UNIVERSIDADE CESUMAR - UNICESUMAR
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM DIREITO

A RESPONSABILIDADE CIVIL DAS EMPRESAS PELO VAZAMENTO DE DADOS PESSOAIS À LUZ DA LGPD

BHRENDA HYOHANNA DA SILVA ASSIS

MARINGÁ – PR
2025

Bhrenda Hyohanna da Silva Assis

A RESPONSABILIDADE CIVIL DAS EMPRESAS PELO VAZAMENTO DE DADOS PESSOAIS À LUZ DA LGPD

Artigo apresentado ao Curso de Graduação em Direito da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharela em Direito, sob a orientação do Prof. Me. Welington Junior Jorge Manzato.

MARINGÁ – PR

2025

FOLHA DE APROVAÇÃO

BHRENDA HYOHANNA DA SILVA ASSIS

A RESPONSABILIDADE CIVIL DAS EMPRESAS PELO VAZAMENTO DE DADOS PESSOAIS À LUZ DA LGPD

Artigo apresentado ao Curso de Graduação em Direito da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharela em Direito, sob a orientação do Prof. Me. Welington Junior Jorge Manzato.

Aprovado em: ____ de _____ de _____.

BANCA EXAMINADORA

_____

Nome do professor – (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

A RESPONSABILIDADE CIVIL DAS EMPRESAS PELO VAZAMENTO DE DADOS PESSOAIS À LUZ DA LGPD

Bhrenda Hyohanna da Silva Assis

RESUMO

Este estudo analisa a responsabilidade civil das empresas diante de vazamentos de dados pessoais à luz da Lei Geral de Proteção de Dados Pessoais (LGPD). O objetivo é identificar os fundamentos legais aplicáveis, os limites de atuação empresarial e os mecanismos de reparação ao titular dos dados. A metodologia empregada é descritiva e bibliográfica, com revisão de doutrina, jurisprudência e práticas de governança de dados. Os principais resultados destacam que a LGPD impõe responsabilidades tanto na esfera administrativa quanto na civil, enfatizando a necessidade de medidas de segurança, governança de dados e *accountability*. Conclui-se que a responsabilização pode ocorrer de maneira objetiva ou subjetiva, conforme o contexto, reforçando a importância de planos de conformidade, auditorias periódicas e políticas de proteção de dados para reduzir riscos jurídicos e reputacionais. Recomenda-se a implementação de programas de proteção de dados, treinamentos e mecanismos de controle interno para assegurar a proteção dos titulares.

Palavras-chave: Governança de Dados. Proteção de Dados. Segurança da Informação.

A CIVIL LIABILIY OF COMPANIES FOR DATA BREACHES IN LIGHT OF THE LGPD

ABSTRACT

This article analyzes the civil liability of companies regarding personal data breaches in the light of the Brazilian General Data Protection Law (LGPD). The objective is to identify the applicable legal foundations, the limits of corporate actions and the mechanisms available to data subjects. The research used a descriptive and bibliographic method, with a review of doctrine, court decisions and data governance practices. The main result highlight that the LGPD imposes responsabilities in both the administrative and civil spheres, emphasizing the need for security measures, data governance and accountability. It was concluded that the liability can occur objectively or subjectively, depending on the context, reinforcing the importance of compliance plans, periodical audits and data protection policies to reduce legal and reputational risks. The implementation of data protection programs, training and internal control mechanisms is recommended to ensure the protection of data subjects.

Keywords: Data Protection. Governance Of Data. Information Security.

1 INTRODUÇÃO

A sociedade em geral tem cada vez mais se mostrado conectada ao ambiente virtual, haja vista que, até a poucos anos, a interação virtual aparentava ser algo distante da vivência dos seres humanos, contudo, constata-se a rápida ascensão dos meios digitais, que se tornaram parte do cotidiano da população no mundo todo.

Com a evolução da tecnologia, seu uso propiciou uma interação entre os dispositivos eletrônicos e as pessoas, reproduzindo, cada vez mais, dados que são processados e armazenados inerentes à rotina dos usuários. Entretanto, os que fazem uso do ambiente virtual, por vezes, não possuem qualquer noção acerca da forma como seus dados são coletados, tratados e compartilhados, de modo que tendem a ser vulneráveis, haja vista que qualquer um poderia ter acesso a essas informações pessoais.

Verifica-se que há ausência de limitações na Internet e no ambiente físico, contexto em que a população, de modo rotineiro, sofre com vazamentos de dados pessoais, o que levou o país a enxergar a necessidade de se possuir um amparo legal para tais adversidades. Nesse sentido, em 14 de agosto de 2018, o Presidente Michel Temer (2016-2018) sancionou a Lei nº 13.709, denominada Lei Geral de Proteção de Dados Pessoais (LGPD). A base desta lei está ancorada no Regulamento Geral de Proteção de Dados (GDPR, conforme sigla em inglês) da União Europeia e seu objetivo consiste no preenchimento de lacunas existentes acerca da temática da proteção de dados, tendo sido considerada um marco legal no ordenamento pátrio quanto à tutela de informações dos brasileiros, tais como: nome, endereço, idade, estado civil, situação patrimonial e outros.

No cenário empresarial brasileiro, vazamentos de dados têm acendido debates sobre a *accountability*, sobretudo no que tange a medidas de prevenção e às consequências jurídicas para as organizações, incluindo sanções administrativas, a reparação de danos e a responsabilização civil. Nesse contexto, compreender como a LGPD regula a responsabilização civil das empresas diante de vazamentos de dados é essencial tanto para a prática jurídica quanto para a governança corporativa.

Nesse sentido, tem-se o seguinte problema a ser analisado pelo presente trabalho: de que maneira a LGPD regula a responsabilidade civil das empresas em casos de vazamento de dados pessoais? Quais seriam os efeitos jurídicos decorrentes dessa responsabilização no contexto empresarial brasileiro? No que tange aos objetivos do presente estudo, tem-se por objetivo geral: investigar as obrigações jurídicas impostas pela LGPD no tocante ao tratamento e à segurança dos dados pessoais. São objetivos específicos: examinar a

interpretação atual da jurisprudência brasileira sobre a responsabilidade civil empresarial em casos de vazamento de dados e identificar mecanismos de prevenção e governança de dados adotados pelas empresas para atender à LGPD e evitar sanções.

