Revista Ibero- Americana de Humanidades, Ciências e Educação- REASE

doi.org/10.51891/rease.v10i5.13668

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: RESPONSABILIDADE CIVIL NO VAZAMENTO DE INFORMAÇÕES

GENERAL PERSONAL DATA PROTECTION LAW: CIVIL LIABILITY FOR INFORMATION LEAKAGE

Larissa de Jesus Oliveira[1]
Thyara Gonçalves Novais[2]

RESUMO: A proteção e a segurança dos dados pessoais têm sido um tema cada vez mais relevante na sociedade contemporânea, sobretudo pelo avanço das tecnologias de informação e comunicação. Nesse contexto, o vazamento de dados pessoais é uma preocupação crescente, demandando do poder jurisdicional a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD), atualmente em vigor no Brasil. Este artigo busca analisar a responsabilidade civil das empresas em casos de vazamentos de dados pessoais, no contexto da LGPD. A fim de trazer mais clareza ao tema proposto, inicialmente, serão abordados os fundamentos da LGPD e as diretrizes estabelecidas pela legislação para o tratamento de dados pessoais, evidenciando a necessidade de proteção dessas informações e os direitos dos titulares. Além de realizar uma análise da responsabilidade civil das empresas em casos de vazamentos de dados pessoais, considerando a conduta adotada pelas empresas na proteção dessas informações e os possíveis danos causados aos titulares dos dados. Serão também destacadas as medidas preventivas que as empresas devem adotar para evitar vazamentos, como a implementação de políticas de segurança da informação e o treinamento de funcionários. Além disso, será examinada de forma lacônica a aplicação coercitiva às empresas que descumprirem a LGPD, através do entendimento jurisprudencial e doutrinário de julgados nos tribunais brasileiros. A pesquisa realizada evidencia que apesar da LGPD representar um marco importante para a proteção de dados no país, sua efetividade esbarra diante de lacunas existentes na legislação, demonstrando uma fragilidade quanto à determinação da culpa, quantificação dos danos e a identificação dos responsáveis.

Palavras-Chaves: LGPD. Vazamento de dados. Responsabilização. Dados pessoais.

ABSTRACT: The protection and security of personal data have become increasingly relevant in contemporary society, especially with the advancement of information and communication technologies. In this context, the leakage of personal data is a growing concern, requiring the judicial power to implement the General Data Protection Law (LGPD), currently in force in Brazil. This article seeks to analyze the civil liability of companies in cases of personal data breaches, within the context of the LGPD. In order to bring more clarity to the proposed topic, the fundamentals of the LGPD and the guidelines established by the legislation for the treatment of personal data will be initially addressed, highlighting the need for protection of this information and the rights of data subjects. In addition to conducting an analysis of the civil liability of companies in cases of personal data breaches, considering the conduct adopted by companies in protecting this information and the potential damages caused to data subjects. Preventive measures that companies should adopt to prevent breaches will also be highlighted, such as the implementation of information security policies and employee training. Furthermore, coercive application to companies that fail to comply with the LGPD will be examined succinctly, through the jurisprudential and doctrinal understanding of judgments in Brazilian courts. The research conducted shows that despite the LGPD representing an important milestone for data protection in the country, its effectiveness is hindered by existing gaps in legislation, demonstrating a fragility regarding the determination of fault, quantification of damages, and identification of those responsible.

Keywords: LGPD. Data leak. Accountability. Personal data.

[1]Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.
[2]Docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.

1 INTRODUÇÃO

Com o avanço da tecnologia e a crescente utilização de dados pessoais por empresas, tornou-se fundamental estabelecer regras e responsabilidades para a proteção dessas informações e, principalmente, para a responsabilização em casos de vazamentos. A LGPD, que entrou em vigor em setembro de 2020, tem como principal objetivo regulamentar o tratamento de dados pessoais, estabelecendo diretrizes e garantias para os titulares desses dados. Dessa forma, as empresas que coletam, armazenam e utilizam informações pessoais devem seguir as diretrizes estabelecidas pela legislação, assegurando a privacidade e a segurança dessas informações.

Além disso, o vazamento de dados pessoais pode levar a consequências graves, como roubo de identidade, fraude financeira e até mesmo prejuízos emocionais, como ansiedade e desconforto gerados pela quebra de privacidade. Ademais, o assunto da responsabilidade civil no vazamento de dados pessoais perpassa diversas áreas do conhecimento, como o direito, a tecnologia da informação e a ética, demandando uma abordagem multidisciplinar para sua compreensão e solução.

No entanto, mesmo com a implementação da LGPD, vazamentos de dados pessoais continuam a ocorrer, o que levanta questões sobre a responsabilidade civil das empresas nesses casos, levando em consideração a conduta adotada pelas mesmas na proteção dessas informações, bem como os possíveis danos causados aos titulares dos dados de ordem material e moral. Todavia, a comprovação da culpa ou negligência da empresa, a demonstração dos danos sofridos e a quantificação das indenizações tornam-se desafios jurisprudenciais complexos.

Portanto, diante do exposto, questiona-se: Como atribuir responsabilidade a empresas prestadoras de serviços que não possuem a posse direta dos dados, mas estão envolvidas no vazamento dessas informações? A LGPD, embora tenha trazido diretrizes e obrigações, ainda apresenta brechas e lacunas que precisam ser preenchidas.

Visando atingir a resposta almejada para a questão cerne deste artigo, a pesquisa será dividida em três capítulos, onde inicialmente serão abordados os fundamentos da LGPD, sua origem, evolução e princípios e os direitos dos titulares dos dados. No segundo capítulo serão analisados os desafios da LGPD e a responsabilização civil diante da ausência de posse direta dos dados das empresas prestadoras de serviços, considerando as particularidades do ambiente digital, além de demonstrar eventuais medidas preventivas e repressivas a essa problemática

Diante dos conceitos e questões analisadas e objetivando uma noção prática do assunto, se faz necessário, ainda que de forma lacônica, analisar os entendimentos jurisprudenciais de

responsabilização civil dos julgados concernentes ao tema. Assim, o último capítulo suscitará os principais julgados concernentes ao tema, onde permitirá compreender como a responsabilidade civil tem sido aplicada diante do vazamento de dados pessoais, contribuindo para a proteção efetiva dos dados dos cidadãos e para estabelecer parâmetros claros de responsabilidade das empresas nesses casos.

