CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

DADOS EM MÃOS ALHEIAS: A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS

Matheus Mestrinelli

Presidente Prudente/SP
2024

CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

DADOS EM MÃOS ALHEIAS: A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS

Matheus Mestrinelli

Monografia apresentada como requisito parcial de conclusão do curso e obtenção do grau de Bacharel em Direito, sob a orientação do Prof. Guilherme Prado Bohac de Haro.

Presidente Prudente/SP
2024

DADOS EM MÃOS ALHEIAS: A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Direito.

_____
Dr. Guilherme Prado Bohac de Haro
Orientador

_____
Dr. Daniel Gustavo de Oliveira Colnago Rodrigues
Examinador 1

_____
Me. Américo Ribeiro Magro
Examinador 2

Presidente Prudente, _____.

Dedico este trabalho a Deus, cuja presença me sustenta e direciona em todos os momentos da minha vida.

AGRADECIMENTOS

Aos meus pais, Léa e Sérgio, e à minha tia Lucília, pelos constantes incentivos e pelo apoio ao longo da minha trajetória acadêmica.

Aos amigos, pelo companheirismo.

Ao Professor Dr. Guilherme Bohac, por ter sido meu orientador e ter desempenhado tal função com dedicação e cuidado.

RESUMO

Este trabalho tem como objetivo analisar a responsabilidade civil no contexto da Lei Geral de Proteção de Dados (LGPD) e sua aplicação no ordenamento jurídico brasileiro, destacando sua importância na regulação do tratamento de dados pessoais. A pesquisa adota uma abordagem teórico-doutrinária, baseando-se em estudos legislativos, jurisprudência, literatura especializada e estudo de casos, com o intuito de compreender os impactos da LGPD no contexto da privacidade e proteção de dados. Inicialmente, apresenta-se o histórico legislativo que culminou na promulgação da LGPD, com destaque para influências internacionais. Em seguida, o estudo aborda os princípios fundamentais da LGPD, como a autodeterminação informativa, a transparência e a responsabilização dos agentes de tratamento. A análise também se estende à responsabilidade civil decorrente de violações da legislação, com foco nas consequências jurídicas e reparatórias. Por fim, são discutidos os desafios práticos na aplicação da LGPD, especialmente em face das inovações tecnológicas e da crescente digitalização das atividades econômicas e sociais. A pesquisa conclui que, embora a LGPD represente um avanço significativo para a proteção de dados no Brasil, sua efetividade depende de um esforço contínuo de adaptação e regulamentação, especialmente na delimitação clara e inequívoca do regime de responsabilidade a ser adotado pela lei.

Palavras-chave: LGPD, proteção de dados, responsabilidade civil, privacidade, legislação.

ABSTRACT

This work aims to analyze civil liability in the context of the General Data Protection Law (LGPD) and its application in the Brazilian legal system, highlighting its importance in regulating the processing of personal data. The research adopts a theoretical-doctrinal approach, based on legislative studies, jurisprudence, specialized literature and case studies, with the aim of understanding the impacts of the LGPD in the context of privacy and data protection. Initially, the legislative history that culminated in the promulgation of the LGPD is presented, highlighting international influences. Next, the study addresses the fundamental principles of the LGPD, such as informational self-determination, transparency and accountability of processing agents. The analysis also extends to civil liability arising from violations of legislation, focusing on legal and reparatory consequences. Finally, the practical challenges in applying the LGPD are discussed, especially in the face of technological innovations and the increasing digitalization of economic and social activities. The research concludes that, although the LGPD represents a significant advance for data protection in Brazil, its effectiveness depends on a continuous effort of adaptation and regulation, especially in the clear and unequivocal delimitation of the liability regime to be adopted by the law.

Keywords: LGPD, data protection, civil liability, privacy, legislation.

LISTA DE SIGLAS E ABREVIATURAS

ANPD – Autoridade Nacional de Proteção de Dados

CDC – Código de Defesa do Consumidor

LGPD – Lei Geral de Proteção de Dados

RGPD – Regulamento Geral de Proteção de Dados

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO 10

2 A LEI GERAL DE PROTEÇÃO DE DADOS 12
2.1 Histórico e Produção Legislativa 12
2.2 Princípios 21
2.2.1 Finalidade 22
2.2.2 Adequação 23
2.2.3 Necessidade 23
2.2.4 Livre Acesso 24
2.2.5 Qualidade de Dados 24
2.2.6 Transparência 25
2.2.7 Segurança 26
2.2.8 Prevenção 26
2.2.9 Não Discriminação 27
2.2.10 Responsabilização e Prestação de Contas 28
2.3 Categorias de Dados Pessoais 29
2.3.1 Dados Pessoais Lato Sensu 30
2.3.2 Dados Sensíveis 30
2.3.3 Dados Anonimizados 32
2.4 Consentimento 33
2.5 Proteção dos Dados Pessoais à luz da Constituição Federal 34
2.6 Crimes Digitais e Mercantilização dos Dados 36
2.6.1 *Blind Phishing* 37
2.6.2 *Smishing* 38
2.6.2 *Pharming* 38
2.6.2 *Man in the Middle Atack* 38