2 CONTEXTO HISTÓRICO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

De início, destaca-se que, no ordenamento jurídico brasileiro, a proteção de dados foi primeiramente admitida como relacionada ao uso da internet, com previsão expressa na Lei nº 12.965/2014, denominada Marco Civil da Internet. Sancionado pela Presidente Dilma Rousseff (2011-2016), em 23 de abril de 2014, o Marco Civil da Internet foi considerado como legislação pioneira no mundo e trouxe, em seu art. 3º, inc. III, a previsão da criação de uma Lei que tratasse especificamente da temática proteção de dados, o que só veio a ocorrer em 10 de julho de 2018, com a sanção, pelo então Presidente Michel Temer (2016-2018) da Lei Geral de Proteção de Dados Pessoais (LGPD).

Embora em vigor desde 2014, o Marco Civil da Internet só obteve sua regulamentação no ano de 2016, por meio do Decreto Presidencial nº 8.771, o qual preservou e complementou as diretrizes de privacidade e liberdade de expressão, trazendo a seguinte previsão em seu art. 13, inc. IV:

> Art. 13 - Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: [...]
> IV - O uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes (Brasil, 2016).

No que concerne à origem da LGPD, está se deu na Câmara dos Deputados, por meio do Projeto de Lei da Câmara nº 053/2018, de autoria do Deputado Federal Milton Monti (SP), sendo escolhido relator da matéria o Deputado Nelson Marchezan Junior (RS). Durante a tramitação, foram realizadas duas consultas públicas, por meio das quais foram recebidas mais de 2.500 (duas mil e quinhentas) sugestões de personalidades nacionais e internacionais. A matéria foi votada e aprovada no plenário da Câmara em 29 de maio de 2018, seguindo, então, para o Senado Federal, em que tramitou em conjunto com os Projetos de Lei do Senado nº 330/2013, 131/2014 e 181/2014 (BRASIL, 2018).

No Senado, o Projeto foi relatado pelo Senador Antônio Carlos Valadares (SE), sendo votado e aprovado em plenário na data de 10 de julho do mesmo ano, seguindo para a sanção presidencial, o que se deu em 14 de agosto daquele ano. Cumpre destacar que o projeto original, aprovado pelo Poder Legislativo e sancionado pelo Poder Executivo, previa um período de *vactio legis* de 18 (dezoito) meses. Todavia, em 7 de dezembro de 2018, o Presidente Michel Temer (2016-2018) editou a Medida Provisória 869/2018 (posteriormente convertida na Lei nº 13.853/2019), alterando este prazo para 24 (vinte e quatro) meses (BRASIL, 2018; 2019).

A contextualização diante da qual o projeto da LGPD aprovado esclarece a sua rápida tramitação no Congresso Nacional. A matéria foi votada em regime de urgência em ambas as Casas Legislativas, sendo aprovada na Câmara em maio e, no Senado, em julho de 2018. Um dos motivos para a urgência seria o fato de o Projeto de Lei do Deputado Milton ter sido apensado a outras proposições já em tramitação. Outro motivo está relacionado aos escândalos de privacidade que ocorreram envolvendo a rede social *Facebook*, a consultoria *Cambridge Analytics*, o *Brexit* e o Serviço Federal de Processamento de Dados (Serpro).

De acordo com Roncolato (2018, [s.p.]):

> [...] a *Cambridge Analytics* era uma empresa privada britânica de consultoria comercial e política que fora criada em 2013. Desde sua criação, ela tinha a finalidade principal de atuar em campanhas eleitorais, coletando, tratando e analisando dados de usuários de redes sociais, principalmente o *Facebook*. Por meio da análise dos dados pessoais e do comportamento dos usuários nas redes, a empresa identificava o público-alvo de suas ações e direcionava propagandas para essas pessoas, com o intuito de arrebanhar eleitores para determinados candidatos. A *Cambridge Analytics* ficou famosa por sua atuação na campanha eleitoral do ex-presidente dos Estados Unidos, Donald Trump, e também por suas ações no *Brexit*. Ela foi acusada de coletar, usar e vender indevidamente dados de milhões de estadunidenses bem como de viralizar *fake news* com o fim de formar opiniões e moldar o pensamento dos usuários da Internet.

No Brasil, houve um caso semelhante que também despertou a atenção: o suposto estratagema de venda de dados pessoais de brasileiros por funcionários do Serviço Federal de Processamento de Dados (Serpro). Segundo reportagem do portal G1, datada de 2018, e assinada pela jornalista Marilia Marques (2018, [s.p.]), “dados como endereço, nome da mãe, sexo e data de nascimento de inscritos no Cadastro de Pessoa Física (CPF) e Jurídica (CNPJ) estavam sendo comercializados por até R$ 273 mil”.

A partir desse episódio, as pessoas que tinham receio quanto a ter suas atividades vasculhadas na Internet ou, simplesmente, quem não gostaria de se expor e compartilhar

dados pessoais começou a se sentir inseguro e desconfiado. Tal cenário de insegurança e desconfiança se deu, principalmente, pelo fato de existir quem afirme que qualquer um que possua interesse e capacidade poderia descobrir o que os outros fazem em seu computador ou *smartphone*. De acordo com Leonardi (2005, p. 7):

> [...] o fato é que a disseminação de informações de modo instantâneo entre milhões de pessoas não traz apenas benefícios. Como qualquer nova tecnologia, a Internet também criou oportunidades inéditas para a prática de atos ilícitos. Entre esses atos ilícitos, podemos ter a violação de nosso direito de privacidade, assim como o uso indevido de nossos dados pessoais por corporações nacionais e internacionais bem como por órgãos governamentais.

É possível observar que as diversas mudanças pelas quais passou a humanidade compeliram o ordenamento pátrio a buscar uma nova maneira de lidar com os riscos e com as chances que as inovações ocasionam. O fato é que os avanços da tecnologia já levaram à elaboração de diplomas normativos, como o Regulamento Geral de Dados (*General Data Protection Regulation* – GDPR), da União Europeia e o Marco Civil da Internet, do Brasil, além da publicação de diversas obras doutrinárias acerca do tema.

