data, e acrescidos de juros moratórios no percentual de 0,5% (meio por cento) ao mês na vigência do CC/16 e de 1% (um por cento) ao mês na vigência do CC/02, incidentes desde a data do evento danoso. 5. Recurso especial provido. (BRASIL,2012).

Há um claro entendimento pelo Superior Tribunal de Justiça acerca de que os danos morais *in re ipsa* podem se aplicar em situações em que não há relação consumerista, em situações diferentes onde há o descumprimento de valores fundamentais tutelados pela Carta Política. No caso da aplicação da legislação de proteção de dados, segundo esse entendimento, é possível a existência de danos morais presumidos, mesmo não se configurando relação de consumo.

Deve-se constar que as atividades do titular de dados e a de um fornecedor, no caso de uma relação consumerista, estão associadas a noção do risco criado, e portanto, até mesmo o perigo de dano pode configurar dano moral *in re ipsa*. O Superior Tribunal de Justiça possui entendimento recente de que a exposição do consumidora risco concreto de lesão à sua saúde

e segurança (perigo de dano) gera dano moral presumido, havendo a responsabilização sem danos. Note-se que esse entendimento seria dificilmente aplicável na conjuntura de tratamento de dados.

Em um contexto de tratamento irregular de dados, porém, a fim de proteger a privacidade dos titulares de dados, é prejudicial a esse não aplicar o entendimento de danos morais presumidos no caso de compartilhamento de dados a terceiros não autorizados pelo agente de tratamento de dados. Torna-se claro que há o descumprimento contratual e de princípios da legislação de proteção de dados pelo controlador ou operador de dados, já que é exigido um novo consentimento específico a fim de compartilhar informações pessoais. Mais grave ainda é quando ocorre a venda de bancos de dados entre agentes de tratamento de dados, contexto em que o próprio Código Consumerista proíbe, de acordo com o seu art. 43. Há uma decisão do Supremo Tribunal de Justiça que corrobora pela aplicação de danos morais *in re ipsa* nesse caso, devido à gravidade da situação, que pode ensejar a reparação de danos morais coletivos. Vejamos:

> EMENTA RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. A existência de fundamento não impugnado – quando suficiente para a manutenção das conclusões do acórdão recorrido – impede a apreciação do recurso especial (súm. 283/STF). 4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697/RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, DJe de 17/11/2014), em que a Segunda Seção decidiu que, no sistema credit scoring, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011 – dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu

> respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentada pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido (BRASIL,2019).

A aplicação de danos morais *in re ipsa* no contexto de vazamentos de dados pode ser justificado devido à gravidade desses casos, pois há sem dúvida violação ao direito de privacidade, garantido pela Carta Política. Há situações em que dados pessoais do usuário passam a ser conhecido por terceiros não autorizados, o que é uma violação aos deveres de segurança da legislação de proteção de dados. O vazamento de dados gera um prejuízo ainda maior quando a extensão do dano é maior, envolvendo mais titulares de dados. Levando-se em conta a cláusula da valorização da dignidade humana, presente na Constituição Federal, presume-se o dano moral sofrido pelos titulares de dados, que não sabem onde seus dados estão sendo compartilhados, o que vai de encontro ao princípio da autodeterminação informativa.

4.4 Vazamento de dados e a aplicação de danos morais *in re ipsa* nas decisões do Tribunal de Justiça do Estado de São Paulo e na doutrina recente

Analisando-se seis julgados recentes do Tribunal de Justiça de São Paulo verifica-se que os princípios da Lei Geral de Proteção de Dados são reafirmados em muitos casos, principalmente em situações em que ocorre a falha de serviço de agentes de tratamento, o que possibilita a aplicação dos artigos 42 e 46 da lei supracitada. No caso do art. 46 dessa lei a não aplicação das medidas de segurança ou o tratamento ilícito de dados em geral, vai gerar a responsabilização dos agentes de tratamento, podendo ocasionar dano moral ou mero dissabor cotidiano, a depender do caso concreto. No sentido de verificação de dano moral presumido, tem-se a seguinte decisão judicial:

> COMPROMISSO DE COMPRA E VENDA DE IMÓVEL. Ação de reparação de danos por falha na prestação do serviço – Código de Defesa do Consumidor que se mostra aplicável ao caso por se tratar de relação de consumo, sendo o consumidor a parte tecnicamente hipossuficiente. DENUNCIAÇÃO DA LIDE Ação em que se discute a responsabilidade das rés pelo acesso que terceiros tiveram aos dados pessoais do autor, e não a conduta das empresas fornecedoras de produtos e serviços que o contataram oferecendo serviços estranhos aos prestados pelas próprias rés - Indevida a denunciação pretendida, sendo a ré parte passiva legítima. INDEVIDO ACESSO DE DADOS - Acesso dos dados do cliente por terceiros, que passaram a efetuar telefonemas e enviar mensagens de texto e e-mails oferecendo serviços e produtos ao adquirente do imóvel Mensagens que mencionavam expressamente o empreendimento adquirido pelo autor Responsabilidade demonstrada. DANO MORAL Importunações que, sem nenhuma dúvida, geraram um transtorno significativo, implicando violação à paz de espírito do autor, que merece ser indenizado - Indenização proveniente de dano moral que deve obedecer aos princípios da razoabilidade e da proporcionalidade no momento da fixação do quantum debeatur Valor que deve ser prudentemente arbitrado, conforme as circunstâncias em concreto, de forma que seja nem exorbitante, dando margem ao injustificado locupletamento da vítima, nem demasiadamente irrisório e insignificante diante da capacidade econômica do demandado Valor estipulado que parece ser adequado, não merecendo reforma. Recursos não providos (SÃO PAULO,2021).

Nesse julgado foi reconhecido a relação de consumo entre o autor e o réu no contrato de promessa de compra e venda de imóvel, e foi levado em conta a pertinência da inversão do ônus da prova, devido a hipossuficiência técnica do requerente. A responsabilidades dos réus é devido ao acesso que terceiros, de forma indevida, tiveram aos dados pessoais do autor. Portanto foi reconhecido a falha do serviço prestado pelos réus, o que é apto a gerar responsabilidade civil objetiva e solidária da cadeia dos fornecedores, de acordo com o art. 14 do Código Consumerista. Foi reconhecido o dano moral *in re ipsa*, pois o prejuízo ao autor não precisou ser comprovado de forma específica e detalhada, já que a conduta ilícita dos réus gerou um transtorno significativo na integridade psíquica do autor.

A partir das jurisprudências analisadas, deve-se considerar que a aplicação de danos morais *in re ipsa* depende de requisitos nos casos concretos. A gravidade do vazamento de dados e a extensão de danos são levados em conta, mas muitos julgados oscilam entre a aplicação de danos morais presumidos ou danos morais subjetivos, mesmo em casos em que há o vazamento de dados por acesso não autorizado de terceiros, o que geraria um presumido dano à privacidade e intimidade dos titulares de dados e possibilitaria a aplicação da inversão do ônus da prova, quando há hipossuficiência técnica e verossimilhança das alegações do titular de dados (art. 42, § 2° da Lei Geral de Proteção de Dados). Pode-se dizer, segundo a análise jurisprudencial, que o vazamento de dados que envolver dados sensíveis gerará um grave abalo moral ao titular de dados, o que faz que seja presumido o dano moral.