3 RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO .. 39
3.1 Responsabilidade Civil Subjetiva 39
3.2 Responsabilidade Civil Objetiva 41

4 RESPONSABILIDADE CIVIL E A LEI GERAL DE PROTEÇÃO DE DADOS 42
4.1 Controlador sendo um ente público 43
4.2 Controlador sendo pessoa natural ou pessoa jurídica de direito privado 45
4.1 Interpretação Sistemática 46
4.1 Interpretação Teleológica 46
4.1 A Regulamentação da responsabilidade civil dos agentes de tratamento de dados na LGPD46

5 ENTENDIMENTO DOUTRINÁRIO SOBRE O REGIME DE RESPONSABILIDADE CIVIL NA LGPD 48
5.1 Responsabilidade Objetiva 48
5.2 Responsabilidade Subjetiva 50
5.3 Responsabilidade Proativa 52

6 ANÁLISE DE CASOS PRÁTICOS 54

6.1 Caso Cyrela 54
6.2 Caso Eletropaulo 55
6.3 Caso SERASA 58
6.4 Caso Seguradora de Vida 60

7 CONCLUSÃO 61

8 REFERÊNCIAS 63

1 INTRODUÇÃO

A era digital trouxe consigo profundas transformações nas formas de interação social, econômica e política, criando um ambiente em que a coleta, armazenamento e compartilhamento de dados pessoais se tornaram práticas corriqueiras. Com o avanço da tecnologia e a globalização das relações comerciais, o tratamento de dados pessoais passou a ser essencial para a dinâmica de diversos setores, desde o comércio eletrônico até o setor público. Em meio a essa nova realidade, surge a necessidade premente de regulamentar o uso desses dados, a fim de proteger a privacidade dos cidadãos e garantir seus direitos fundamentais.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, sancionada no Brasil em 2018 e em vigor desde 2020, representa uma resposta legislativa robusta à crescente demanda por proteção de dados pessoais. Inspirada no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, a LGPD estabelece um marco regulatório para o tratamento de dados, impondo obrigações rigorosas a empresas, órgãos públicos e outros agentes que manipulam informações pessoais. Ao prever a aplicação de sanções administrativas, como multas e a suspensão do uso de dados, a LGPD visa assegurar que o tratamento de dados seja realizado de forma ética, transparente e em conformidade com a lei.

A LGPD introduziu princípios fundamentais que norteiam a proteção de dados no Brasil, como a finalidade, necessidade, adequação, transparência, segurança, prevenção e não discriminação. Esses princípios estabelecem diretrizes claras para a coleta e tratamento de dados, garantindo que os titulares tenham controle sobre suas informações pessoais e que possam exercer direitos como o acesso, retificação, exclusão e portabilidade de seus dados. Nesse sentido, a lei também assegura a autodeterminação informativa, conceito essencial para o exercício da privacidade na sociedade da informação.

Contudo, a implementação da LGPD no Brasil não está isenta de desafios. Em primeiro lugar, a adequação das empresas e do setor público às exigências legais tem sido um processo gradual e, muitas vezes, oneroso. A conformidade com a LGPD requer a adoção de novas práticas, políticas internas de governança de dados e a implementação de medidas de segurança robustas, a fim de evitar o vazamento ou mau uso de informações sensíveis. Além disso, a criação da Autoridade Nacional de Proteção de Dados (ANPD) como órgão regulador é crucial para a fiscalização e aplicação das normas, porém, sua atuação ainda está em fase de consolidação.

Outro ponto de destaque é a responsabilidade civil dos agentes de tratamento de dados. A LGPD prevê que tanto os controladores quanto os operadores podem ser responsabilizados por danos materiais e morais decorrentes de violação à legislação, seja pela má gestão dos dados ou por falhas de segurança. Essa responsabilização objetiva impõe a necessidade de uma estrutura de compliance rigorosa e bem delineada dentro das organizações, de forma a evitar penalidades e proteger os direitos dos titulares de dados. A questão da responsabilidade civil também envolve a discussão sobre a reparação de danos em casos de vazamentos de dados, prática que tem se tornado cada vez mais comum em um ambiente digital vulnerável a ataques cibernéticos.