Conforme Vieira (2019, p. 13):

> [...] diante desse quadro, a segurança de dados e a privacidade passaram a ser pautas recorrentes, recaindo uma pressão na classe política no sentido de regulamentar essas questões, já que não havia no país uma legislação com objetivo específico de tutelar os dados dos usuários e definir responsabilidades relativas ao tratamento destes, em que pesem as legislações esparsas, como o Código de Defesa do Consumidor (CDC), o Código Civil (CC) e a Constituição, que já traziam dispositivos de tutela de dados.

Verifica-se, pois, que foi este o cenário que levou à criação da LGPD, sancionada em 14 de agosto de 2018 pela Presidência da República. Destaca-se que, à época, sob a chefia de Michel Temer, o Poder Executivo vetou diversos dispositivos da lei, dentre eles, o que criava a Autoridade Nacional de Proteção de Dados (ANPD). Temer alegou que havia vício de iniciativa na criação da ANPD, cuja atribuição seria fiscalizar a aplicação da lei. Entretanto, quatro meses depois, em 27 de dezembro daquele ano, o então mandatário recriou o órgão por meio da Medida Provisória nº 869, a qual também alterou o início da vigência da nova lei para vinte e quatro meses após sua publicação no Diário Oficial da União (Brasil, 2018).

2.1 PRINCÍPIOS DA LGPD EM RELAÇÃO AO VAZAMENTO DE DADOS PESSOAIS

Com o objetivo de controlar o tratamento de dados pessoais, a fim de que os indivíduos possam desempenhar de modo pleno seu poder de autodeterminação informativa, ao longo do tempo, a doutrina criou diversos princípios norteadores da prática.

De acordo com Doneda (2011, p. 98):

> [...] não obstante a clara evolução do tema durante tal período, é possível agrupar materialmente alguns objetivos e linhas de atuação principais, presentes em diversos ordenamentos, em diversos graus. Através disso, percebe-se uma forte convergência do tratamento da matéria nos diferentes ordenamentos rumo à consolidação de alguns princípios básicos e à vinculação cada vez mais estreita com os direitos fundamentais e a proteção da pessoa.

Tais princípios se originaram em leis de primeira e segunda geração, podendo, inclusive, reportar-se aos mesmos princípios que nortearam o *National Data Center* na década de 1960. De modo sucinto, são eles: princípio da publicidade ou transparência, princípio da exatidão, princípio da finalidade, princípio do livre acesso e princípio da segurança lógica e física. Pelo **princípio da publicidade ou transparência**, entende-se que eventual existência de banco de dados deve ser de conhecimento público, o que deve ocorrer por meio de autorização estatal prévia para funcionamento, de uma comunicação às autoridades sobre sua existência ou, ainda, mediante pareceres periódicos de livre acesso ao público.

Já por meio do **princípio da exatidão**, verifica-se a necessidade de manutenção da qualidade dos dados. Consiste na exigência de que as informações de um banco de dados espelhem a realidade, o que se traduz pela imprescindibilidade de manutenção do devido cuidado quanto à coleta, ao tratamento e à correção, além de revisões periódicas, de acordo com a precisão. Em consonância com o **princípio da finalidade,** observa-se que o uso de dados pessoais deve, de modo obrigatório, seguir os fins anunciados ao cedente antes da coleta. Tal obrigatoriedade é de suma importância prática, haja vista que limita a transferência de dados pessoais a terceiros, sendo possível, até mesmo, construir um critério de valoração quanto a ser ou não razoável o uso de certos dados para finalidades diferentes daquela para a qual foram coletados (o que poderia resultar em abusos).

A seu turno, o **princípio do livre acesso** garante a total disponibilização dos dados armazenados aos seus proprietários, assegurando a obtenção de cópia dos registros e, em conformidade com o princípio da exatidão, a correção de informações errôneas ou desatualizadas. Tem-se, ainda, o **princípio da segurança lógica e física**, o qual propicia a

proteção dos dados contra o extravio, a destruição, a alteração, a cessão ou o acesso não autorizado pelos legítimos proprietários, tanto no ambiente físico quanto no *ciberespaço*. Conforme leciona Doneda (2011, p. 100):

> [...] tais princípios passaram a ser encontradas em diversas normativas sobre a proteção de dados, e passaram a ser chamados de *Fair Information Principles*. Esse núcleo comum se consolidou como tal principalmente a partir da Convenção de Strasbourg, e das *guidelines* da OCDE, no início da década de 80.

Mais recentemente, o Brasil, por meio da implementação da LGPD passou a tratar o tema de modo claro, estabelecendo, no art. 6º da referida lei, que as atividades relacionadas ao tratamento e à proteção de dados pessoais deverão se pautar na boa-fé e em outros 10 (dez) princípios que se correlacionam, distribuídos em seus incisos (Brasil, 2018). Antes de adentrar propriamente no estudo dos referidos princípios, é necessário compreender que, ao mencionar esta forma do Direito, está a se falar do sustentáculo teórico e dos valores ante os quais o legislador fixou sua base quando da criação da norma.

Conforme definição de Plácido e Silva (2003, p. 639), os:

> [...] princípios, no plural, significam as normas elementares ou os requisitos primordiais instituídos como base, como alicerce de alguma coisa. Revelam o conjunto de regras ou preceitos, que se fixam para servir de norma a toda espécie e ação jurídica, traçando, assim, a conduta a ser tida em qualquer operação jurídica. Exprimem sentido mais relevante que o da própria norma ou regra jurídica. Mostram-se a própria razão fundamental de ser das coisas jurídicas, convertendo-as em perfeitos axiomas. Significam os pontos básicos, que servem de ponto de partida ou de elementos vitais do próprio Direito.

Verifica-se, assim, que é de grande relevância o estabelecimento pela legislação pátria de princípios inerentes ao tratamento de dados. Todavia, em se tratando de um setor totalmente interligado com o mundo digital e tecnológico, existe o risco de criação de um ordenamento juridicamente rígido que acarrete uma paralisação prematura da nova normativa.

Desse modo, é possível constar que, ante a questão exposta, o legislador, ao instituir princípios no que tange ao tratamento de dados, tentou estabelecer uma norma capaz de se adaptar a um ambiente dinâmico, de modo a conferir maior validade temporal à lei.

