

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO PROFESSOR JACY DE ASSIS

ANA LUÍSA TEODORO QUEIROZ

A RESPONSABILIDADE DO CONTROLADOR QUANTO AOS DANOS
CAUSADOS PELA VIOLAÇÃO DE DADOS PESSOAIS

Uberlândia - MG

2023

ANA LUÍSA TEODORO QUEIROZ

A RESPONSABILIDADE DO CONTROLADOR QUANTO AOS DANOS
CAUSADOS PELA VIOLAÇÃO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso
apresentado à Faculdade de Direito da
Universidade Federal de Uberlândia
como requisito parcial para obtenção do
título de bacharel em Direito.

Orientador: Prof. Dr. Almir Garcia
Fernandes

Uberlândia - MG

2023

RESUMO

O trabalho científico em questão aborda a evolução das leis de proteção de dados pessoais, com foco na Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro, com o objetivo de analisar as responsabilidades dos controladores de dados. A pesquisa apresenta a evolução dessas leis ao longo do tempo, fornecendo um panorama histórico do desenvolvimento dessas regulamentações. Além disso, examina como a LGPD tutela os dados pessoais e dados pessoais sensíveis, a partir da exploração das obrigações dos controladores e operadores de dados, detalhando as suas obrigações, papéis e medidas de segurança que devem ser adotadas para garantir a conformidade com a legislação. Por fim, a pesquisa se debruça sobre a violação de dados pessoais e a extensão dos danos que podem ocorrer nesses casos. Por fim, a Conclusão reúne os principais insights do estudo e destaca a importância da LGPD na proteção dos dados pessoais. Em resumo, este trabalho científico fornece uma visão abrangente sobre o desenvolvimento das leis de proteção de dados pessoais, com foco na LGPD, analisando aspectos como tutela dos dados, responsabilidade do controlador e a gestão de violações. Os resultados e conclusões destacam a importância da conformidade com a LGPD e a necessidade de medidas rigorosas para proteger os dados pessoais no cenário atual.

Palavras-chave: Proteção de Dados. Responsabilidade. Controlador de Dados. Danos pela Violação de Dados Pessoais.

ABSTRACT

This scientific work addresses the evolution of personal data protection laws, focusing on the General Data Protection Law (LGPD) in the Brazilian context, with the aim of analyzing the responsibilities of data controllers. The research presents the evolution of these laws over time, providing a historical overview of the development of these regulations. Furthermore, it examines how the LGPD protects personal data and sensitive personal data, by exploring the obligations of data controllers and operators, detailing their obligations, roles and security measures that must be adopted to ensure compliance with the legislation. . Finally, the research focuses on personal data breaches and the extent of the damage that can occur in these cases. Finally, the Conclusion brings together the main insights of the study and highlights the importance of LGPD in protecting personal data. In summary, this scientific work provides a comprehensive view of the development of personal data protection laws, with a focus on LGPD, analyzing aspects such as data protection, controller responsibility and breach management. The results and conclusions highlight the importance of compliance with the LGPD and the need for strict measures to protect personal data in the current scenario.

Keywords: Data Protection. Responsibility. Data Controller. Damages for Personal Data Breach.

SUMÁRIO

INTRODUÇÃO	6
I – Desenvolvimento e evolução das leis de proteção de dados pessoais	7
II – A tutela dos dados pessoais e dados pessoais sensíveis sob a Lei Geral De Proteção de Dados (Lei 13.709/18).....	9
III – A responsabilidade do controlador de dados no contexto da LGPD.....	11
IV – Violação dos dados pessoais e extensão dos danos.....	14
CONCLUSÃO.....	18

INTRODUÇÃO

A se considerar a era digital em que a sociedade está inserida, tornou-se ainda mais necessário compreender como as normas jurídicas regulam as relações virtuais e suas consequências. Com a expansão do comércio *online*, por exemplo, os usuários da *internet* cada vez mais se utilizam desse meio para viver. Por meio dele, é possível trabalhar, fazer compras, consultas, realizar transações bancárias, estudar, se divertir em redes sociais, dentre outros.

Ocorre que, para acessar essas atividades o indivíduo fornece seus dados pessoais, sejam eles sensíveis ou não. Dessa maneira, constrói-se uma enorme rede de informações pessoais, que precisam ser protegidos, respeitando o direito de privacidade e liberdade dos indivíduos. Sendo assim, o presente trabalho irá analisar os danos decorrentes da violação desses dados, bem como os limites da responsabilidade do controlador diante disso.

O desenvolvimento digital tomou proporções incalculáveis e consequentemente o fluxo de dados ficou cada vez mais intenso. Portanto, com vasto acesso aos dados pessoais dos indivíduos na rede, tornou-se imprescindível o estudo das legislações que regem sobre a proteção de dados e a responsabilidade em caso de violação.

Nesse sentido, a lei nº 13.709/2018 tem como principal objetivo a proteção de dados, trouxe em seu dispositivo uma série de regulamentações referente ao tratamento e transferência de dados, à segurança e ao sigilo desses, bem como a responsabilidade do controlador perante a violação de dados e as sanções administrativas aplicadas.