A pesquisa obedece ao método qualitativo, sendo realizada por meio de estudos bibliográficos, jurisprudenciais e análise doutrinária.

2 FUNDAMENTOS DA LGPD

2.1 Origem, Evolução e Princípios da Legislação de Proteção de Dados

A Lei Geral de Proteção de Dados Pessoais (LGPD) tem como objetivo garantir o direito à privacidade e à proteção dos dados pessoais dos cidadãos. Além disso, define diretrizes claras para o manuseio de informações dos usuários, visando reforçar a segurança das interações legais e a confiança do indivíduo na gestão de suas informações pessoais, assegurando a liberdade de atuação, a equidade no mercado e a proteção dos vínculos comerciais e de consumo. Ela foi inspirada no Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) em vigência na União Europeia desde 2018 entrando em vigor no no Brasil em setembro de 2020.

De acordo com Oliveira (2020):

> Um dos principais aspectos da LGPD é o consentimento do titular dos dados. As empresas só podem coletar, utilizar ou compartilhar dados pessoais com o consentimento explícito do titular, que deve ser informado de forma clara e específica sobre a finalidade do uso desses dados. (oliveira, 2020)

A LGPD marca um avanço significativo na proteção de dados no Brasil, ao definir direitos e responsabilidades claras tanto para as empresas quanto para os indivíduos titulares dos dados. Seu objetivo é encontrar um equilíbrio entre a proteção da privacidade dos cidadãos e o estímulo à inovação e ao desenvolvimento econômico.

No entanto, segundo Souza e Silva (2019):

> [...] sua implementação enfrenta desafios, como a criação de mecanismos de fiscalização eficientes, a conscientização da população sobre seus direitos e a adaptação das empresas às novas regras. É fundamental que as empresas se adequem à LGPD, implementando medidas de segurança e respeitando a privacidade dos titulares dos dados, para evitar sanções e prejuízos à sua reputação [...] (Souza; Silva, 2019).

A LGPD estabelece diretrizes e princípios para o tratamento de dados pessoais por parte de empresas, organizações e órgãos públicos. Ela define o que são dados pessoais, quais são os direitos dos titulares desses dados e quais são as obrigações das empresas em relação à coleta, armazenamento, uso e compartilhamento desses dados (Oliveira, 2020).

Dentre os princípios estabelecidos pela LGPD, destaca-se o princípio da finalidade, que determina que o tratamento de dados pessoais deve atender a propósitos legítimos, específicos e explícitos, devendo ser realizado de forma compatível com essas finalidades. “Isso significa que as empresas e entidades que lidam com dados pessoais devem coletar apenas as informações necessárias para as finalidades previamente determinadas e informadas aos titulares dos dados, evitando a utilização excessiva ou inadequada das informações" (Teixeira, 2021).

Cabe ressaltar que de acordo com Koga (2021) “o princípio de maior destaque é o da adequação, que estabelece que o tratamento de dados deve ser compatível com as finalidades informadas aos titulares.” Isso implica que as empresas devem utilizar os dados de forma adequada ao contexto em que foram coletados, de modo a evitar qualquer uso indevido ou desproporcional das informações pessoais. A LGPD traz o princípio da transparência, que “determina que as empresas devem adotar medidas claras e transparentes em relação ao tratamento de dados pessoais, informando de maneira clara e acessível aos titulares sobre as práticas de tratamento realizadas” (Koga, 2021).

Outros princípios presentes na LGPD incluem a necessidade, o livre acesso, a qualidade dos dados, a segurança, a prevenção e a não discriminação. Segundo Koga (2021), Todos esses princípios têm como objetivo assegurar que o tratamento de dados pessoais seja realizado de forma ética, responsável e respeitando os direitos fundamentais dos titulares das informações.

Sobre as diretrizes aduz Souza e Silva (2019):

> [...] as diretrizes da LGPD estabelecem os parâmetros para a aplicação e execução da legislação. Elas englobam orientações gerais sobre o cumprimento das disposições legais, como a garantia da segurança dos dados, a prevenção de danos aos titulares, a adoção de medidas para o cumprimento da lei, entre outros aspectos fundamentais para a efetiva aplicação da LGPD (Souza; Silva, 2019).

Portanto, os princípios e diretrizes da LGPD constituem o fundamento para o tratamento ético e responsável das informações pessoais, sendo cruciais para salvaguardar a privacidade e os direitos dos cidadãos em um cenário cada vez mais digital e interligado. A

adesão a esses princípios e diretrizes é essencial para promover uma cultura de respeito à privacidade e à segurança das informações no contexto empresarial e institucional.

Além disso, a LGPD estabelece que as empresas devem adotar medidas de segurança e de prevenção de incidentes para proteger os dados pessoais que possuem. “Elas também devem manter um registro das operações de tratamento de dados e realizar avaliações de impacto sobre a proteção de dados” (Souza; Silva, 2019).

A legislação também institui a figura do encarregado de proteção de dados, "cuja função é assegurar a conformidade com a lei dentro das organizações e servir como elo entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". Esta entidade é encarregada de supervisionar e regulamentar a aplicação da legislação no Brasil.(Souza; Silva, 2019).

As empresas que descumprem a LGPD estão sujeitas a sanções e penalidades, como advertências, multas, bloqueio ou eliminação dos dados pessoais tratados de forma irregular, entre outras. "Essas penalidades variam de acordo com a gravidade da infração, podendo chegar a até 2% do faturamento anual da empresa, limitado a R$ 50 milhões" (Souza; Silva, 2019).

2.2 Direitos dos Titulares de Dados Pessoais

À medida que a tecnologia avança e a preocupação com a privacidade e segurança das informações cresce, os direitos dos titulares de dados pessoais se tornam cada vez mais significativos. Com a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil, esses direitos foram fortalecidos e expandidos, concedendo aos indivíduos um maior controle sobre suas informações pessoais.