Feita esta breve explanação introdutória, é crucial examinar individualmente os princípios jurídicos atinentes à atividade de tratamento de dados expressos na LGPD. São eles: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência;

segurança; prevenção; não discriminação; e responsabilização e prestação de contas. Por força do **princípio da finalidade**, é necessário que o tratamento de dados obtenha um resultado específico e legítimo (Brasil, 2018).

De acordo com Cots e Oliveira (2020, p. 1977), "o princípio da finalidade não vale apenas para limitar o objetivo final do tratamento, mas para tornar previsível o que dele se espera, inviabilizando tratamento posterior desvinculado com a finalidade original".

Assim, é possível citar como situações que constituem exemplos de violação ao referido princípio: participar o proprietário dos dados acerca do destino que será dado aos seus dados ora coletados, qual seja, o para o faturamento de produto ou serviço, mas utilizá-los em campanhas de *marketing*; cientificar o proprietário dos dados de que suas informações serão compartilhadas com a empresa X, mas realizar o compartilhamento com a empresa Y; dizer que os dados não serão copiados, mas fazer cópia dos mesmos; dentre outras situações.

No que concerne ao **princípio da adequação**, este possui relação direta com o princípio anterior, todavia, é diferente, já que aquele tem por objetivo o fim do tratamento. Segundo Cots e Oliveira (2020, p. 1988), "o princípio da adequação tem como objeto o meio, ou seja, o procedimento realizado pelo agente de tratamento para chegar na finalidade pretendida". Nesse sentido, são exemplos de violação ao referido princípio: informar a comunicação com determinados operadores, mas comercializar livremente os dados coletados no mercado; indicar que os dados serão eliminados, mas manter cópia dos mesmos; dizer que os dados serão mantidos em anonimato, mas torna-los públicos, entre outras.

Já, de acordo com o **princípio da necessidade**, é dever do agente de tratamento, ao realizar a atividade, circunscrever-se aos mínimos dados necessários, de acordo com Cots e Oliveira (2020, p. 1988), "descartando o que for em excesso e desnecessário".

Como exemplos de ocorrências que violam o supracitado princípio é possível citar: requisitar a cor da pele para faturar produtos ou serviços; pedir que candidato a emprego informe sua orientação sexual ou, ainda, requerer todos os endereços nos quais a pessoa possa ser encontrada, para entrega de produto em apenas um deles etc.

A seu turno, pelo **princípio da não discriminação**, segundo Cots e Oliveira (2020, p. 2002), "há vedação legal de tratar dados para fins discriminatórios ilícitos ou abusivos". Para exemplificar a violação deste princípio, é possível citar as seguintes situações: dispensar empregado em virtude de sua crença religiosa; ofertar produtos ou serviços apenas para pessoas de certa nacionalidade; não permitir o acesso de mulheres a certos produtos ou serviços, entre outras. Destaca-se, ainda, o **princípio da transparência**, o qual, segundo Cots

e Oliveira (2020, p. 2015), “garante ao titular das informações o direito a ter sempre explicações claras, precisas e acessíveis em relação ao tratamento de seus dados pessoais”.

Como exemplos de violações, tem-se os seguintes cenários: a falta de informação acerca da qualificação completa do controlador dos dados; a não descrição da abrangência do tratamento realizado; o não fornecimento fácil de acesso aos dados em tratamento, entre outros. O **princípio da segurança** e o **princípio da prevenção** são princípios complementares, segundo os quais os agentes de tratamento – controlador e operador – possuem o dever de utilizar técnicas que protejam os dados pessoais de eventuais acessos não consentidos pelo proprietário, bem como de ocorrências acidentais ou ilícitas (tais como: perda, alteração ou difusão), que venham a ocasionar dano ao seu titular, tendo sempre o referido princípio como ideal para a preservação, em local seguro, dos dados em tratamento.

Conforme leciona Pestana (2020, p. 07), “deverão ser utilizadas, sempre, técnicas atuais de segurança e procedimentos constantemente aprimorados, com vistas a garantir a manutenção da segurança e prevenção”. Nesse sentido, salienta-se que, por força do referido princípio, os agentes de tratamento são obrigados a fornecerem, continuamente, uma efetiva segurança aos dados, visto que, diante de falha, o operador ou controlador poderão ser responsabilizados, tanto na esfera cível quanto na esfera administrativo.

Já o **princípio da responsabilização e prestação de contas** possui relação com a demonstração, por parte do agente de tratamento, de que adotou medidas eficazes e capazes de comprovar a disciplina e o cumprimento das normas de proteção de dados pessoais.

Segundo Pestana (2020, p. 8):

> [...] o agente não só deverá comprovar ter adotado os procedimentos e praticado os atos permitidos pela LGPD, como também que todos eles tenham tido a eficácia esperada, pois caso contrário, ainda que tenha agido com boa-fé, ocorrido o descumprimento das normas de proteção de dados, haverá ofensa ao Princípio da Responsabilização e da de Contas.

Destaca-se, ainda, que o referido princípio diz respeito, inclusive, à eficácia das próprias medidas de segurança. A seu turno, o **princípio da qualidade dos dados** consiste em uma garantia aos titulares, acerca da exatidão, da clareza e da atualização dos dados, consoante a necessidade, e para fins de cumprimento quanto à finalidade de seu tratamento, haja vista que dados de qualidade duvidosa podem colocar em risco a integralidade da atividade de tratamento de dados pessoais e, desse modo, fazer com que não sejam alcançadas as finalidades desejadas.

Por fim, tem-se o **princípio do livre acesso**, considerado um dos princípios centrais da LGPD, que, segundo Cots e Oliveira (2020, p. 2000), “garante aos titulares dos dados o acesso facilitado acerca do modo e do período de tratamento, assim como sobre a totalidade de suas informações pessoais”. Ressalta-se que, em geral, esta atividade é desenvolvida pelo encarregado definido pelo controlador dos dados.

2.2 VAZAMENTO DE DADOS PESSOAIS E A LGPD

Na atualidade, a vida cotidiana das pessoas é marcada pela presença constante da Internet e, frequentemente, de forma inconsciente, os indivíduos acabam revelando dados e informações privadas a diversos destinatários. Além disso, grandes empresas do mercado tecnológico, como o *Google*, o *WhatsApp* e o *Facebook* oferecem acesso gratuito às suas plataformas e seus aplicativos, recebendo em troca os dados e as informações pessoais dos usuários como forma de compensação.