É de extrema relevância o resguardo de direitos fundamentais como direito à privacidade e liberdade do indivíduo. Por isso, neste estudo iremos analisar os danos causados ao titular de um dado violado e os limites da responsabilidade do controlador e como este deve agir.

Diante do exposto, o intuito geral desta pesquisa é demonstrar a importância de um tratamento de dados adequado, que respeite a privacidade do titular, bem como o desdobramento dos danos gerados em caso de violação e a responsabilidade do controlador. Ademais, visa ressaltar a relevância da Lei Geral de Proteção de Dados como papel fundamental e norteador da tutela dos dados.

Mais especificamente, pretende-se apontar as consequências da violação de dados pessoais; demonstrar a reponsabilidade do controlador diante dos danos causados pelo vazamento de dados; destacar a importância da lei nº 13.709/2018 na regulamentação da proteção dos dados pessoais e dados pessoais sensíveis; apresentar a evolução das leis de proteção de dados; e sugerir melhorias no tratamento de dados por parte do controlador.

Para isso, será utilizado como método de pesquisa o método dedutivo, na tentativa de se fazer das regras gerais, a solução para casos específicos. Os processos metodológicos a serem utilizados serão o estudo dogmático jurídico, visto a impossibilidade de um estudo profundo sem que se recorra à lei, à doutrina, ou à jurisprudência neste sentido. Além disso, destaca-se o uso de artigos científicos e de pesquisa histórica sobre a evolução da legislação e entendimento do tema ao longo do tempo.

I – Desenvolvimento e evolução das leis de proteção de dados pessoais

Como argumenta Bioni (2020), o momento atual é marcado por uma vigilância descentralizada, com múltiplos intervenientes envolvidos no processamento de dados sem separar as vidas *online* e *offline*. Nesta perspectiva, as violações de vários direitos fundamentais dos titulares dos dados estão aumentando, à medida que os seus direitos à privacidade são continuamente violados.

No contexto da ampla disponibilidade de dados na *internet*, com a chamada ‘dataficação das coisas’, os titulares dos dados percebem que alguns de seus direitos básicos são violados, e a Lei 13.709/2018, popularmente denominada Lei Geral de Proteção de Dados (LGPD), surgiu no Brasil com a necessidade de normativas que regulassem a participação dos titulares de dados no processamento de dados. A LGPD, nesse sentido, dá clara importância à exigência de consentimento e introduz a ideia de que essa permissão do titular seria um passo em direção ao princípio da autodeterminação informada.

Entretanto, para compreender a chegada da LGPD no Brasil, demonstra-se necessário perpassar pela trajetória da regulamentação do manejo dos dados no mundo. Sobre o assunto, como ensinam Andréa, Arquite e Camargo (2020), os debates sobre a privacidade dos usuários da *internet* surgiram após mais de trinta anos da sua existência.

A partir disso, tem-se a Convenção 108, de 1980, pioneira no tema, que teve como objetivo principal garantir a proteção de dados como um direito fundamental, e depois teve seu texto utilizado como referência para a *General Data Protection Regulation* (GDPR), que é a principal legislação sobre o assunto.

Ainda de acordo com Andréa, Arquite e Camargo (2020), a GDPR (General Data Protection Regulation), da União Europeia, entrou em vigor em 25 de maio de 2018 se trata de um regulamento geral aplicável a todas as empresas que exerçam algum tipo de atividade em algum país da Europa. Sendo o texto legal, essas organizações devem conceder um tratamento especial no tocante aos dados dos seus usuários.

Segundo o estudo de Andréa, Arquite e Camargo (2020), no contexto da América do Sul, o Chile foi o primeiro país a tratar sobre o tema, em 1999, por meio da *Ley 19.628 (Proyecto de Ley Protección de datos de caracter personal)*, seguido pela Argentina, em 2000, com a Lei de Proteção de Dados Pessoais 25.326/00. Já em 2008, o Uruguai publicou a *Ley de Protección de Datos Personales y Acción de “Habeas Data” 18.331/12*, considerada equivalente à da União Europeia. O Peru, por sua vez, surgiu com uma legislação sobre o tema em 2011, com a *Ley de Protección de Datos Personales 29.733/13*.

Do ponto de vista do Brasil, o direito à privacidade dos dados pessoais já era garantido pela Constituição, conforme consta do artigo 5º, inciso XII. Além disso, a segurança dos dados pessoais já está prevista em outros códigos, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei 12.414/11), a Lei 12.737/2012 (Lei Carolina Dieckmann), e, especialmente, o Marco Civil da *Internet* (Lei nº 12.965, de 2014).

A Lei n. 12.965/2014 em questão é o primeiro diploma legal brasileiro que define diretamente os princípios, garantias, direitos e responsabilidades do uso da *internet* no Brasil. Posteriormente, no entanto, os legisladores brasileiros iniciaram um trabalho para que essas normas fossem consolidadas em um código especial, o que originou as primeiras minutas da Lei Geral de Proteção de Dados (LGPD), que prevê especificamente a proteção de dados pessoais, como alternativa ao Marco Civil da *Internet*.