Um dos principais direitos garantidos aos titulares de dados pessoais pela LGPD é o direito à informação. Sobre esse direito, reiteram Guimarães e Santos (2021):

> Esse direito à informação permite que os titulares conheçam e compreendam como suas informações estão sendo tratadas, possibilitando uma tomada de decisão consciente sobre o consentimento para o uso de seus dados. Isso significa que as empresas e entidades que coletam dados devem informar de forma clara e transparente sobre a coleta, o armazenamento, o uso e a compartilhamento dessas informações, além de esclarecer as finalidades para as quais os dados serão utilizados. (Guimarães; Santos, 2021).

O direito de acesso, que confere aos titulares o poder de solicitar e obter informações sobre quais dados pessoais estão sendo tratados, a forma como estão sendo utilizados e a quem estão sendo fornecidos, também corresponde a um direito essencial. "Além disso, os titulares têm o direito de receber uma cópia dos seus dados pessoais em formato estruturado e de uso comum, permitindo que possam transferi-los para outra organização, se desejado (Garcia; Nunes, 2021)".

A referida legislação também garante o direito de retificação, possibilitando que os titulares solicitem a correção, atualização ou inclusão de informações incompletas, imprecisas ou desatualizadas que possuam. Neste sentido, reiteram Garcia e Nunes (2021):

Esse direito é fundamental para assegurar que os dados pessoais estejam corretos e fiéis à realidade, evitando prejuízos causados por informações incorretas. A legislação prevê o direito

de eliminação dos dados pessoais, denominado "direito ao esquecimento". Esse direito confere aos titulares a possibilidade de solicitar a exclusão de suas informações, desde que o tratamento não seja necessário para cumprimento de obrigação legal, regulatória ou exercício regular de direitos (Garcia; Nunes, 2021).

Ademais, os direitos assegurados pela LGPD incluem portabilidade, revogação de consentimento e oposição a certos tratamentos de dados, como para marketing direto. Eles visam proteger a privacidade, transparência e segurança no manuseio de informações pessoais, conferindo maior autonomia aos indivíduos. “O cumprimento desses direitos pelas empresas é crucial para construir confiança e respeito com os clientes, promovendo uma cultura de proteção de dados e privacidade” (Garcia; Nunes, 2021).

3 DESAFIOS DA LGPD: TRATAMENTO DE DADOS PESSOAIS, RESPONSABILIDADE CIVIL E MEDIDAS PREVENTIVAS

3.1 Definição e Tipos de Dados Pessoais

A Lei Geral de Proteção de Dados trouxe uma série de implicações e desafios para o tratamento de dados pessoais no Brasil. Antes de discutir os desafios que a LGPD apresenta, é essencial compreender o conceito de dados pessoais, um dos pilares fundamentais da legislação.

De acordo com Diniz (2021):

> Dados pessoais, segundo a LGPD, são informações relacionadas a uma pessoa identificada ou identificável. Isso abrange um amplo espectro de informações, incluindo desde o nome, documento de identificação, endereço, até características físicas, genéticas, culturais e sociais específicas da identidade de uma pessoa física (Diniz, 2021).

A definição de dados pessoais abrange não apenas aqueles que diretamente identificam uma pessoa, como o nome ou o número de identificação, mas também informações que, utilizadas em conjunto ou cruzadas com outras fontes, permitam a identificação de um indivíduo. Dessa forma, “a legislação reconhece a importância de proteger não apenas os dados explícitos, mas também aqueles que podem propiciar a identificação de uma pessoa em seu contexto” (Diniz, 2021).

A Lei Geral de Proteção de Dados (LGPD) estabelece um amplo conjunto de disposições referentes ao tratamento de dados pessoais, considerando as operações realizadas com essas informações, sobretudo no ambiente digital. A legislação brasileira estabelece diversos tipos de tratamento de dados e impõe normas e obrigações específicas para cada um deles, conforme Bioni (2021) aponta:

> **a)Tratamento de dados pessoais:** O tratamento de dados pessoais envolve todas as etapas de coleta, processamento, armazenamento, compartilhamento e descarte de informações

identificáveis de indivíduos. A LGPD estabelece diretrizes para essas operações visando garantir a privacidade e segurança dos dados.

b)Tratamento de dados sensíveis: A LGPD define a categoria de dados sensíveis, que incluem informações sobre origem étnica, crenças religiosas, opiniões políticas, filiação a grupos religiosos, filosóficos ou políticos, informações de saúde ou vida sexual, dados genéticos ou biométricos vinculados a indivíduos. O tratamento desses dados é mais rigoroso, requerendo consentimento específico e destacado do titular, além de estar sujeito a regras de proteção mais rigorosas.

c)Tratamento de dados de crianças e adolescentes: A legislação define regras específicas para o tratamento de dados de crianças e adolescentes, exigindo consentimento destacado e específico para o uso dessas informações, além de medidas para garantir que sejam utilizadas conforme os interesses dos menores.

d)Tratamento de dados para fins de segurança: A legislação aborda o tratamento de dados para garantir segurança física e patrimonial, como por meio de sistemas de monitoramento e controle de acesso. É essencial que esses dados sejam usados exclusivamente para esses propósitos e em conformidade com os princípios da LGPD.

e)Tratamento de dados para fins de cumprimento de obrigações legais ou regulatórias: A LGPD permite o tratamento de dados pessoais para cumprir obrigações legais ou regulatórias do controlador, em processos judiciais, administrativos e arbitrários.

f)Tratamento de dados para realização de estudos por órgãos de pesquisa: Para fins de estudo, realização de estatísticas, por órgãos de pesquisa garantindo, sempre que possível, a anonimização dos dados pessoais (Bioni, 2021).

Todos os processos de tratamento de dados mencionados devem seguir estritamente as orientações da LGPD. Isso engloba a obtenção de consentimento do titular dos dados, a garantia da segurança da informação, o respeito à finalidade da coleta de dados e o acesso transparente dos titulares às suas informações.