Verifica-se uma tendência, nos julgados analisados, de não verificação de dano moral quando o titular de dados, autor da ação que pleiteia danos morais, não comprova a ocorrência de abalo moral sofrido quando seus dados pessoais são supostamente vazados. Não se provando o dano não haverá qualquer reparação por danos morais, refutando-se a tese, muito comum no âmbito consumerista, de que a expectativa de dano geraria em si a responsabilidade do fornecedor de serviços. Segue-se o entendimento jurisprudencial:

> APELAÇÃO CÍVEL Interposição contra sentença que julgou improcedentes os pedidos formulados, nos autos da ação de obrigação de fazer c.c. indenizatória por danos morais. Vazamento de informações pessoais dos consumidores, no caso, da consumidora autora do banco de dados da empresa ré. Falha configurada, todavia, que no caso, não caracterizadora de danos morais. Ausência de demonstração robusta e convincente, no caso, de que os dados da consumidora tenham sido indevidamente utilizados ou causado algum dano**.** Honorários advocatícios majorados em grau recursal, nos termos do artigo 85, § 11, do Código de Processo Civil/2015. Sentença mantida. Apelação não provida (SÃO PAULO,2021).

Nesse julgado constata-se que houve a aplicação da legislação consumerista ao caso, apesar de não haver o reconhecimento ao direito à inversão do ônus da prova. Houve um vazamento massivo de dados do cadastro da empresa Eletropaulo Metropolitana Eletricidade de São Paulo S/A, e o autor requer que seja reconhecido dano moral *in re ipsa* devido ao incidente de segurança. Porém o julgado possui entendimento contrário, sendo que seria necessário que o autor tivesse provado que seus dados vazados possuíam alguma relação com o vazamento massivo de dados e ainda mais que provasse que seus dados supostamente vazados teriam sido utilizados de forma irregular por terceiros (hackers). Portanto não há uma

presunção de que o autor tenha sido submetido a uma situação prejudicial que seja apta a configurar dano moral.

Em outro julgado relacionado também ao vazamento de dados pela empresa supracitada não houve também o reconhecimento de dano moral *in re ipsa*, pois se verificou que o acesso não autorizado de terceiros ao banco de dados configurou situação de excludente de culpabilidade, devido à culpa exclusiva de terceiro (art. 14, § 1° do Código Consumerista), mesmo havendo a adoção de medidas de segurança das informações. Não se aplicou danos morais pois o autor não logrou provar o dano e principalmente, o nexo causal entre a conduta ilícita da empresa ré e o seu suposto dano. Além do mais esse julgado destaca que se aplicariam danos morais apenas se os dados fossem classificados como sensíveis, o que é bastante criticável.

Indo de encontro à tese da aplicação de dano moral *in re ipsa*, pode-se dizer que:

> O vazamento de dados, embora possa ser considerado um ato ilícito (um dos requisitos adotados pela legislação brasileira para a responsabilização civil), não pode ser interpretado como causador de um dano moral em si, já que aquele que teve seus dados vazados poderá não ter qualquer prejuízo extrapatrimonial. Se o prejuízo vier a ocorrer, é certo que a partir de então nascerá o direito à respectiva indenização (ANDRADE, 2021).

Sem dúvida, há uma variação do entendimento entre os julgados analisados, inclusive devido as decisões judiciais serem recentes (2020/2021). Verifica-se que na maioria dos julgados foi reconhecido o dano material devido à falha na prestação de serviço, mas não foi aplicado, na maioria dos julgados, o dano moral *in re ipsa*, devido à falta de comprovação do prejuízo pelos titulares de dados pessoais. Não foi reconhecido na maioria dos casos de vazamento de dados a violação ao direito fundamental à privacidade, apta a ensejar danos morais.

5. CONSIDERAÇÕES FINAIS

A partir da doutrina e legislações analisadas, verifica-se que o titular de dados, o qual é equiparado ao consumidor quando reconhecido sua vulnerabilidade ínsita na relação de consumo, possui um direito à autodeterminação informativa. Segundo a Lei Geral de Proteção de Dados, o titular de dados tem o direito de ter conhecimento do fluxo de seus dados pessoais, o que envolve a localização dos dados, por quem está sendo tratado e para qual finalidade, consentida pelo titular de dados, estão sendo coletados, armazenados e processados seus dados pessoais. Havendo compartilhamento de dados a terceiros, deverá haver a renovação do consentimento pelo usuário, caso contrário se constituirá num tratamento irregular de dados.