Acerca do assunto, leciona Rodotá (2018, p. 15) que:

> [...] as informações fornecidas pelas pessoas para que obtenham determinados serviços são tais em quantidade e qualidade, que possibilitam uma série de usos secundários, especialmente lucrativos para os gestores dos sistemas interativos.

Ao disponibilizar essas informações, os *websites* e aplicativos adquirem acesso a dados detalhados sobre os perfis de cada usuário, incluindo comportamentos de compra, dados pessoais, inclinações políticas, condições financeiras, entre outros aspectos.

A LGPD deve ser implementada em todas as operações que envolvem o tratamento de dados pessoais, realizadas tanto por indivíduos em atividades econômicas quanto por entidades jurídicas, sejam elas de direito público ou privado, independentemente de o armazenamento ser físico ou digital. Portanto, as entidades e corporações devem sofrer sanções civis em razão do descumprimento das normas estabelecidas pela legislação. O proprietário das informações pode enfrentar diversas consequências negativas devido ao vazamento de seus dados pessoais, incluindo a exposição a ataques discriminatórios, a má utilização de suas informações pessoais e o risco de se tornar alvo de fraudes e golpes (BRASIL, 2018).

De acordo com a legislação vigente, em situações de vazamento de informações, os responsáveis pela falha de segurança são os agentes que tratam os dados, especificamente o controlador e o operador. Dessa forma, tanto a empresa quanto os empregados mencionados

deverão responder pela infringência. O controlador é uma das figuras fundamentais no que tange ao manejo de dados pessoais, já que é encarregado das principais decisões relacionadas ao processamento desses dados. Assim, conforme o artigo 5º, inc. VI, da LGPD, o controlador é definido como a "entidade, seja uma pessoa física ou jurídica, pública ou privada, que tem a responsabilidade pelas escolhas sobre o tratamento de dados pessoais" (BRASIL, 2018).

Em relação ao operador, este é considerado um tipo de auxiliar do controlador, uma vez que executa o processo de tratamento de dados em nome deste, devendo assegurar que sua atuação esteja em linha com a LGPD e as orientações fornecidas pelo controlador. O operador no processamento de dados pessoais é definido, conforme o artigo 5º, inc. VII (BRASIL, 2018), como "a entidade física ou jurídica, seja pública ou privada, que realiza o tratamento de dados pessoais em nome do controlador".

A legislação determina que cabe aos agentes de tratamento e às organizações implementarem medidas de segurança tanto no âmbito administrativo quanto no técnico, com o intuito de oferecer uma proteção aprimorada contra acessos não autorizados aos sistemas, assim como para prevenir eventos acidentais ou ilegais que possam resultar em destruição, modificação ou perda de qualquer forma de tratamento inadequado e/ou ilegal. Quanto a esse assunto, o artigo 46 da LGPD estabelece que:

> 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.
> § 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 (BRASIL, 2018).

A LGPD determina, assim, que os responsáveis pelo tratamento têm o dever de implementar medidas de segurança, tanto em relação a aspectos administrativos quanto técnicos, para salvaguardar os dados de acessos não permitidos, além de evitar eventos acidentais ou ilegais que possam levar à destruição, à modificação ou à perda dos dados. Em particular, o artigo 46 da LGPD, como já mencionado anteriormente, especifica essas

responsabilidades, ressaltando a relevância de um manejo apropriado e seguro das informações pessoais.

3 RESPONSABILIDADE CIVIL DAS EMPRESAS DIANTE DO VAZAMENTO DE DADOS

A responsabilidade das empresas em razão de prejuízos gerados pelo vazamento de informações pessoais de clientes é apoiada não apenas pela LGPD, mas igualmente pelo Código de Defesa do Consumidor (CDC). Em termos de responsabilização civil, a doutrina e a jurisprudência reconhecem que a responsabilização pode ser objetiva ou subjetiva, dependendo do enquadramento fático-jurídico: a responsabilização objetiva pode emergir em situações de risco inerente ao tratamento de dados, especialmente quando a governança é inadequada ou quando a norma impõe regimes de proteção mais estritos, independentemente de culpa específica, enquanto a responsabilização subjetiva depende da demonstração de culpa, dolo ou culpa concorrente.

O nexo de causalidade entre a conduta da empresa e o dano efetivamente suportado pelo titular é essencial para a condenação civil. Esse nexo pode ser dificultado diante da comprovação de causalidade complexa, da necessidade de provas técnicas sobre vulnerabilidades, das falhas de processo ou da participação de terceiros na cadeia de tratamento, o que, às vezes, leva à responsabilização solidária entre o controlador, o operador e terceiros envolvidos. O artigo 14 do CDC estabelece de maneira clara que as empresas têm a obrigação de ressarcir os prejuízos causados aos clientes, mesmo sem ter culpa, em caso de falha nos serviços prestados. Portanto, em situações de violação de dados, a deficiência na prestação do serviço – evidenciada pela falta de sistemas efetivos de proteção de dados – pode ser vista como um defeito que acarreta a responsabilidade de indenizar. Consoante Souza e André (2025, p. 12):

> [...] a implementação responsabilidade objetiva nas hipóteses de incidentes de segurança envolvendo dados pessoais encontra especial relevância em tempos de digitalização intensa, em que as empresas detêm e processam vastos volumes de informações dos consumidores. A expectativa de que tais dados sejam devidamente protegidos é legítima, e sua violação configura uma quebra da confiança que fundamenta a relação de consumo. Nesse sentido, o tratamento inadequado de dados ou a exposição indevida de informações sensíveis configura um serviço defeituoso, ensejando o dever de reparar o dano causado.

A LGPD solidifica essa compreensão ao estabelecer, no artigo 42, que tanto o controlador quanto o operador de dados que, durante a realização de atividades de processamento de dados pessoais, provocarem danos patrimoniais, morais, individuais ou coletivos, terão que assumir a responsabilidade por esses prejuízos. A responsabilidade pode ser afastada somente se o agente conseguir provar que não conduziu o tratamento de dados, que não houve infração à legislação vigente ou que o dano foi provocado unicamente por culpa do titular ou de terceiros (BRASIL, 2018).