É válido mencionar que, antes do Projeto de Lei 53/2018, que se tornou a Lei Geral de Proteção de Dados no Brasil, outros existiram. No entanto, apresentaram-se

incompletos e não tratavam do tema como se deveria. Sendo assim, conforme Carta ao Senado pela imediata aprovação do PLC 53/2018 (2018):

A proposta é o resultado possível e maduro de diálogo e negociação intensa entre diversos interessados na consolidação de uma moderna lei geral de proteção de dados pessoais, adequada ao atual contexto tecnológico, compatível com futuros avanços e compromissada com direitos fundamentais. Hoje, o mundo todo repensa a relação entre inovações tecnológicas e riscos coletivos gigantescos. E o Brasil pode dar um passo certo na direção de mais segurança jurídica e de uma economia de dados centrada no respeito a direitos.

Em julho de 2018, então, o referido projeto de lei foi aprovado pelo Senado Federal, sancionado e publicado em agosto do mesmo ano, sob o título de Lei 13.709/2018, com vigência 24 meses após sua publicação no Diário Oficial da União.

II – A tutela dos dados pessoais e dados pessoais sensíveis sob a Lei Geral De Proteção de Dados (Lei 13.709/18)

No intuito de regular o tratamento de dados, a LGPD subdivide os dados, entre pessoais - aqueles que são compostos por informações relacionadas a pessoa natural identificada ou identificável (artigo 5º, I) – e “sensíveis”, que se referem à “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (art. 5º, II).

Conforme ensina Mulholland (2018), mesmo que tenha sido introduzida uma definição expandida de dados pessoais sensíveis por esta lei, a maneira como esses dados são tratados legalmente já era conhecida no contexto da legislação brasileira desde que a Lei de Cadastro Positivo (Lei 12.414/11) foi promulgada. Essa lei proíbe, em seu artigo 3º, § 3º, II, a inclusão de informações sensíveis em bancos de dados usados para análise de crédito, considerando como sensíveis informações relacionadas à origem social e étnica, saúde, informação genética, orientação sexual, convicções políticas, religiosas e filosóficas. Isso significa que, para fins de análise de concessão de crédito, é proibido incluir em bancos de dados qualquer informação de natureza pessoal que não esteja

diretamente relacionada com o objetivo da análise de crédito, a fim de evitar qualquer forma de discriminação.

O princípio da não discriminação, nesse contexto, é de considerável importância, independentemente se realizado por entidades privadas, como fornecedores de produtos e serviços, ou por entidades públicas.

Inicialmente, a Lei Geral de Proteção de Dados concede uma ênfase substancial no consentimento do titular dos dados como base para o tratamento de dados pessoais. Isso implica que o tratamento de dados pessoais só é permitido quando o titular expressa seu consentimento livre, informado e inequívoco para uma finalidade específica (art. 5º, XII). Além disso, a LGPD estabelece restrições significativas no tratamento de dados sensíveis e requer que o consentimento seja obtido de forma específica e destacada, para finalidades singulares (artigo 11, I, LGPD).

Insta salientar que essa legislação também permite o tratamento de dados sensíveis sem a necessidade de consentimento do titular quando for essencial para o tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos pelo setor público (artigo 11, II, b, LGPD), além de outras exceções que se relacionam principalmente a interesses públicos. Nesses casos, o consentimento do titular dos dados sensíveis, seja genérico ou específico, é dispensado com base em uma avaliação de interesses feita pela lei, que prioriza os interesses públicos em detrimento dos interesses do titular, mesmo que estes últimos sejam considerados Direitos Fundamentais.

Sendo assim, a grande inovação da Lei 13.709/2018 reside no fato de que ela introduz uma abordagem moderna para o tratamento de dados, independente da finalidade. Embora os objetivos ainda desempenhem um papel significativo nesse tratamento e sejam considerados necessários, a lei em comento estabelece diretrizes para o manuseio de dados pessoais. Ao contrário das regulamentações setoriais que tradicionalmente se concentram no tratamento de dados pessoais para finalidades específicas em setores regulamentados, a LGPD coloca mais poder nas mãos dos cidadãos.

Diante de todo o exposto, conclui-se que a Lei Geral de Proteção de Dados representa um dispositivo fundamental que posiciona o Brasil como um país que trata os

dados com segurança, além de ser uma legislação inovadora em comparação com o restante da legislação brasileira, que carecia de regulamentação específica para a proteção de dados.

Entre as inovações introduzidas pelo texto em análise, destaca-se a definição de consentimento, o qual ainda é colocado como sujeito a várias outras regulamentações no texto, devendo ser "livre, informado e inequívoco" nesse contexto de troca de dados. Desse modo, o consentimento se mostra importante ao controlador de dados.

III – A responsabilidade do controlador de dados no contexto da LGPD

A Lei 13.709/2018, ao firmar os direitos de proteção aos dados pessoais, estabelece, ao mesmo tempo, um rol de deveres voltados a quem exerce a atividade de tratamento dessas informações.