Além dos aspectos internos de conformidade, a LGPD reflete uma preocupação com a harmonização das normas de proteção de dados no cenário internacional. A globalização das transações comerciais e o fluxo de dados transfronteiriços exigem que o Brasil adote padrões elevados de proteção de dados, de modo a facilitar o intercâmbio de informações com outros países, especialmente aqueles que compõem a União Europeia, onde o RGPD estabelece critérios rigorosos para a transferência de dados para terceiros países. A adequação à LGPD, portanto, também tem como objetivo alinhar o Brasil às melhores práticas internacionais, promovendo a competitividade do país no mercado global.

A presente monografia busca analisar de forma aprofundada a Lei Geral de Proteção de Dados, explorando sua relevância no contexto jurídico brasileiro e internacional, e abordando os principais desafios e oportunidades gerados pela sua implementação. O estudo se concentra, especialmente, nas implicações jurídicas da LGPD em relação à responsabilidade civil dos agentes de tratamento, à eficácia das sanções previstas, bem como às dificuldades práticas enfrentadas pelas organizações para se adequarem à nova legislação.

Por fim, também é analisada a jurisprudência recente que envolve a aplicação da LGPD, avaliando como os tribunais brasileiros têm interpretado e decidido casos relacionados à proteção de dados pessoais. O objetivo é traçar um panorama completo sobre a LGPD, compreendendo seu impacto no ordenamento jurídico nacional, os direitos assegurados aos titulares de dados e as obrigações impostas aos agentes de tratamento. Ao final, espera-se contribuir para uma melhor compreensão dos desafios da proteção de dados no Brasil e propor reflexões sobre o futuro da privacidade em um mundo cada vez mais digitalizado.

2 A LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, é uma legislação brasileira que estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo maior controle e transparência às empresas e organizações que lidam com essas informações. O processo legislativo que culminou na criação da LGPD foi marcado por debates e discussões sobre a necessidade de proteger a privacidade e a liberdade dos cidadãos em um contexto de crescente digitalização e uso de dados.

2.1 Histórico e Produção legislativa

Embora a LGPD represente uma inovação no cenário da proteção de dados pessoais no Brasil, sendo a primeira lei nacional exclusivamente dedicada a essa área, a ideia em si não é nova e há muito tempo vem sendo discutida e implementada em outras partes do mundo. Apesar de sua natureza inovadora, a iniciativa brasileira chega em um momento relativamente tardio em comparação com outros países.

De acordo com Pinheiro:

> [...] o motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização (PINHEIRO, 2020).

Consequentemente, surgiu a necessidade de implementar normas que definissem compromissos de instituições para com os indivíduos da atual sociedade da informação, com foco na proteção e na garantia dos direitos fundamentais, especialmente, como se verá adiante, o da privacidade.

A primeira legislação oficialmente dedicada a esse tema foi promulgada na Alemanha durante a década de 1970. O avanço da computação e da indústria nos países mais desenvolvidos levou o país a considerar meios para regulamentar a proteção da privacidade. Embora o conceito de proteção de dados pessoais tenha sido desenvolvido no início daquela década, a lei só foi implementada em 1978. A partir desse marco, países como França e

Suécia, influenciados pela legislação alemã, também elaboraram suas próprias leis de proteção dos dados aos seus cidadãos.

O debate sobre o assunto se intensificou e em 24 de outubro de 1995 a União Europeia implementou a Diretiva nº 95/64/CE, que trata sobre a proteção das pessoas no que diz respeito ao tratamento de dados pessoais e sobre sua livre circulação. Em 12 de julho de 2002, foi criada a Diretiva nº2002/58/CE, que regulamenta o tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrônicas. E, em março de 2006, foi elaborada a Diretiva nº 2006/24/CE, que versa sobre a conservação de dados gerados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, alterando a Diretiva de 2002.

Sobre as diretivas criadas pela União Europeia:

> Em um primeiro momento, as diretivas supracitadas definiram os elementos essenciais relacionados à matéria tratada, tal como o conceito de tratamento de dados pessoais, bem como cuidaram de estabelecer princípios que versam sobre a legitimidade do tratamento e da qualidade dos dados e ainda conferiu um rol de garantias aos usuários, que, na presente relação, assumem o papel de fornecedores dos dados coletados (AIME; OBREGÓN, 2020. p. 05).

O primeiro instituto que tratou da proteção de dados pessoais no Brasil foi o *habeas data*, previsto no artigo 5º LXXII, da Constituição Federal de 1988. Esse instituto assegurou aos cidadãos a proteção de seus dados pessoais perante o Estado, sendo interpretado como um direito material de acesso e retificação em relação aos dados pessoais. Entretanto, o dispositivo constitucional não demonstrou ser suficiente para a formulação completa do direito de proteção de dados pessoais, pois, na prática, acabou sendo substituído por alternativas que se mostraram mais eficazes como o mandado de segurança, que por sua vez, também foi insuficiente para o entabulamento da criação do direito material respectivo.