É essencial que as organizações estejam atentas a essas determinações, realizando uma análise detalhada de todas as atividades de tratamento de dados que realizam, a fim de assegurar a plena conformidade com a LGPD. A adoção de medidas de segurança da informação, a criação de políticas de privacidade e a capacitação dos colaboradores são algumas das ações necessárias para garantir a conformidade com as disposições da legislação e a proteção efetiva dos dados pessoais (Peck, 2020).

3.1.2 Desafios e Impactos da LGPD para as Empresas

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD) marca uma transformação substancial na forma como as empresas gerenciam informações pessoais. Apesar de ser um marco crucial para resguardar a privacidade dos cidadãos, a implementação dessa legislação traz diversos desafios e impactos para as empresas.

Sobre os desafios e impactos preconiza Doneda et. al., (2020):

> Um dos principais desafios para as empresas é a necessidade de se adequarem às exigências da LGPD. Isso envolve a revisão de políticas de

> privacidade, a implementação de medidas de segurança da informação, a designação de um encarregado de dados (DPO), a realização de avaliações de impacto à proteção de dados, entre outros. Esse processo pode ser complexo e demanda recursos consideráveis. (Doneda et. al., (2020)

Ademais, a legislação também impõe desafios por estabelecer regras rigorosas para a coleta e tratamento de dados, exigindo consentimento explícito, transparência e finalidade específica. Isso influencia diretamente os processos de negócios, demandando revisão nas práticas de coleta, armazenamento e uso de dados. Além disso, a legislação requer investimentos em segurança da informação, como tecnologia e treinamento de funcionários. O descumprimento das normas pode resultar em sanções, incluindo multas e ações judiciais movidas pelos titulares de dados. Isso pode impactar negativamente a reputação e confiança, levando à perda de clientes e oportunidades de negócios.

Para superar esses desafios e minimizar os impactos da LGPD, as empresas precisam adotar uma abordagem proativa em relação à proteção de dados. Isso envolve a revisão e atualização de políticas, procedimentos e tecnologias, bem como a conscientização e o treinamento dos funcionários. Ademais, a criação de uma cultura organizacional voltada à privacidade, a realização de análises de riscos e a parceria com especialistas legais e em segurança da informação são essenciais para garantir a conformidade com a LGPD (Bioni; Dias, 2020).

3.2 Responsabilidade Civil no Vazamento de Dados Pessoais

3.2.1 Conceito de responsabilidade civil

A responsabilidade civil é um tema fundamental no ordenamento jurídico brasileiro. Ela está presente em diversas áreas do direito, desde o direito civil até o direito do consumidor, passando pelo direito ambiental, trabalhista, entre outros. “A sua aplicação

busca assegurar a reparação de danos causados a terceiros e a promoção da justiça nas relações sociais" (Teixeira, 2019).

No direito civil, a responsabilidade civil é regida pelo Código Civil brasileiro, mais especificamente nos artigos 186 e 927. De acordo com esses dispositivos, quem causar dano a alguém, seja por ação ou omissão voluntária, negligência ou imprudência, fica obrigado a reparar o prejuízo causado que pode ser de ordem material e moral. (Teixeira, 2019).

Além disso, a responsabilidade civil também é aplicada em outras áreas do direito. No direito do consumidor, por exemplo, a responsabilidade civil visa proteger os direitos e interesses dos consumidores. “Nesse contexto, a responsabilidade civil se aplica quando um fornecedor de

produtos ou serviços causar danos a um consumidor, sendo obrigado a reparar esses danos" (Teixeira, 2019).

Na conjuntura da responsabilidade civil, é importante ressaltar o conceito de culpa. Segundo Oliveira (2019):

> Para que uma pessoa seja responsabilizada civilmente, é necessário comprovar que ela agiu de forma ilícita ou negligente, ou seja, que houve culpa. No entanto, em algumas situações, a responsabilidade civil pode ser objetiva, ou seja, dispensando a comprovação de culpa, como ocorre em acidentes de consumo, por exemplo (Oliveira, 2019).

Outro ponto relevante é a quantificação dos danos. Ao ser responsabilizado civilmente, o causador do dano deve reparar o prejuízo sofrido pela vítima. "Essa reparação pode ser feita de diversas formas, como pagamento de uma indenização em dinheiro, restituição de bens ou serviços, entre outros" (Oliveira, 2019).

3.2.2 Análise da Responsabilidade das Empresas em Casos de Vazamento de Dados

A responsabilidade civil no vazamento de dados pessoais é um tema cada vez mais relevante hodiernamente. Com o avanço das tecnologias e a crescente utilização da internet, a proteção e privacidade dos dados das pessoas se tornaram uma preocupação constante. Nesse sentido, " a Lei Geral de Proteção de Dados (LGPD) é uma das principais legislações que visa regulamentar essa questão e impor responsabilidades para as empresas que manipulam dados pessoais" (Teixeira, 2019).

A LGPD estabelece que "os titulares dos dados possuem direitos sobre suas informações pessoais, como o direito de acesso, retificação, exclusão, entre outros". Além disso, a lei também "impõe obrigações às empresas, como a necessidade de consentimento explícito para a coleta e uso dos dados pessoais, a adoção de medidas de segurança para proteção desses dados, a notificação imediata em caso de vazamento, entre outras" (Teixeira, 2019).

No contexto do vazamento de dados pessoais, a responsabilidade civil das empresas se estabelece quando ocorre uma violação desses dados. Seja por uma falha de segurança, um ataque cibernético ou qualquer outra forma de acesso não autorizada, a empresa pode ser responsabilizada pelos danos causados aos titulares dos dados. " Esses danos podem ser de ordem moral, patrimonial ou até mesmo à integridade física de uma pessoa" (Oliveira, 2020).

De acordo com Souza e Silva (2019):

> A responsabilização das empresas pelos vazamentos de dados pessoais está fundamentada na teoria da responsabilidade civil objetiva, prevista no Código Civil brasileiro. Segundo essa teoria, basta a comprovação da existência do dano e do nexo de causalidade entre a conduta da empresa e o prejuízo sofrido pelo titular dos dados, sem a necessidade de demonstração de culpa por parte da empresa. Ou seja, a empresa é

> responsabilizada independentemente de ter agido de forma negligente, imprudente ou dolosa (Souza; Silva, 2019).