Como ditam Divino e Lima (2020), o tratamento de dados deve obrigatoriamente aderir a diversos princípios, incluindo a finalidade, a adequação e a necessidade. O operador ou controlador de dados deve, nesse contexto, comunicar ao titular quais são os objetivos específicos do tratamento de dados, bem como como se esse tratamento se relaciona com a sua atividade econômica. Isso ocorre porque a privacidade e a proteção das informações ganham uma perspectiva mais transparente no tratamento de dados, estabelecendo uma relação na qual aquele que realiza o processo deve definir de forma clara como os dados são utilizados. Isso permite ao titular, em situações de litígio judicial ou em casos de danos morais e materiais, identificar com precisão onde ocorreu qualquer problema.

Ainda, conforme ensina Capanema (2020), a LGPD estabelece distinções nos deveres a serem cumpridos com base na relação que têm com o tratamento de dados, identificando o responsável pela tomada de decisões no tratamento como ‘controlador’, enquanto a parte que executa o tratamento sob as instruções do controlador é denominada ‘operador’. Juntos, eles são referidos como ‘agentes de tratamento’. Sob uma perspectiva civilista, o controlador equivale ao mandante, e o operador ao mandatário. Pode-se até considerar que a relação controlador-operador constitui uma forma especial de mandato, especialmente aplicável a situações que envolvem o tratamento de dados pessoais.

Nessa relação jurídica, existe um terceiro ator, o ‘encarregado’, que pode ser uma pessoa natural ou jurídica, fazendo parte ou não da equipe do controlador ou operador. O encarregado desempenha várias funções, incluindo a mediação entre os outros agentes, em particular a Autoridade Nacional de Proteção de Dados (ANPD), além de orientar a aplicação das regras de proteção de dados.

Dito isso, a responsabilidade civil, no âmbito da Lei Geral de Proteção de Dados, está regulamentada na Seção III, do Capítulo VI, do referido texto legal. Vale ressaltar que as regras ali descritas são aplicáveis a todos os casos envolvendo o tema, podendo inclusive ser aplicadas normas específicas, como o Código do Consumidor, segundo o artigo 45 da LGPD.

Essa responsabilidade surge da prática de atividades de proteção de dados que violem a legislação de proteção de dados. Com essa terminologia, o legislador reconhece que a proteção de dados constitui um microssistema legal com normas presentes em várias leis, sendo a LGPD sua principal estrutura. Pode-se fazer uma analogia com o conceito de ‘legislação tributária’ do artigo 96 do CTN, abrangendo não apenas as leis relacionadas à proteção de dados, mas também as normas regulamentares emitidas pela ANPD ou outras entidades.

No entanto, a responsabilidade civil prevista na LGPD não se limita à violação do microssistema jurídico de proteção de dados, devendo-se interpretar o art. 42¹, caput em conjunto com o art. 44, parágrafo único².

O artigo 46³, por sua vez, determina que os responsáveis pelo tratamento de dados devem adotar medidas de segurança, tanto técnicas quanto administrativas, com o intuito

¹ Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

² 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.

³ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

de proteger os dados pessoais. Essas normas de segurança podem ser elaboradas pela Autoridade Nacional de Proteção de Dados (ANPD).

Consequentemente, na LGPD, é possível identificar duas situações que podem gerar responsabilidade civil: a violação de normas legais no âmbito do microssistema de proteção de dados; a violação de normas técnicas voltadas para a segurança e proteção de dados pessoais.

Naturalmente, a responsabilidade civil só se concretizará se a violação dessas normas, seja de natureza legal ou técnica, resultar em dano material ou moral a um indivíduo ou a uma comunidade.

O artigo 42 limita a responsabilidade civil ao controlador ou ao operador. A conjunção alternativa ‘ou’ estabelece uma alternativa entre o controlador e o operador. Entretanto, se a relação do titular com o controlador e o operador for de natureza consumerista, as normas de responsabilidade solidária estabelecidas nos artigos 12 e 18 do Código de Defesa do Consumidor (CDC) serão aplicadas.

O parágrafo 1º do artigo 42 apresenta duas exceções a essa regra de alternância, permitindo a solidariedade em dois casos específicos para garantir uma indenização efetiva ao titular dos dados. No primeiro caso (inciso I), o operador é solidariamente responsável se ele descumprir a legislação de proteção de dados ou não seguir as instruções lícitas do controlador, equiparando-se, nesse aspecto, à situação do mandatário que não segue as instruções do mandante. Já no segundo caso (inciso II), a solidariedade se aplica entre os controladores que estiverem diretamente envolvidos no tratamento e que tenham contribuído para decisões que violem o microssistema da proteção de dados ou as normas técnicas aplicáveis.

O parágrafo 2º do artigo 42 permite a inversão do ônus da prova, a critério do juiz, a favor do titular de dados, desde que a alegação seja verossímil, haja hipossuficiência para a produção de provas ou a produção de provas pelo titular seja excessivamente onerosa. Essa norma sobre a inversão do ônus da prova é semelhante àquelas encontradas em outras leis, como o artigo 373, parágrafo 1º do Código de Processo Civil (CPC)⁴ e o

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

⁴ § 1º Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova

artigo 6º, inciso VIII do CDC⁵, que se aplica a ações de natureza consumerista e exige menos requisitos.