A combinação da legislação da LGPD com o CDC reforça a defesa do consumidor em situações de segurança, uma vez que ambas as normas visam garantir a dignidade humana, a clareza nas relações contratuais e a proteção contra os perigos associados à atividade econômica. O Superior Tribunal de Justiça (STJ) já se manifestou de forma favorável à responsabilização de empresas em situações de vazamento de informações, reconhecendo a responsabilidade objetiva e aceitando a compensação por danos morais, mesmo sem necessidade de evidência de um prejuízo material direto, devido à quebra da privacidade e da confiança. De acordo com Souza e André (2025, p. 15):

> [...] é importante destacar que a responsabilidade civil nas relações de consumo também tem função pedagógica e preventiva, ao estimular que os fornecedores invistam em medidas de proteção de dados, tecnologias seguras e programas de compliance digital. Ao mesmo tempo, promove justiça ao titular de dados, que muitas vezes é colocado em situação de vulnerabilidade e exposição pública, com impactos profundos em sua vida pessoal e profissional.

Outro aspecto importante é a possibilidade de responsabilização conjunta entre diversos agentes que lidam com dados, como definido pela LGPD. Se várias organizações estiverem participando do processo de manipulação das informações (como uma empresa controladora que delega o armazenamento a outra), ambas podem ser corresponsáveis perante o titular pelos prejuízos ocasionados. Isso destaca a importância de contratos bem elaborados e de uma governança eficaz entre os parceiros de negócios, a fim de reduzir riscos e assegurar a conformidade com a lei. A esse respeito, Blum (2018, p. 39) leciona que:

> [...] é evidente que a responsabilidade civil objetiva representa uma importante ferramenta de proteção do consumidor na sociedade da informação. Sua aplicação, aliada aos princípios e dispositivos da LGPD, impõe às empresas um dever redobrado de cautela e diligência no tratamento de dados pessoais, sob pena de sanções administrativas e obrigações indenizatórias.

A responsabilidade das empresas, assim, não deve ser vista apenas de forma punitiva, mas como uma ferramenta para equilibrar as relações legais, sendo fundamental para a criação de um ambiente *online* mais ético, seguro e claro. Portanto, os dois lados da relação de manejo de dados precisam observar e operar em conformidade com os princípios destacados no artigo 6º da LGPD:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
> VIII - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> IX - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> X - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> XI - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> XII - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> XIII - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> XIV - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> XV - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> XVI - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> XVII - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

Como foi observado no parágrafo anterior, a legislação confere uma grande ênfase ao princípio da boa-fé, destacando-o em relação aos demais princípios e colocando-o isoladamente no início do artigo. Dessa forma, conclui-se que a boa-fé serve como fundamento para todos os outros princípios. Ademais, a referida lei estabelece que as organizações que lidam com dados pessoais devem garantir a proteção contra acesso não autorizado, bem como contra casos acidentais ou ilegais de destruição, perda, modificação,

divulgação ou disseminação de dados. Além disso, pontua que as empresas precisam implementar medidas preventivas para evitar prejuízos aos titulares dos dados.

3.1 INTERPRETAÇÃO JUDICIAL QUANTO À RESPONSABILIDADE CIVIL DIANTE DE VAZAMENTO DE DADOS

A exposição de informações é uma questão que vem ganhando destaque no mundo digital, e, segundo a LGPD, é um problema grave e que precisa ser abordado com seriedade. A LGPD estabelece uma série de normas e regras para o gerenciamento de situações de vazamento de dados pessoais, responsabilizando conjuntamente tanto o controlador quanto o operador. A norma impõe a necessidade de informar a Autoridade Nacional de Proteção de Dados (ANPD) e os proprietários dos dados sempre que um incidente de vazamento ocorra e que possa causar perigos ou danos a pessoas. A comunicação à ANPD precisa ser realizada dentro de um prazo estabelecido e deve incluir informações específicas sobre o evento, tais como: o tipo de dados afetados, as medidas implementadas para reduzir os riscos e as providências tomadas para corrigir a situação:

> 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 [...].
> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (Brasil, 2018).

A LGPD estabelece os limites da responsabilidade para as empresas e instituições que recolhem e processam dados pessoais. É um requisito que elas implementem ações técnicas e organizacionais para assegurar a proteção das informações e evitar vazamentos. Outrossim, salienta-se que a ausência de segurança apropriada e a falta de atenção quanto à salvaguarda de dados podem levar a penalizações rigorosas e compensações financeiras:

> 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.
> §1º - A fim de assegurar a efetiva indenização ao titular dos dados:
> I - O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador,

> hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei (Brasil, 2018).

Nesse sentido, cumpre salientar que a jurisprudência do STJ acerca do tema é no sentido de que um mero vazamento de dados pessoais comuns não gera automaticamente o direito à indenização por danos morais "*in re ipsa*". A esse respeito, importa mencionar a decisão proferida pela referida Corte nos autos de Recurso Especial nº 2.130.619-SP:

> PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. *In casu*, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais, mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis. V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido (BRASIL, 2023).

No caso acima, a 2ª Turma do STJ tomou uma decisão por unanimidade, afirmando que o vazamento de dados pessoais comuns, conforme estabelecido pela LGPD, não é suficiente, por si só, para justificar uma indenização por danos morais. Essa foi a primeira vez que a Corte se posicionou sobre essa questão. Os Ministros avaliaram o caso de uma consumidora da Enel São Paulo, que solicitou compensação devido ao vazamento e ao uso

indevido de suas informações pessoais. Ela citou dados como nome completo, o número de RG, a data de nascimento e telefone, além de detalhes referentes ao seu contrato. A mulher solicitou uma reparação no valor de 15 mil reais, que foi inicialmente recusada pelo juiz de primeira instância. Entretanto, a decisão foi modificada pelo Tribunal de Justiça do Estado de São Paulo (TJSP) em grau de apelação, em que os desembargadores da 27ª Câmara de Direito Privado aceitaram os argumentos apresentados pela cliente (Brasil, 2023).