O direito fundamental de privacidade dos titulares de dados está associado ao dever que as empresa públicas e privadas têm de apenas realizar o tratamento de dados se forem salvaguardados os direitos dos titulares de terem acesso aos dados, assim como a possibilidade de esses, de forma simplificada, peticionarem para os agentes de tratamento, com o fito de retificar os dados desatualizados, de revogarem o consentimento anterior ou de bloquearem os dados. Nesses dois últimos casos deverá haver a eliminação dos dados desnecessários, sob pena de aplicação de sanções administrativas e de responsabilização civil.

O direito à privacidade deve ser resguardado devido a vulnerabilidade dos titulares de dados, que possuem hipossuficiência técnica, informacional e econômica em relação aos agentes de tratamento. Além do mais os direitos à privacidade estão explicitados na Constituição Federal (incisos V e X), e deixar de reconhece-los nas relações civis e consumeristas vai de encontro ao efeito vinculante e irradiante que o qualquer direito fundamental deve ter, devido à imperatividade e supremacia da Lei Constitucional.

Ressalta-se que é essencial, na atividade de tratamento de dados, o cumprimento dos deveres de informação e de adoção de medidas técnicas e de segurança, que estão relacionadas às boas práticas/compliance, por parte dos agentes de tratamento. O Código Consumerista também ressalta o dever de informação em relação ao fornecedor, no seu art. 6°, inciso IV. Inclusive, no art. 43 do Código Consumerista, depreende-se o dever dos fornecedores de produtos e serviços de informação clara e atualizada em relação aos cadastros de consumidores que formam banco de dados, possibilitando acesso integral dos dados pessoais aos consumidores interessados. Nesse mesmo artigo, em seu §1°, evidencia-se um prazo

máximo de cinco anos para os cadastros de consumidores manterem informações negativas referentes a aqueles.

Um dos pontos mais destacados da Lei Geral de Proteção de Dados é o consentimento do titular de dados. Esse é essencial para, na maioria dos casos se iniciar a coleta e o tratamento de dados pessoais. O consentimento deve ser livre, informado e inequívoco, a fim de legitimar os dados pessoais que os terceiros utilizem, pois assim se garantirá a tutela do direito fundamental à privacidade

Em relação a responsabilização civil dos agentes de tratamento, essa possui correspondência com a responsabilidade civil no Código Consumerista. Há uma responsabilidade objetiva e solidária entre a cadeia de fornecedores ou de terceiros (agentes de tratamento), que violam os deveres de informação e de segurança atrelados a essas atividades. Inclusive, em muitas situações, passa a ser necessário a aplicação conjunta de princípios estabelecidos pela Lei Geral de Proteção de Dados (art. 6°) e pelo Código de Defesa do Consumidor, estabelecidos como direitos básicos do consumidor (art. 6°).

Quanto a violação de dados sigilosos, esses incidentes causam prejuízos aos titulares de dados, frustrando a expectativa que esses têm de que seus dados serão tratados em conformidade com a legislação de proteção de dados. Um incidente de segurança, devido à falta de medidas preventivas, inviabiliza o tratamento de dados, gerando um grande ônus ao usuário, que muitas vezes não possui nem acesso aos seus dados e além disso tem uma grande possibilidade de sofrer danos devido ao tratamento irregular de dados. Portanto, nesse contexto, a fim de resguardar a tutela da privacidade dos usuários, responsabilizam-se os agentes de tratamento por danos morais.