Além da inversão do ônus da prova, a responsabilidade civil na LGPD é do tipo objetiva, ou seja, não é necessário discutir a culpa do agente. Como afirmam Divino e Lima (2020), no que se refere a atos ilícitos praticados por indivíduos particulares, a responsabilidade é de natureza objetiva. Isso significa que o artigo 43 da LGPD lista situações em que esses sujeitos somente não serão responsabilizados se conseguirem comprovar as condições ali estabelecidas. Nesse contexto, não se leva em consideração a culpa ou o dolo; a responsabilidade é imposta de maneira automática com base nas circunstâncias estipuladas na lei.

Por outro lado, quando se trata de atos ilícitos cometidos por entidades públicas no tratamento de dados, a legislação é omissa. A princípio, a responsabilidade parece ser subjetiva, devido à falta de descrição e tipificação legal específica na LGPD. No entanto, por meio de uma interpretação hermenêutica, aplicando o método hermenêutico concretizador e considerando também a Constituição Federal, mais precisamente em seu artigo 37, parágrafo 6º, a responsabilidade é delimitada como objetiva para as entidades públicas pertencentes ao aparato administrativo.

Portanto, mesmo que a legislação não aborde explicitamente os termos da responsabilidade das entidades públicas, entende-se que ela deva ser de natureza objetiva, sem a possibilidade de exceções devido ao silêncio do legislador sobre o assunto.

IV – Violação dos dados pessoais e extensão dos danos

do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído.

⁵ Art. 6º São direitos básicos do consumidor:
(...)

VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências;

Segundo Ribeiro e Carvalho (2020), a Lei Geral de Proteção de Dados teria um impacto positivo na compensação dos consumidores, uma vez que tornaria as consequências dos vazamentos e violações de dados pessoais ainda mais evidentes e públicas. Isso incentivaria não apenas as empresas a se conformarem com as regulamentações de tratamento de dados, mas também incentivaria os titulares desses dados a tomar precauções ao compartilhar informações sensíveis.

Entretanto, fato é que, devido à ampliação constante da exposição da sociedade provocada pela tecnologia da informação, é comum ocorrerem inúmeros incidentes de violação de dados pessoais e divulgação não autorizada de informações, o que resulta na exposição de informações confidenciais pertencentes aos titulares.

Nesse contexto, nos termos do que ensina Dias (2021), a coleta de dados pessoais, sem o conhecimento e consentimento do indivíduo, resulta em sérias violações à privacidade. Um exemplo disso seria quando dados pessoais compartilhados por um usuário para concluir uma transação comercial são vendidos a um anunciante sem o conhecimento do indivíduo. A transferência de dados entre diferentes contextos representa um desafio, especialmente quando os usuários não têm ciência de que isso está ocorrendo.

Isso ressalta a importância do dever do responsável pelo tratamento de dados de compreender o contexto no qual os dados são coletados e de respeitar a integridade desse contexto. Esse princípio está alinhado com o conceito de ‘finalidade’ no tratamento de dados, conforme previsto na LGPD, que exige a coleta de dados pessoais apenas para fins legítimos, informando claramente aos usuários a finalidade dessa coleta.

No cotidiano, ao navegar na *web* ou usar aplicativos de *e-mail* e redes sociais, estamos expostos a métodos que podem comprometer nossos dados pessoais, tornando-os suscetíveis a serem coletados por criminosos. Cibercriminosos podem explorar indivíduos e roubar informações confidenciais por meio de várias estratégias, como *Phishing*, *Spoofing* e *Pharming*⁶.

⁶ De acordo com a Texas Tech University (<https://www.ttu.edu/cybersecurity/lubbock/digital-life/digital-identity/scams-spam-phishing-spoofing-pharming.php>), *Phishing* é um e-mail enviado por um criminoso da Internet disfarçado de e-mail de uma fonte legítima e confiável. O objetivo da mensagem é induzi-lo a revelar informações confidenciais. Por outro lado, *Spoofing* descreve um criminoso que se faz passar por outro indivíduo ou organização, com a intenção de coletar informações pessoais ou comerciais. Por fim, *Pharming* é um site malicioso que se assemelha a um site legítimo, usado para coletar nomes de usuário e senhas.

Além disso, muitas vezes, os responsáveis pelo tratamento de dados pessoais (sejam controladores ou operadores) transferem esses dados de um contexto para outro, como retirar informações de transações de clientes e vendê-las para uso em publicidade direcionada. Em resumo, a inteligência preditiva direciona as estratégias de publicidade e propaganda com o objetivo de estimular um desejo de consumo latente nos usuários de seus serviços.

Portanto, as políticas de proteção de dados devem garantir que essa descontextualização não prejudique os titulares de dados. Além disso, elas devem assegurar que os titulares de dados tenham a oportunidade de expressar suas preferências sobre se, quando e como isso deve ocorrer e garantir a anonimização dos dados.

Nesta senda, a Lei Geral de Proteção de Dados atua como um intermediário, comunicando às empresas que elas devem se conformar com as regulamentações de coleta e uso de dados pessoais. Não é mais viável para as empresas determinarem unilateralmente como agir nesse sentido, já que os usuários agora têm voz e podem reivindicar seus direitos.