No entanto, é importante ressaltar que a responsabilidade civil no vazamento de dados pessoais não se limita apenas às empresas. “Profissionais liberais que atuam na área de tecnologia da informação, por exemplo, também podem ser responsabilizados caso tenham participado diretamente ou negligenciado o desenvolvimento ou a segurança do sistema que causou o vazamento" (Souza; Silva, 2019).

Para mitigar esses riscos, as empresas precisam implementar medidas de segurança apropriadas e investir na proteção dos dados pessoais. Souza e Silva aduzem que “é fundamental realizar auditorias internas e contar com especialistas em segurança da informação para garantir a eficácia dessas medidas e estar em conformidade com as normas da LGPD” (Souza; Silva, 2019).

Sendo assim, a responsabilidade civil no vazamento de dados pessoais é um assunto que demanda atenção e cuidado por parte das empresas. A lei brasileira, representada pela LGPD, estabelece direitos e deveres claros para garantir a segurança e privacidade dos dados pessoais. Cabe às empresas se adequarem a essas normas, adotando medidas de segurança adequadas e assumindo os riscos que envolvem o tratamento desses dados. Somente assim

será possível preservar a confiança dos titulares dos dados e evitar danos à reputação e financeiros decorrentes de vazamentos de informações pessoais.

3.2.3 Danos e Impactos para os Titulares de Dados Pessoais

Os danos e impactos para os titulares de dados pessoais são uma preocupação central em relação à proteção de dados e privacidade. Com a crescente coleta, armazenamento e processamento de informações pessoais, especialmente no contexto digital, “os possíveis

riscos associados ao tratamento inadequado ou ilegal desses dados têm sido amplamente destacados, especialmente em virtude de violações de dados e exposições indevidas” (Tartuce, 2021; Melo et. al., 2021).

Tartuce e Melo (2021) entendem ser os principais danos e impactos para os titulares de dados pessoais:

> **a)Violação da privacidade:** Um dos principais impactos para os titulares de dados pessoais é a violação da privacidade. A coleta e o uso indevido de informações pessoais podem expor aspectos íntimos da vida dos indivíduos, violando sua esfera pessoal e gerando desconforto e constrangimento.
>
> **b) Discriminação e preconceito:** O tratamento inadequado dos dados pessoais pode resultar em discriminação e preconceito, já que as informações coletadas podem ser utilizadas de maneira inadequada para tomar decisões que afetam a vida e as

oportunidades dos titulares de dados, como em processos seletivos de emprego, concessão de crédito, acesso a serviços, entre outros.

c) Riscos à segurança: A exposição indevida de dados pessoais pode colocar os titulares em risco de fraudes, golpes e crimes cibernéticos. Dados sensíveis, como informações financeiras, de saúde ou de identificação, quando violados, podem ser explorados por criminosos para atividades ilícitas, gerando prejuízos financeiros e emocionais para as vítimas.

d) Perda de controle sobre as próprias informações: Quando os dados pessoais são coletados e tratados sem consentimento ou em desacordo com os princípios de proteção de dados, os titulares perdem o controle sobre suas informações, criando sentimentos de vulnerabilidade e desconfiança em relação a quem possui esses dados.

e) Impactos psicológicos e emocionais: A exposição indevida de informações pessoais pode gerar impactos psicológicos e emocionais nos titulares, causando ansiedade, estresse, desconfiança e insegurança. A percepção de falta de controle sobre suas informações pode levar a sentimento de impotência e violação (Tartuce, 2021; Melo et. al., 2021).

Diante desses impactos significativos para os titulares de dados pessoais, a proteção adequada das informações pessoais torna-se fundamental. A implementação de medidas eficazes de segurança da informação, políticas de privacidade transparentes, consentimento informado e o respeito aos princípios de minimização e finalidade no tratamento de dados são essenciais para minimizar os riscos e proteger a privacidade e os direitos dos titulares (Melo et. al., 2021).

Desse modo, a proteção dos dados pessoais é crucial para evitar danos e impactos negativos para os titulares. "As empresas e organizações que tratam informações pessoais devem adotar práticas e medidas eficazes de segurança e proteção de dados", a fim de "resguardar a privacidade e os direitos dos indivíduos, promovendo assim um ambiente digital mais seguro e respeitoso" (Mulholland, 2020).

Além dos pontos anteriormente abordados, é importante ressaltar que a LGPD prevê que os titulares de dados pessoais têm o direito de acessar suas informações, corrigi-las, e até mesmo solicitar a exclusão dos dados que não foram coletados em conformidade com a lei. Há também o impacto emocional da violação da privacidade, que pode resultar em danos psicológicos significativos para os titulares de dados. "O medo de ter informações pessoais sensíveis expostas, bem como a sensação de ter a sua privacidade invadida, pode causar um grande impacto no bem-estar emocional dos indivíduos afetados" (Júnior, 2020).

3.3 Medidas Preventivas e Repressivas

3.3.1 Políticas de segurança da informação

A proteção da informação é um elemento essencial para toda empresa, não importando seu porte ou segmento de atuação. "Com o aumento constante de ataques cibernéticos e a crescente preocupação com a proteção de dados, as políticas de segurança da informação

tornaram-se essenciais para proteger ativos críticos e garantir a continuidade dos negócios" (Giacomolli, 2020). Neste cenário, as medidas preventivas e repressivas desempenham um papel crucial na mitigação de riscos e na proteção das informações sensíveis.

Nesta senda Medeiros (2021) preceitua Medidas Preventivas como sendo:

> Conscientização e treinamento: A conscientização dos colaboradores em relação às ameaças de segurança e boas práticas é o primeiro passo para a implementação eficaz de políticas de segurança da informação. Treinamentos regulares e programas de conscientização podem ajudar a reduzir o risco de ataques cibernéticos, fornecendo informações sobre como identificar ameaças, como lidar com e-mails maliciosos, evitar a engenharia social, entre outros.
>
> Políticas de segurança: Estabelecer políticas de segurança da informação claras e abrangentes é essencial para garantir que todos os colaboradores compreendam as práticas recomendadas e as diretrizes para o uso seguro de dados e sistemas. Isso inclui políticas de acesso, uso de dispositivos pessoais, senhas, entre outros.
>
> Controles de acesso: A implementação de controles de acesso tem como objetivo garantir que apenas pessoas autorizadas tenham acesso a informações confidenciais. Isso pode ser alcançado por meio de autenticação multifatorial, gerenciamento de identidade e acesso, e revisões periódicas das permissões de acesso.
>
> Criptografia de dados: A criptografia de dados em trânsito e em repouso é uma prática recomendada para proteger informações confidenciais contra acessos não autorizados. Isso garante que mesmo em caso de vazamento de dados, as informações permaneçam ilegíveis para os invasores (Medeiros, 2021, p. 09).