É importante enfatizar, consoante a análise das decisões judiciais cumuladas com a recente doutrina referente a legislação de dados que, a fim de se aplicar dano moral *in re ipsa*, é necessário levar em conta, ainda mais que a extensão de dano, a gravidade da culpa do ofensor. Ou seja, caso o agente de tratamento viole dados sigilosos por meio do compartilhamento de dados a terceiros não autorizados, e ainda mais gere a inscrição indevida do titular de dados em um cadastro de inadimplemento, estará presumido o dano moral. Logo, a presunção de dano moral aqui se dá pela ilicitude da conduta associada ao vazamento de dados, e não ao vazamento de dados em si.

Constata-se que não basta a não adoção de medidas técnicas e de segurança, além do compartilhamento indevido ou o acesso não autorizado de terceiros para se presumir o dano, pois nesses casos restaria ao titular de danos a comprovação do abalo moral sofrido. Parte-se da lógica que o autor da ação deve comprovar o fato constitutivo do seu direito (art. 373, inciso I do Código de Processo Civil) e o réu deve provar fatos que extinguem, impedem ou modificam o direito do autor. Contudo, a fim de se garantir o devido processo legal, resguardando-se o princípio da isonomia, é importante a aplicação da inversão do ônus da prova, a fim de que o titular de dados, em caso de vazamento de dados, cada vez mais frequentes, possa se desincumbir do ônus de provar que houve o vazamento de danos em si.

Seria absurdo não levar em conta a necessidade da inversão do ônus da prova a fim de se provar o dano moral, caso de fato não seja presumido o dano. É importante haver a tutela da privacidade do titular de danos, que é a parte vulnerável no contexto de tratamento de dados pessoais. Para isso é importante se aplicar os requisitos do Código Consumerista, que são mais favoráveis aos titulares de dados, para a efetivação da inversão do ônus da prova, que envolve requisitos alternativos, os quais são a verossimilhança das alegações e a hipossuficiência socioeconômica.

Pode-se dizer que, nas decisões judiciais referentes a legislação de proteção de dados há o predomínio da tese de que o dano moral deve ser comprovado pelo titular de dados. Esse deve provar que não houve apenas uma alteração leve em sua esfera psíquica, algo que não gere mais que um dissabor cotidiano. Além da questão do grau de culpa do agente de tratamento de dados, que gera um dano maior com prejuízos mais evidentes ao titular de dados, um fator que tem implica no reconhecimento ou não do dano moral *in re ipsa* é a natureza do dado vazado. A violação de dados sensíveis, aqueles que tem maior potencial de serem fatores de descriminação para o usuário, sem dúvida tem uma maior repercussão na esfera de privacidade desses, o que gera uma presunção de dano moral.

Pode-se dizer que a tese jurisprudencial predominante, de acordo com a análise dos julgados do Tribunal de Justiça de São Paulo, de que o abalo moral sofrido pelo titular de dados deve ser provado, vai de encontro a uma série de julgados na esfera consumerista, em que a presunção de dano moral é necessário para a adequada tutela da dignidade humana e dos direitos de personalidade do consumidor. Além das teses do Superior Tribunal da Justiça de que a inscrição indevida em cadastro de inadimplentes e a falha de serviço devido ao atraso de voo pela companhia aérea ocasiona dano moral presumido, a ausência de comunicação dos gestores

de banco de dados acerca da comercialização de informações pessoais em banco de dados também é também uma hipótese de dano moral *in re ipsa.*

Importante destacar que essa decisão do Superior Tribunal de Justiça, já citada anteriormente, foi anterior a vigência da Lei Geral de Proteção de Dados, levando em conta apenas o artigo 42 do Código Consumerista, que trata sobre banco de dados. É visível que na comercialização sem consentimento de dados para terceiros, há um compartilhamento indevido com o intuito de lucro. Logo a ausência de consentimento cumulada com o vazamento de dados com a finalidade ilícita de auferir lucro com base no prejuízo do titular de dados, reforça a necessidade de se presumir o dano moral sofrido por esse, sob risco de grave violação ao direito de privacidade do consumidor.