Como leciona Madeira (2022), quando se trata da compensação por danos morais resultantes de violações de dados pessoais, é importante destacar a possibilidade de tal violação se configurar como um dano *in re ipsa*, ou seja, presumido. No campo jurídico brasileiro, existem diversas opiniões divergentes sobre o ônus da prova em casos de danos morais. Muitos na doutrina argumentam que, devido à natureza intrínseca dos danos morais, o ônus da prova deve recair sobre o agressor, uma vez que seria difícil comprovar a extensão de danos puramente extrapatrimoniais, que se limitam ao domínio da subjetividade.

Portanto, para esse segmento da doutrina, é incumbência das vítimas de danos morais demonstrar que a conduta do causador do dano foi capaz de prejudicar aspectos juridicamente protegidos de sua existência, como direitos da personalidade e garantias fundamentais. Não seria necessário provar que o dano resultou em transtorno psicológico, abalo mental ou qualquer sentimento negativo. Esses efeitos psicológicos podem ser considerados como indícios de dano patrimonial, mas não são determinantes para estabelecer a existência de um dano moral efetivo.

Por outro lado, alguns autores, como Humberto Theodoro Júnior, argumentam que, embora seja impossível penetrar na mente da vítima para avaliar se a conduta causou, de fato, um abalo psicológico, é incumbência do juiz analisar as repercussões do dano "em relação à sua lesividade psicológica natural, com base na experiência da vida, ou seja, no que comumente ocorre na vida social do indivíduo 'médio'. Para esse autor, o conceito de dano moral *in re ipsa* é útil para demonstrar que certas condutas ou atividades já são amplamente reconhecidas como capazes de causar danos extrapatrimoniais.

No entanto, apesar da opinião predominante na doutrina, no campo judicial, há muitos julgamentos discordantes que ainda consideram necessária a avaliação do critério do *pretium doloris*, ou seja, a existência de um abalo psicológico para configurar o dano moral. Poucos casos julgados destacam que o dano moral é, de fato, presumido.

Nesse sentido, o dano moral presumido pode ser visto como um instrumento judiciário que amplia a proteção da responsabilidade civil em situações específicas, proporcionando um ônus probatório mais favorável à vítima em relação ao dano em ocorrências que já tenham um potencial lesivo e gravidade reconhecidos de forma repetida.

No contexto da proteção de dados, a discussão doutrinária e jurisprudencial sobre a possibilidade de presumir o dano moral ainda está em estágio inicial, já que existem poucos casos julgados que tratam diretamente desse tópico. É importante considerar e diferenciar a natureza dos dados envolvidos ao discutir o ônus da prova e a presunção do dano moral na área de proteção de dados. No caso de dados pessoais sensíveis, que contêm informações sobre aspectos íntimos do titular, o dano causado à vítima pode ser ainda mais grave em comparação com uma violação que envolva, por exemplo, a divulgação de dados pessoais não sensíveis a terceiros.

Isso ocorre porque, apesar de toda a operação de tratamento de dados pessoais envolver a manipulação de um direito pessoal do titular, as atividades de tratamento de dados sensíveis envolvem a utilização, transferência e divulgação de informações relacionadas aos aspectos mais íntimos da pessoa. O titular dos dados pode optar por não compartilhar essas informações com pessoas próximas, o que torna a sensibilidade dessas operações ainda mais acentuada.

Como exemplo, se ocorrer um incidente de segurança que leve à divulgação pública de informações relacionadas à opinião política ou à afiliação a um grupo político

de um indivíduo, as consequências desse incidente podem ser devastadoras, resultando possivelmente em perseguição no ambiente de trabalho, discriminação em futuras contratações e assédio por parte de grupos políticos adversos.

É importante destacar que a LGPD concede uma proteção mais abrangente às categorias de dados identificadas como sensíveis devido ao evidente potencial prejudicial e discriminatório do uso inadequado dessas informações. Portanto, considerando a concepção atual do dano moral presumido no sistema judiciário, fica evidente que a violação de dados pessoais sensíveis se encaixa perfeitamente nesse conceito, uma vez que seu principal objetivo é aumentar a eficácia da responsabilidade civil em casos em que a gravidade já é amplamente reconhecida, simplificando o ônus da prova.

Com este gancho, demonstra-se importante versar sobre como os danos sofridos graças às violações dos dados são quantificados no âmbito judicial. Como ensina Medeiros (2021), os dados pessoais geralmente têm importância financeira para as entidades que os coletam e utilizam, inclusive para fins comerciais. No entanto, muitas vezes, seu valor não pode ser facilmente quantificado pelos titulares desses dados. Em certas situações, como em casos de fraudes, é possível identificar danos financeiros diretos, e a compensação é calculada com base nessas perdas. No entanto, na maioria das situações, os danos são de natureza não financeira, ou seja, extrapatrimoniais.

Além da extensão dos danos, existem outros critérios para avaliar a quantia a ser paga em indenização, incluindo a capacidade econômica do responsável pela violação e o aspecto educativo da compensação. Um dos fatores que pode e deve ser considerado na avaliação dos danos morais sofridos é o valor financeiro dos próprios dados quando usados de maneira contrária às normas legais e técnicas.