De acordo com Teffé e Viola (2020) são Medidas repressivas:

> Monitoramento contínuo: A implementação de sistemas de monitoramento contínuo permite que a equipe de segurança da informação identifique e responda rapidamente a atividades suspeitas ou não autorizadas nos sistemas. Isso inclui a detecção de tentativas de logins não autorizados, tráfego de rede anômalo, entre outros.
>
> Resposta a incidentes: Ter um plano eficaz de resposta a incidentes é crucial para lidar com situações emergenciais, como violações de dados, ataques de ransomware, entre outros. A capacidade de responder rapidamente a incidentes e minimizar o impacto é fundamental para reduzir os danos.
>
> Sistemas de backup e recuperação: Implementar sistemas de backup e recuperação de dados robustos é essencial para garantir a disponibilidade e integridade das informações em caso de incidentes de segurança, como ransomware, exclusão acidental ou corrupção de dados.
>
> Forense digital: Em caso de violação de dados, a análise forense digital é essencial para investigar as causas do incidente, identificar o escopo do ataque e coletar evidências para suportar ações legais ou regulatórias (Teffé; Viola, 2020, p. 13).

Desse modo, as políticas de segurança da informação devem ser abrangentes, combinando medidas preventivas e repressivas para garantir a proteção eficaz dos ativos de informação da organização. “A implementação dessas políticas exige um compromisso contínuo e investimento em tecnologias e práticas de segurança, mas é essencial para minimizar riscos, proteger a reputação da marca e garantir a confiança dos clientes e parceiros de negócios" (Giacomolli, 2020).

3.3.2 Treinamento de funcionários

"Com a entrada em vigor da LGPD, as empresas passam a ser responsáveis pela proteção e tratamento adequado dos dados pessoais, sob pena de sofrerem sanções e medidas de responsabilização civil em caso de descumprimento da lei" (Tasso, 2020).

Dessa forma, é essencial que as organizações invistam em treinamentos específicos para seus colaboradores, a fim de garantir que todos compreendam as exigências da LGPD e estejam preparados para lidar com as responsabilidades associadas. "O treinamento deve abranger não apenas a equipe de tecnologia da informação, mas também funcionários de todos os setores da empresa que lidam com dados pessoais, como recursos humanos, marketing, vendas, jurídico, entre outros" (Tasso, 2020).

De acordo com Tasso (2020):

> Os treinamentos devem abordar a importância da proteção de dados pessoais, os direitos dos titulares das informações, os princípios da LGPD, as obrigações da empresa em relação ao tratamento de dados pessoais, as medidas de segurança necessárias para proteger as informações, as consequências do descumprimento da lei e os procedimentos a serem adotados em caso de incidentes de segurança ou violações de dados (Tasso, 2020).

Assim, segundo o autor, é fundamental que os funcionários compreendam a importância de adotar uma cultura de privacidade e segurança da informação em todo o ambiente de trabalho. Isso inclui a adoção de políticas de segurança da informação, o uso adequado de senhas e sistemas de autenticação, a restrição de acesso às informações

confidenciais, a adoção de medidas de criptografia, entre outras práticas recomendadas (Tasso, 2020).

Neste sentido Maimone (2020) enfatiza que:

> Outro ponto relevante é que os treinamentos devem ser adaptados à realidade de cada organização, levando em consideração seus processos, sistemas e fluxos de trabalho específicos. Além disso, é importante que os treinamentos sejam realizados de forma contínua, para garantir que os colaboradores estejam sempre atualizados em relação às melhores práticas de segurança e em conformidade com a LGPD, que está sujeita a atualizações e ajustes (Maimone, 2022).

Portanto, os treinamentos de funcionários para lidar com a LGPD devem ser vistos como investimentos essenciais para as empresas, uma vez que contribuem para a construção de uma cultura organizacional voltada para a proteção de dados, a minimização de riscos e a prevenção de sanções e medidas de responsabilização civil. "Além disso, demonstram o comprometimento da empresa com a transparência e a privacidade, fatores que podem influenciar positivamente a confiança dos clientes e parceiros de negócios" (Maimone, 2022).

4. ANÁLISE JURISPRUDENCIAL

4.1 Brevíssimas Considerações Jurisprudenciais da Responsabilização das Empresas nos Casos de Vazamento de Dados

Em conclusão, a jurisprudência relacionada à responsabilidade civil em casos de vazamento de dados tem sido crucial para a consolidação dos direitos dos titulares, promovendo a efetiva proteção dos dados pessoais e estimulando as empresas a adotarem medidas preventivas

e reparadoras. Através dessas decisões, os tribunais têm demonstrado a importância de se garantir a segurança e privacidade das informações pessoais, bem como a necessidade de responsabilização das empresas em caso de violação da LGPD.

A atuação jurisdicional relacionada à responsabilidade civil em casos de vazamento de dados tem se mostrado crescente nos tribunais em todo o país, à medida que a proteção de dados pessoais se torna uma preocupação latente. As decisões judiciais em torno desses casos têm o papel crucial de estabelecer os limites, a responsabilidade e as consequências para as empresas que negligenciam a proteção dos dados pessoais, bem como para os titulares dos dados afetados.

Em geral, as decisões têm apontado para a responsabilidade das empresas em adotar medidas de segurança adequadas para proteger os dados pessoais e em comunicar os titulares e as autoridades em caso de vazamentos. Além disso, há jurisprudência consolidada que reconhece o direito dos titulares dos dados à reparação por eventuais danos morais e materiais decorrentes do vazamento.