O vazamento de dados, surgido em consequência do tratamento irregular de dados (art. 46 da Lei Geral de Proteção de Dados), ocasionará o dano moral *in re ipsa* caso o compartilhamento irregular de dados a terceiros seja acumulado com a finalidade ilícita, por parte dos agentes de tratamento, de comercializarem os dados pessoais ou no contexto em que compartilhamento irregular de dados gerar como consequência a inscrição indevida dos titulares de dados em cadastros de inadimplentes.

Por conseguinte, para haver o dano moral *in re ipsa*, não basta o compartilhamento irregular de dados devido a acesso não autorizado de terceiro. O titular de dados deve provar o fato que constitui o seu direito, sendo admitida, contudo, a inversão do ônus da prova, por essa ser um meio processual importante para facilitar o sucesso do titular de dados no seu pleito indenizatório.

Deve-se ressaltar que a problemática inicial do presente trabalho se constituía da noção que os agentes de tratamento, quando da ocorrência de vazamentos de dados, são responsabilizados objetivamente pelos danos morais *in re ipsa* ocasioanados aos titulares de dados. A violação aos deveres de prevenção, segurança e de reparação por parte dos agentes de tratamento, por sua vez, geram a presunção de dano moral aos usuários, que deverão ser indenizados.

No entanto se constatou, a partir das decisões judiciais do Tribunal de Justiça de São Paulo e da doutrina analisada, que a aplicação dos danos morais *in re ipsa* no contexto de vazamento de dados não é a regra geral. Os titulares de dados devem provar a violação dos

dados pessoais, diferente do que ocorre na hipótese de dano moral presumido no caso dos acidentes de consumo. Indenizam-se as expectativas de dano nos casos em que houver vazamento de dados sensíveis ou quando há, além do vazamento de dados, a comercialização dos dados pessoais dos usuários por parte dos agentes de tratamento.

REFERÊNCIAS

ANDRADE, Carlos. **Vazamento de dados e a necessidade de comprovação do efetivo dano extrapatrimonial para que se reconheça o dever de indenizar**. Migalhas, 2021. Disponível em: migalhas.com.br. Acesso em: 26/08/2021.

BRASIL. Lei n°. 13.709/2018, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br. Acesso em: 08/07/2021.

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 08/07/2021.

BRASIL. Constituição Federal (1988). Disponível em: https:// www.planalto.gov.br. Acesso em: 20/07/2021.

BRASIL. Superior Tribunal de Justiça. (Terceira Turma). Recurso Especial n° 1292141 SP 2011/0265264 – 3. Relatora Ministra Andrighi. Brasília, 04 de agosto de 2012. Disponível em: stj.jusbrasil.com.br. Acesso em: 18/08/2021.

BRASIL. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial n° 1.758.799 – MG 2017/0006521 – 9. Relatora Ministra Nancy Andrighi. Brasília, 19/11/2019. Disponível em: conjur.com.br. Acesso em: 20/08/2021.

BRASIL. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial n° 1.424.304 –SP 2013/0131105 – 05. Relatora Ministra Nancy Andrighi. Brasília, 19/05/2014. Disponível em: stj.jusbrasil.com.br. Acesso em: 20/08/2021.

CAPANEMA, Walter Aranha. **A Responsabilidade civil na Lei Geral de Proteção de Dados.** Disponível em: www.tjsp.jus.br. Acesso em: 06/08/2021.

COSTA, Michele Romero da. **Responsabilidade pelo fato do produto ou do serviço**. Santa Maria/RS, 2007. Disponível em: periódicos.ufsm.br. Acesso em: 22/03/2021.

DIVINO, Sthéfano Bruno Santos; LIMA, Taisa Marina Macena de. **Responsabilidade civil na Lei Geral de Proteção de Dados Brasileira.** Disponível: https:// revista.univem.edu.br. Disponível: 09/08/2021.

FLUMIGNAN, Wévertton; FLUMIGNAN, Silvano. **Princípios que regem o tratamento de dados pessoais no Brasil.** Disponível em: www.researchgate.net. Acesso em: 26/07/2021.