Portanto, a fim de garantir que a proteção legal dos titulares de dados pessoais não seja prejudicada em casos de violações que resultem em danos, especialmente danos extrapatrimoniais, é essencial analisar os elementos específicos do caso em questão ao determinar o valor da indenização.

CONCLUSÃO

Em face do crescente avanço da sociedade na era digital e da ampla utilização da *internet* para as mais diversas atividades cotidianas, o armazenamento e tratamento de dados pessoais tornaram-se uma questão crucial. A proteção da privacidade e da liberdade individual se faz necessária para garantir que as relações virtuais se desenvolvam de maneira segura e ética. A legislação, exemplificada pela lei nº 13.709/2018, desempenha um papel vital na regulamentação e proteção dos dados pessoais e sensíveis.

O estudo realizado demonstra a importância de um tratamento de dados adequado, destacando as consequências da violação de dados pessoais e a responsabilidade do controlador diante dos danos resultantes. Além disso, ressalta o papel essencial da Lei Geral de Proteção de Dados como um guia para a tutela dos dados.

Analisando a evolução global da regulamentação de dados, observa-se que a União Europeia foi pioneira com a GDPR, que entrou em vigor em 2018. No Brasil, embora a Constituição já garantisse o direito à privacidade dos dados pessoais, a LGPD representou um avanço na regulamentação e consolidação dos princípios, direitos e responsabilidades relacionados à proteção de dados. A LGPD substituiu o Marco Civil da *Internet* e trouxe um arcabouço legal mais completo para a proteção dos dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) estabelece uma distinção crucial entre dados pessoais e sensíveis, alinhando-se com as melhores práticas internacionais. No contexto da regulamentação de dados sensíveis, a legislação em comento reforça o princípio da não discriminação, proibindo a inclusão de informações sensíveis em bancos de dados de análise de crédito, a fim de evitar qualquer forma de discriminação.

O consentimento do titular dos dados é um elemento central da Lei 13.709/2018, garantindo que o tratamento de dados pessoais seja baseado em consentimento livre, informado e inequívoco. A lei estabelece restrições significativas no tratamento de dados sensíveis e exige que o consentimento seja obtido de forma específica e destacada, para finalidades singulares.

Em resumo, a LGPD é uma legislação fundamental que coloca o Brasil em conformidade com os padrões de proteção de dados e destaca-se como uma regulamentação inovadora no contexto da legislação brasileira. Ela define claramente o consentimento como "livre, informado e inequívoco", estabelecendo um marco para a segurança no tratamento de dados pessoais. Essa lei é um passo importante para garantir a proteção dos direitos dos cidadãos em um mundo cada vez mais digital.

A Lei Geral de Proteção de Dados visa a proteger a privacidade e a liberdade individual, regulando o armazenamento e tratamento de dados pessoais e estabelece distinções entre dados pessoais e sensíveis, enfatizando o consentimento do titular dos dados e proibindo discriminação. Além disso, estabelece responsabilidade civil para controladores e operadores em caso de violações, com inversão do ônus da prova a favor do titular em casos verossímeis. A presunção do dano moral é essencial na proteção de dados sensíveis. Em suma, a LGPD fortalece a proteção de dados pessoais e os direitos dos titulares, assegurando uma compensação justa em casos de violações de dados.

REFERÊNCIAS

ANDRÉA, Gianfranco Faggin Mastro; ARQUITE, Higor Roberto Leite; CAMARGO, Juliana Moreira. PROTEÇÃO DOS DADOS PESSOAIS COMO DIREITO FUNDAMENTAL: A EVOLUÇÃO DA TECNOLOGIA DA INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL. Thomson Reuters Legal One: Revista de Direito Constitucional e Internacional, Brasil, v. 121, n. 202011423, p. 115-139, set. 2020. DTR\2020\11423. Disponível em: <https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/revistas-especializadas/rdci-121-gianfranco-andrea-e-outros.pdf>. Acesso em: 16 out. 2023.

BIONI, B. R. Xequi-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em: 06 set. 2023.

BRASIL. Lei nº 13709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lgpd). Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 12 set. 2023.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF, 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 08 set. 2023.

BRASIL. Lei nº 12965, de 23 de abril de 2014. Estabelece Princípios, Garantias, Direitos e Deveres Para O Uso da *Internet* no Brasil. Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 06 out. 2023.

BRASIL. Lei nº 10406, de 10 de janeiro de 2002. Institui O Código Civil. Brasília, DF, 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 06 out. 2023.

BRASIL. Projeto de Lei da Câmara 53, de 2018. Disponível em: [\[https://legis.senado.leg.br/sdleg-getter/documento?dm=7738705&ts=1571776630943&disposition=inline\]](https://legis.senado.leg.br/sdleg-getter/documento?dm=7738705&ts=1571776630943&disposition=inline). Acesso em: 15 out. 2023

COALIZÃO DIREITOS NA REDE. Carta ao Senado pela imediata aprovação do PLC 53/2018. Disponível em: [\[\[https://medium.com/direitos-na-rede/pela-imediata-aprovacao-do-plc53-18-e50072b37713\]](https://medium.com/direitos-na-rede/pela-imediata-aprovacao-do-plc53-18-e50072b37713). Proteção dos dados pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil. Acesso em: 15 out.2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 14 out. 2023.