É importante ressaltar que a jurisprudência relacionada à responsabilidade civil em casos de vazamento de dados tem se pautado pela interpretação da LGPD e por princípios gerais do direito, como a responsabilidade objetiva das empresas em casos de danos causados por vazamento de dados pessoais. A atuação do Poder Judiciário tem sido essencial para garantir a eficácia da LGPD e para assegurar a proteção dos direitos dos titulares dos dados.

Além disso, a jurisprudência tem tido um papel fundamental na delimitação dos critérios para a fixação de indenizações em casos de vazamento de dados, considerando a extensão do dano, a gravidade da conduta da empresa, a culpa e o nexo causal. A partir desse direcionamento jurisprudencial, as empresas têm sido orientadas a adotar medidas de prevenção e reparação de danos para evitar a responsabilização civil.

Por se tratar de um tema atual, a jurisprudência relacionada à responsabilidade civil em casos de vazamento de dados pessoais tem sido moldada por decisões judiciais emblemáticas que estabelecem parâmetros para a aplicação da LGPD.

O Tribunal de Justiça de São Paulo tem proferido decisões importantes no sentido de responsabilizar as empresas por vazamento de dados, tais como Acórdão nº 1005140-96.2019.8.26.0292, que reconheceu o direito à indenização por danos morais em caso de vazamento de dados pessoais, considerando a violação da intimidade e privacidade dos titulares. Outro ponto relevante é que a jurisprudência também tem abordado a responsabilidade das empresas no ressarcimento de danos materiais decorrentes do vazamento de dados. Nesse sentido, o Tribunal de Justiça do Paraná, por meio do Acórdão nº 1581673-32.2016.8.16.0001, confirmou a

condenação de uma empresa ao pagamento de indenização por prejuízos materiais relacionados ao uso indevido de informações pessoais.

A Terceira Turma do Superior Tribunal de Justiça tem reforçado a responsabilidade das empresas diante de vazamentos de dados e uso inadequado por terceiros.

Segundo o entendimento adotado, as instituições financeiras são responsáveis pelo vazamento de dados pessoais sigilosos dos consumidores, relacionados a suas operações e serviços bancários, quando estes são obtidos por criminosos para a prática de fraudes, como o conhecido "golpe do boleto". (Recurso Especial nº. 2.077.278). Conforme a Relatora, Min. Nancy Andrighi, "O tratamento indevido de dados pessoais bancários configura defeito na prestação de serviço, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor".

Por outro lado, de acordo com o julgamento do Agravo em Recurso Especial nº. 2.130.619-SP, a Segunda Turma do Superior Tribunal de Justiça adota o entendimento de que, em casos de vazamento de dados, é imprescindível a comprovação do dano. Segundo o relator, Ministro Francisco Falcão, "O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações." No entanto, tratamento diferenciado deve ser dado aos dados sensíveis, relativamente à saúde, orientação sexual ou religião, conforme observado no referido acórdão, nos quais o dano é presumido.

Outro ponto de destaque é que, em caso de vazamento de dados com fins lucrativos, também há uma tendência de reconhecimento do dano presumido, conforme julgamento do REsp 1.758.799, a Min. Nancy Andrighi assevera que "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. Hipótese em que se configura o dano moral in re ipsa."

Em conclusão, a jurisprudência relacionada à responsabilidade civil em casos de vazamento de dados tem sido crucial para a consolidação dos direitos dos titulares, promovendo a efetiva proteção dos dados pessoais e estimulando as empresas a adotarem medidas preventivas e reparadoras. Através dessas decisões, os tribunais têm demonstrado a importância de se garantir a segurança e privacidade das informações pessoais, bem como a necessidade de responsabilização das empresas em caso de violação da LGPD.

CONSIDERAÇÕES FINAIS

Ao longo deste artigo, foi explorada a questão da responsabilidade civil no vazamento de dados pessoais à luz da LGPD. Inicialmente foram suscitadas as bases legais da LGPD e as diretrizes estabelecidas pela legislação no que tange à proteção de dados pessoais. Em seguida, foram analisadas as diferentes modalidades de responsabilidade civil aplicáveis em casos de vazamento de dados, destacando a responsabilidade objetiva e subjetiva.

Também foi abordada a necessidade de reparação de danos morais e materiais decorrentes de violações à LGPD, assim como a importância da comprovação do nexo causal e do dolo ou culpa para a caracterização da responsabilidade civil. Também foram discutidos

os impactos do vazamento de dados para os titulares, bem como as medidas preventivas que as empresas devem adotar para mitigar os riscos de vazamento de dados e evitar a responsabilização.

Desse modo, a presente pesquisa versa contribuir para a compreensão aprofundada da responsabilidade civil no contexto do vazamento de dados pessoais, sobretudo diante da entrada em vigor da LGPD. Ao abordar as nuances da responsabilidade civil e suas implicações no âmbito da proteção de dados, este artigo oferece um panorama abrangente das questões jurídicas e dos desafios enfrentados pelas empresas e pelos titulares de dados. Ademais, ao discutir as jurisprudências relacionadas à responsabilidade civil em casos de vazamento de dados resta evidenciada a interpretação e aplicação da legislação na prática, contribuindo para o conhecimento dos profissionais de direito, pesquisadores e demais interessados no tema.

Para futuras pesquisas, é sugerido o aprofundamento na análise das ações judiciais relacionadas à responsabilidade civil em vazamento de dados, bem como a realização de estudos comparativos entre a LGPD e outras legislações internacionais de proteção de dados, visando identificar as melhores práticas e contribuir para a evolução do marco legal brasileiro.

REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. 3. ed. Rio de Janeiro: Grupo GEN, 2021. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 16/02/2024.

BIONI, Bruno Ricardo; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Orientador: Daniel Dias. 2020. 23 p. Tese de Doutorado, Rio de Janeiro, 2020. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/. Acesso em: 16/02/2024.