FREITAS, Vitor Hugo das Dores. **Responsabilidade extracontratual dos agentes de tratamento.** Disponível em: < Publicadireito.com.br > Acesso em: 12/08/2021.

GARCIA, Leonardo de MEDEIROS. O Princípio da informação na pós-modernidade: direito fundamental do consumidor e o equilíbrio nas relações de consumo. **Revista UNIFACS**, Disponível em: www://revistas.unifacs.br. Acesso em: 08/08/2021.

LOPES, Laís de Figueiredo; CEZARINO, Maraísa Rosa**. LGPD e Compliance**: o encarregado de dados e o canal de denúncias nas organizações da sociedade civil. Migalhas, 2021. Disponível em: https://www.migalhas.com.br/depeso/348247/lgpd-e-compliance. Acesso em: 10/08/2021.

MODESTO, Alexandre Lindolfo; SILVA, Rodrigo Pereira Damásio da. **A responsabilidade civil em face de vazamento de dados de consumidores de sites de venda pela internet.** Disponível em: https://jus.com.br. Acesso em: 26/08/2021.

MENDES, Laura Schertel. **Transparência e privacidade:** Violação e proteção da informação pessoal na sociedade de consumo. Dissertação de Mestrado, Pós-Graduação em Direito, Faculdade de Direito da Universidade de Brasília, Brasília, junho de 2008.

MIRAGEM, Bruno. **A lei geral de proteção de dados (Lei 13.709/2018) e o Direito do Consumidor.** Porto Alegre/RS, Revista dos Tribunais, 2019. Disponível em: www.brunomiragem.com.br. Acesso em: 22/03/2021.

RUARO, Regina Linden; RODRIGUEZ, Daniel Pineiro. **O direito à proteção de dados pessoais e a privacidade.** Disponível em: https://revistas.ufpr.br. Acesso em: 20/07/2021

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. Apelação Cível n° 1049939-27.2020.8.26.0002 – Voto n° 82773. Relator Enio Zuliani. São Paulo, 18 de agosto de 2021. Disponível em: esaj.tjsp.jus.br. Acesso em: 20/08/2021.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. Apelação Cível n° 1005932 – 48.2020.8.26.0099 – Voto n° 17430. Relatora Ana Catarina Strauch. São Paulo, 20 de julho de 2021. Disponível em: esaj.tjsp.jus.br. Acesso em: 20/08/2021.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. Apelação Cível n° 1000407 – 06.2021.8.26.0405 – Voto n° 42127. Relator Soares Levada. São Paulo, 16 de agosto de 2021. Disponível em: esaj.tjsp.jus.br. Acesso em: 20/08/2021.

São Paulo. Tribunal de Justiça do Estado de São Paulo. Apelação Cível n° 1016844 – 03.2020.8.26.0068 – Voto n° 14.884. Relatora Heloísa Martins Mimessi. São Paulo, 05 de julho de 2021. Disponível em: esaj.tjsp.jus.br. Acesso em: 01/09/2021.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. Apelação Cível n° 1028828 – 93.2017.098.26.0001 – Voto n° 31.787/21. Relator Osvaldo Magalhães. São Paulo, 30 de agosto de 2021. Disponível em: esaj.tjsp.jus.br. Acesso em: 01/09/2021.

TARTUCE, Flávio. **DIREITO CIVIL:** DIREITO DAS OBRIGAÇÕES E RESPONSABILIDADE CIVIL. 13° edição. São Paulo, Editora Forense.

TEIXEIRA, RCA **O princípio da vulnerabilidade do consumidor do ciberespaço.** Disponível em: portalseer.ufba.br. Acesso em: 26/07/2020.

WOLKOFF, Alexander Porto Marinho. **A teoria do risco e a responsabilidade civil objetiva do empreendedor.** Disponível em: www.tjrj.jus.br. Acesso em: 12/08/2021.