Por sua vez, os julgadores da Corte Superior, ao julgarem o Recurso Especial, sedimentaram o entendimento no sentido de que o vazamento de informações pessoais, embora represente uma falha indesejada na gestão de dados de indivíduos por entidades jurídicas, não é suficiente, por si só, para ocasionar dano moral que possa ser compensado (BRASIL, 2023). Em outras palavras, consoante jurisprudência firmada pelo Colendo STJ, o dano moral não é configurado automaticamente, sendo imprescindível que o proprietário dos dados demonstre o prejuízo resultante da divulgação dessas informações.

3.2 POLÍTICAS DE PRIVACIDADE E CONTRATOS DE ADESÃO

As políticas de privacidade são consideradas contratos de adesão, uma forma contratual frequentemente presente nas interações entre consumidores. Esse tipo de contrato é definido pela imposição de direitos e obrigações de maneira unilateral, sem possibilidade de negociação. A aceitação ou a rejeição dos seus termos fica a critério da outra parte, que não participa do processo de elaboração ou da negociação das cláusulas do contrato em questão.

Esse documento contratual tem como função detalhar as normas que garantem a proteção da privacidade e os métodos de gerenciamento das informações pessoais de clientes e de qualquer indivíduo que utilize os serviços de um determinado agente de tratamento (denominados “usuários”). Portanto, a política de privacidade visa informar os usuários sobre como seus dados serão utilizados e as finalidades para as quais são coletados.

Consoante explica Freitas (2020, [s.p.]):

> [...] a política de privacidade deve apontar quais informações pessoais do usuário são coletadas, sejam aquelas fornecidas diretamente por ele ou coletadas a partir dos seus dados de navegação; qual é o objetivo de coleta dessas informações; como essas informações são tratadas, armazenadas e compartilhadas pelo agente de tratamento e/ou terceiros; e como o usuário pode alterar suas informações. Com a entrada em vigor da LGPD, tornou-se obrigatório informar aos usuários, além dos pontos acima indicados, todos os seus direitos previstos no Capítulo III da referida lei, bem como apontar, detalhadamente, como os Usuários podem exercê-los. São exemplos de direitos dos usuários e devem estar expressamente previstos na política de

> privacidade: o acesso às informações pessoais coletadas pelo agente de tratamento; a solicitação de eliminação ou anonimização das informações pessoais, isto é, impedir que o usuário possa ser identificado pessoalmente com base nas suas informações coletadas; a possibilidade de negar ou revogar o consentimento fornecido ao agente de tratamento para a coleta e o tratamento de informações pessoais; o direito de reportar à ANPD e/ou à órgãos de defesa ao consumidor sobre quaisquer incidentes relacionados às informações pessoais do usuário. Para o exercício desses direitos, o agente de tratamento deverá designar uma pessoa responsável por receber e responder às solicitações dos usuários relacionadas à proteção de dados pessoais, bem como receber comunicações da ANPD e do Poder Judiciário, prestar esclarecimentos e adotar providências — profissional definido pela LGPD como "encarregado".

Salienta-se, ainda, que a política de privacidade deve incluir os dados de contato do responsável – frequentemente referido como *data protection officer* (DPO). A política deve esclarecer as bases legais que fundamentam a coleta e o processamento das informações pessoais dos usuários. Novamente, conforme explica Freitas (2020, [s.p.]):

> [...] o artigo 7º da LGPD indica as dez hipóteses legais para a coleta e o tratamento de dados pessoais, previstas de forma taxativa — ou seja, não existe nenhuma outra hipótese além das expressamente descritas ali. Essas hipóteses são: o consentimento, que consiste na manifestação livre, informada e inequívoca do usuário para que seja realizado o tratamento dos seus dados pessoais; o cumprimento de obrigação legal ou regulatória; a execução de políticas públicas pela administração pública; a execução de estudos por órgãos de pesquisa; a execução de contrato; o exercício regular de direitos em processo judicial, administrativo ou arbitral; a proteção da vida, a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; o atendimento de interesse legítimo do controlador; e a proteção ao crédito, inclusive quanto ao disposto em regulação pertinente.

É importante destacar que atender a uma das previsões legais é suficiente para que o manuseio das informações dos usuários seja considerado válido, permitindo-se, também, que essas justificativas sejam combinadas. Assim, não é necessário mencionar todas as justificativas legais estipuladas na LGPD, mas apenas aquelas que realmente se aplicam.

Quando dados pessoais do usuário são coletados de maneira involuntária, como por meio das informações de navegação, é essencial que o usuário esteja ciente dessa coleta. Os *cookies* exemplificam bem como a coleta e a guarda de dados do usuário podem ocorrer simplesmente pelo acesso a uma plataforma. Portanto, o uso dessa tecnologia deve ser claramente comunicado ao usuário, em conformidade com as exigências da LGPD.

Ainda conforme Freitas (2020, [s.p.]):

> [...] a política de privacidade é um documento essencial à manutenção das relações consumeristas, especialmente aquelas que envolvem a coleta e o tratamento de dados pessoais. Assim, considerando a entrada em vigor da LGPD, as regras de segurança da informação sofreram relevantes alterações, que devem ser refletidas nas políticas de privacidade conforme exposto acima — de forma exemplificativa. Caso a política de privacidade não estabeleça os direitos do usuário de forma clara e de acordo com as regras e procedimentos previsto pela LGPD, o usuário que se sentir lesado quanto ao manuseio de seus dados pelo agente de tratamento — ou o próprio Procon e Ministério Público no exercício de suas atribuições — poderá acioná-lo administrativa ou judicialmente, podendo gerar sanções com impactos financeiros e na própria reputação do agente de tratamento. Além de mitigar as possibilidades em que o agente de tratamento pode ser demandado judicial ou administrativamente, a elaboração ou atualização da política de privacidade, de forma clara, detalhada e em conformidade com a LGPD e as demais normas vigentes, proporciona o aumento da credibilidade do agente de tratamento perante os seus clientes, parceiros, fornecedores e colaboradores.

Por fim, destaca-se que a elaboração de documentos legais e outras ações para atender à LGPD é um projeto que precisa ser realizado não somente com a colaboração de consultores jurídicos especializados, mas também com a participação das equipes de tecnologia. Tal contexto é essencial para garantir que as soluções implementadas não impactem as operações relacionadas à coleta, ao processamento e à utilização dos dados dos usuários.