CASTRO, Luiz Felipe. Maior vazamento de dados pessoais do país expõe riscos da era digital. A ação mostrou que as empresas não estão preparadas para fugir da ação dos hackers. 12 fev. 2021. Atualizado em: 12 mar. 2021. Disponível em: https://veja.abril.com.br/tecnologia/maior-vazamento-de-dados-pessoais-do-paisexpoe-riscos-da-era-digital/. Acesso em: 16/02/2024.

DINIZ, Maria Helena. Curso de direito civil brasileiro: responsabilidade civil. 36. ed. São Paulo: Saraiva, 2021. v. 7. ISBN 9786555598650. Disponível em: https://integrada.minhabiblioteca.com.br/books/9786555598650. Acesso em: 16/02/2024.

DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Grupo GEN, 2020. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16/02/2024.

GARCIA, Maria Carolina Brunharotto; NUNES, Paula Freire Santos Andrade. Responsabilidade Civil, Dano Moral e Tratamento de Dados Pessoais: estudo prático de jurisprudência sobre como se dará o dever de indenizar. 03 ago. 2021. Disponível em: https://www.migalhas.com.br/depeso/349526/responsabilidade-civil-dano-moral-etratamento-de-dados-pessoais. Acesso em: 16/02/2024.

GIACOMOLLI, Caroline Mrack. A tutela da boa-fé objetiva na lei geral de proteção de dados: algumas considerações. 2020. 25 p. Artigo (Graduação em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS, Porto Alegre, 2020.

GUIMARÃES, Anna Luísa; SANTOS, Isabela Maria Rosal. Vazamento em ministério: instituições públicas sabem lidar com dados sensíveis? 17 dez. 2021. Disponível em: https://www1.folha.uol.com.br/tec/2022/01/pf-ainda-investigaataques-hacker-e-megavazamento-de-dados-um-ano-depois.shtml. Acesso em: 16/02/2024.

HOBBES, T. Leviatã ou matéria, forma e poder de um Estado eclesiástico e civil. Coleção Os Pensadores. (1º volume). 4ª Edição, Nova Cultural, 1988.

JÚNIOR, Marcos Ehrhardt. A LGPD finalmente entrou em vigor. E agora? Migalhas. 8 dez. 2020. Disponível em: https://www.migalhas.com.br/depeso/337481/a-lgpd-finalmenteentrou-em-vigor--e-agora. Acesso em: 16/02/2024.

KOGA, Bruno Yudi Soares. Indenização por vazamento de dados pessoais na jurisprudência do TJ/SP. Todos os dias surgem notícias de vazamentos de dados pessoais, mas como o Tribunal de Justiça de São Paulo tem lidado com as ações indenizatórias? 28 set. 2021. Disponível em: https://www.migalhas.com.br/depeso/352361/indenizacao-por-vazamento-de-dadospessoais-na-jurisprudencia-do-tj-sp. Acesso em: 16/02/2024.

LIMA, Cintia Rosa Pereira de. In I Simpósio de Responsabilidade Civil e Proteção de Dados. Evento realizado pelo Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC. Agosto, 2020. Disponível em < https://www.youtube.com/watch?v=igbbxkbqeKI&t=4213s>. Acesso em 16/02/2024.

MAIMONE, Flávio Henrique Caetano de Paula. Responsabilidade civil na LGPD (recurso eletrônico]: efetividade na proteção de dados pessoais / Flávio Henrique Caetano de Paula Maimone. - Indaiatuba, SP : Editora. Foco, 2022

MEDEIROS, Thais Carneiro. Responsabilidade Civil pela Violação ao Direito à Proteção de Dados Pessoais / Thais Carneiro Medeiros. – 2021.

MELO, Maria Heloísa Chiaverini, et al. Uma análise de conjuntura da Lei Geral de Proteção de DAdos Pessoais (LGPD): Tramitação, aprovação e vigência. Revista Humanidades e Inovação, [s. l], v. 8, n. 47, p. 56-70, jun. 2021.

MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? Migalhas. 30 jun. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-ofundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais-culpaou-risco. Acesso em: 16/02/2024.

OLIVEIRA, Gabriel Prado Souza de. Sigilo de Dados no Brasil: da Previsão Constitucional à Nova Lei Geral De Proteção De Dados Pessoais. São Paulo, 2019. Disponível em ‹https://ambitojuridico.com.br/cadernos/direito-constitucional/sigilo-de-dados-no-brasil-da-previsao-constitucional-a-nova-lei-geral-de-protecao-de-dados-pessoais/›. Acesso em 12/08/2023.

PECK, Patrícia. Proteção de dados pessoais. 2. ed. São Paulo: Saraiva, 2020. ISBN 9788553613625. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553613625/. Acesso em: 08 out. 2022.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. Pensar, Revista de Ciências Jurídicas. Fortaleza, 2019.

TARTUCE, Flávio. Responsabilidade Civil. – 3. ed. – Rio de Janeiro: Forense, 2021.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. Cadernos Jurídicos: Direito Digital e proteção de dados pessoais, São Paulo, ano 21, n. 53, São Paulo, jan./mar.2020, p. 97-116

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com., Rio de Janeiro, ano 9, n. 1, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 16/02/2024.

TEIXEIRA, João Pedro Ferraz. LGPD 101 - Comentários à Lei Geral de Proteção de Dados. 2019. Disponível em: https://joaopfteixeira.jusbrasil.com.br/artigos/753086549/lgpd-101-comentarios-a-lei-geral-de-protecao-de-dados›. Acesso em 12/08/2023.

TEIXEIRA, Tarcísio. A LGPD e o e-commerce. 2. ed. São Paulo: Saraiva, 2021. ISBN 9786555598155. Disponível em: https://integrada.minhabiblioteca.com.br/books/9786555598155. Acesso em: 16/02/2024.

TERRA, Aline de Miranda. GUEDES, Gisela Sampaio da Cruz. TEPEDINO, Gustavo (Orgs.). Responsabilidade Civil. Rio de Janeiro: Forense, 2020.

TROVÃO, Antonio Lucas M.C.; PIETZSCH, Ingo Dieter. Lei Geral de Proteção de Dados e o Direito na Era Digital. Disponível em: https://www.radloff.com.br/lei-geral-de-protecao-de-dados-e-o-direito-na-era-digital/. Acesso em 16/02/2024.