BRASIL. Lei nº 8078, de 11 de setembro de 1990. Dispõe Sobre A Proteção do Consumidor e Dá Outras Providências. Brasília, DF, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 20 set. 2022

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Biblioteca Digital Jurídica do Superior Tribunal de Justiça, São Paulo, v. , n. , p. 163-170, jan. 2020. Cadernos Jurídicos da Escola Paulista da Magistratura. Disponível em: <https://core.ac.uk/reader/322682320>. Acesso em: 16 out. 2023.

DIAS, José Lucas da Costa. AS SANÇÕES ADMINISTRATIVAS DA LGPD, RESPONSABILIDADE E RESSARCIMENTO DE DANOS:: uma ótica a partir da violação aos dados pessoais pelo compartilhamento irregular e falta de segurança da informação. 2021. 56 f. TCC (Graduação) - Curso de Escola de Direito e Relações Internacionais, Coordenação Adjunta de Trabalho de Curso Monografia Jurídica, Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1648/1/JOSE%cc%81%20LUCAS%20DA%20COSTA%20DIAS.pdf>. Acesso em: 17 out. 2023.

DIVINO, Stéfano Bruno Santos; LIMA, Taisa Maria Macena de. RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA. Revista Em Tempo, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: <<https://revista.univem.edu.br/emtempo/article/view/3229>>. Acesso em: 16 out. 2023. doi: <https://doi.org/10.26729/et.v20i1.3229>.

FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti. A RESPONSABILIDADE CIVIL DOS PROVEDORES DE BUSCA DE PRODUTOS NA *INTERNET*. Revista da Faculdade de Direito da Uerj, Rio de Janeiro, v. 37, n. 37, p. 75-95, 01 jun. 2020. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/rfduerj/article/view/36191>. Acesso em: 16 out. 2023.

MULHOLLAND, CAITLIN SAMPAIO. “Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)”. Revista de Direitos e Garantias Fundamentais, vol. 19, no 3, dezembro de 2018, p. 159–80. sisbib.emnuvens.com.br, <https://doi.org/10.18759/rdgf.v19i3.1603>.

FERNANDES, Almir Garcia; RODRIGUES, Marcela Cunha Santos. Responsabilidade Civil e Fake News. In: VEIGA, Fabio da Silva; ALVES, Rodrigo Vitorino Souza;

FONSECA, Maria Hemilia. Diálogo dos Direitos Humanos. Porto: Instituto Iberoamericano de Estudos Jurídicos, 2022. p. 143-156.

GUIMARÃES, João Alexandre Silva Alves; FACCIO, Letícia Preti. A Tutela do Consumidor Digital: Vulnerabilidade Algorítmica, Publicidade Virtual e Responsabilidade Civil. In: VEIGA, Fabio da Silva; ALVES, Rodrigo Vitorino Souza; FONSECA, Maria Hemilia. Diálogo dos Direitos Humanos. Porto: Instituto Iberoamericano de Estudos Jurídicos, 2022. p. 129-142.

LUGATI, L. N.; ALMEIDA, J. E. de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. Revista de Direito, [S. l.], v. 12, n. 02, p. 01–33, 2020. DOI: 10.32361/2020120210597. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/10597>. Acesso em: 10 out. 2023.

MADEIRA, Anselmo Henrique Mamede. A POSSIBILIDADE DE CONFIGURAÇÃO DE DANO MORAL IN RE IPSA EM DECORRÊNCIA DE VIOLAÇÃO DE DADOS PESSOAIS. 2022. 47 f. TCC (Graduação) - Curso de Faculdade Nacional de Direito, Centro de Ciências Jurídicas e Econômicas, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2022. Disponível em: <https://pantheon.ufrj.br/bitstream/11422/19875/1/AHMMadeira-min.pdf>. Acesso em: 17 out. 2023.

MEDEIROS, Thais Carneiro. RESPONSABILIDADE CIVIL PELA VIOLAÇÃO AO DIREITO À PROTEÇÃO DE DADOS PESSOAIS. 2021. 47 f. TCC (Graduação) - Curso de Faculdade de Direito, Departamento de Direito Privado, Universidade Federal do Ceará, Fortaleza, 2021. Disponível em: https://repositorio.ufc.br/bitstream/riufc/63443/1/2021_tcc_tcmedeiros.pdf. Acesso em: 17 out. 2023.

RIBEIRO, Micaela Mayara; CARVALHO, Thomaz Jeferson. LEI GERAL DE PROTEÇÃO DE DADOS: CONSEQUÊNCIAS JURÍDICAS DA VIOLAÇÃO DA PRIVACIDADE PARA OBTENÇÃO DE DADOS. Anais Eletrônico Isbn 978-65-5615-164-9: X Mostra Interna de Trabalhos de Iniciação Científica III Mostra Interna de Trabalhos de Iniciação em Desenvolvimento Tecnológico e Inovação, Brasil, 1-4, jun. 2020.