5 CONSIDERAÇÕES FINAIS

Este trabalho examinou o vazamento de dados pessoais à luz da LGPD e da atuação da ANPD, com especial atenção à responsabilização civil das empresas diante de incidentes de segurança. A partir de uma revisão de literatura, da doutrina, da jurisprudência e das diretrizes regulatórias, foi possível evidenciar que a proteção de dados não se restringe a um conjunto de regras pontuais, mas exige uma abordagem integrada de governança, conformidade normativa e *accountability*. Observa-se uma tendência crescente de convergência entre as sanções administrativas e a responsabilização civil, impulsionada pela necessidade de proteger direitos fundamentais e de promover padrões consistentes de governança de dados no ambiente organizacional.

As evidências apontam que a responsabilização civil não decorre apenas de falhas isoladas, mas frequentemente resulta de uma combinação de fatores: falhas na governança, inadequação de controles técnicos e administrativos, uso inadequado de dados por terceiros e

insuficiente transparência com os titulares. Nesse contexto, a efetividade da LGPD depende, sobretudo, da implementação de mecanismos de governança de dados que permitam a detecção precoce de riscos, uma resposta ágil a incidentes e a demonstração de conformidade perante os titulares, os reguladores e o mercado. Em termos regulatórios, as decisões da ANPD e de tribunais vêm consolidando referências sobre a aplicação de princípios como a finalidade, a necessidade, a minimização e a *accountability*, ao mesmo tempo em que enfatizam a necessidade de documentação, auditorias e melhoria contínua das práticas de proteção de dados.

Verificou-se, ademais, que a LGPD exige que incidentes de vazamento de dados sejam comunicados e atribui às empresas e instituições a responsabilidade de salvaguardar as informações pessoais que possuem. Essa legislação ressalta a relevância da segurança da informação e da clareza no manejo de dados pessoais, com o intuito de assegurar a privacidade e os direitos dos indivíduos em um contexto digital que se torna cada vez mais complexo e interligado. Dessa forma, a LGPD atua como um recurso fundamental para enfrentar os problemas e os impactos decorrentes dos vazamentos de informações na sociedade atual. Sob o ponto de vista prático, as principais recomendações envolvem a adoção de planos de resposta a incidentes bem estruturados, a condução de avaliações de impacto à proteção de dados (DPIA) em situações de alto risco e a implementação de controles de acesso, criptografia, monitoramento e treinamentos periódicos.

Entre as limitações deste estudo, destaca-se a dependência de fontes públicas disponíveis, que nem sempre refletem a totalidade de casos ou de diretrizes implementadas; além disso, a dinâmica regulatória e jurisprudencial sobre a LGPD ainda está em consolidação, o que exige atualização contínua. Contudo, a partir das evidências apresentadas, é possível concluir que uma abordagem proativa de governança de dados, aliada a uma leitura integrada das obrigações legais e das sanções regulatórias, é crucial para promover a responsabilidade civil eficaz diante de vazamentos de dados.

A promoção de boas práticas, a transparência na comunicação com titulares e a robustez de mecanismos de conformidade devem orientar tanto as estratégias empresariais quanto as políticas públicas voltadas à proteção de dados no Brasil. Destaca-se que, à luz da recente decisão do STJ mencionada, qualquer compensação por vazamentos de dados necessita da demonstração do dano efetivo, excluindo-se a possibilidade de dano moral presumido "*in re ipsa*" nos casos de vazamento de dados ordinários.

REFERÊNCIAS

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e a proteção dos dados do consumidor**. São Paulo: Almedina, 2018.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 53/2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República, [2018]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 25 ago. 2025.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 5 jul. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2021]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 ago. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2025]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 set. 2025.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 16 set. 2025.

BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 23 ago. 2025.

BRASIL. Senado Federal. **Projeto de Lei nº 131/2014**. Dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros. Brasília, DF: Presidência da República, [2014]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/116969. Acesso em: 15 set. 2025.

BRASIL. **Projeto de Lei nº 181/2014**. Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais. Brasília, DF: Presidência da República, [2014]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/117736. Acesso em: 15 set. 2025.

BRASIL. Senado Federal. **Projeto de Lei nº 330/2013**. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Brasília, DF: Presidência da República, [2013]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947. Acesso em: 10 set. 2025.

BRASIL. Superior Tribunal de Justiça (2. Turma). **Recurso Especial nº 2.130.619-SP**. Relator: Min. Francisco Falcão, 10 mar. 2023. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?termo=2.130.619&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO. Acesso em: 16 set. 2025.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2011.

FREITAS, Bernardo. LGPD em vigor: o papel e a importância das políticas de privacidade. **Legislação & Mercados**, 30 set. 2020. Disponível em: https://legislacaoemercados.capitalaberto.com.br/lgpd-em-vigor-o-papel-e-a-importancia-das-politicas-de-privacidade/. Acesso em: 16 set. 2025.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de Internet**. São Paulo: Juarez de Oliveira, 2005.

MARQUES, Marilia. MP do DF aponta suposto esquema de venda de dados pessoais de brasileiros pelo Serpro. **G1**, 1 jun. 2018. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/mp-do-df-aponta-suposto-esquema-de-venda-de-dados-pessoais-de-brasileiros-pelo-serpro.ghtml. Acesso em: 5 jun. 2025.

PESTANA, Márcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). **Consultor Jurídico**, 25 maio 2020. Disponível em: https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf. Acesso em: 16 set. 2025.

RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2018.

SILVA, Oscar Joseph de Plácido e. **Vocabulário Jurídico**. 22. ed. Rio de Janeiro: Forense, 2003.

SOUZA, Vitória Lima de; ANDRÉ, Victor Conte. Lei Geral de Proteção de Dados: coleta de dados sensíveis do consumidor e a responsabilidade civil. **Revista Multidisciplinar do Nordeste Mineiro**. V. 6, n. 1, p. 1-21, 2025. Disponível em: https://remunom.ojsbr.com/multidisciplinar/article/view/3717. Acesso em: 5 jun. 2025.

VIEIRA, Victor Rodrigues Nascimento. **Lei Geral de Proteção de Dados**: uma análise da tutela de dados pessoais em casos de transferência internacional. 2019. 76 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: https://repositorio.ufu.br/bitstream/123456789/26233/1/LeiGeralProtecao.pdf. Acesso em: 17 set. 2025.