O início do desenvolvimento regulamentar e jurisprudencial da proteção de dados pessoais no Brasil seguiu um marco cronológico, sendo o Código de Defesa do Consumidor (CDC) um dos primeiros pontos de referência. Esse código, reconhecido por sua aplicação de responsabilidade objetiva, inclui disposições específicas sobre a proteção dos dados pessoais dos consumidores, conforme evidenciado no artigo 43, *caput*, e parágrafos 1º, 2º, 3º e 6º. A existência desse direito de proteção de dados pessoais na legislação resultou em um aumento significativo de demandas judiciais relacionadas à tutela desses dados, contribuindo para o estabelecimento de jurisprudências sobre o tema no Brasil.

Segundo o Ministro Ricardo Villas Bôas Cueva, o primeiro caso a ser analisado pelo STJ referente à utilização de dados pessoais foi construído considerando o teor do art. 43, do CDC, no REsp 22.337-8/RS, de relatoria do ministro Ruy Rosado, que identificou um direito fundamental à autodeterminação informativa De acordo com o voto do ministro, ainda no ano de 1995, já havia a preocupação com "uma crescente vulnerabilidade do indivíduo ante a coleta e o armazenamento de informações que invadem sua intimidade", violando o direito constitucional da privacidade.

A partir desse ponto, surgiram as primeiras discussões sobre danos indenizáveis decorrentes do tratamento discriminatório de dados pessoais, especialmente no contexto dos cadastros de proteção ao crédito, que resultaram em ações de indenização por danos morais devido a inscrições indevidas nos órgãos de proteção ao crédito. A demanda por intervenção judicial foi tão significativa que levou à criação da Súmula nº 385 pelo Superior Tribunal de Justiça (STJ).

Desse modo, visando melhor tratamento do assunto, em 09 de junho de 2011, foi publicada a Lei do Cadastro Positivo (Lei nº 12.414), que buscou regulamentar "a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais [...] para a formação de histórico de crédito". Para Doneda, a referida lei:

> [...] foi a primeira normativa brasileira concebida a partir de conceitos e de uma sistemática comum à tradição de proteção de dados, que já estava consolidada em outros países", embora insuficiente para a construção de uma "cultura jurídica de proteção de dados. DONEDA, Danilo. Panorama histórico da proteção de dados pessoais (DONEDA, 2021, p. 15).

Posteriormente, em 18 de novembro de 2011, a Lei de Acesso à Informação (Lei nº 12.965) entrou em vigor e, conforme apontado de Boff e Fortes, determinou:

> [...] que o tratamento das informações pessoais detidas por entidades e instituições nela abrangidas seja realizado de modo transparente, respeitando o direito fundamental à proteção da intimidade, da vida privada, da honra e da imagem das pessoas, o que, corresponde à proteção do direito fundamental à privacidade. A lei impõe restrições substanciais de acesso a informações pessoais, como o acesso restrito às informações, pelo prazo máximo de cem anos, a agentes públicos autorizados, bem como a possibilidade de acesso ou divulgação a terceiros, mediante prévio consentimento do titular das informações, exceto nos casos previstos no regulamento (BOFF; FORTES, 2016. p. 356-357.)

Adiante, em meados de 2013, a questão da regulamentação para proteger o processo de tratamento de dados voltou a ocupar o centro dos debates após a revelação de um

escândalo de espionagem envolvendo a Agência de Inteligência dos Estados Unidos (CIA-*Central Intelligence Agency*), por meio do ex-funcionário Edward Snowden. Ele vazou informações confidenciais de segurança dos EUA e expôs detalhes sobre alguns dos programas de vigilância utilizados pelo país para monitorar a população norte-americana, incluindo o uso de servidores de empresas como Google, Apple e Facebook, além de vários países da Europa e América Latina, incluindo o Brasil. O caso teve como consequência a imposição de um regime de urgência para a tramitação do Projeto de Lei do Marco Civil da Internet na Câmara dos Deputados.

Desde a denúncia de espionagem, o Brasil assumiu uma posição eminente na discussão sobre privacidade dos usuários e, consequentemente, sobre governança da Internet no mundo.

Sampaio concluiu que:

> Diante disso, era importante que o Brasil detivesse algo próprio para acrescentar e para demonstrar na discussão, e o Marco Civil, que se encontrava emperrado na Câmara, era um projeto avançado nesse sentido. Não se pode menosprezar a importância da sociedade civil organizada para a aprovação, mas acredito que o caso Snowden certamente tenha aberto uma janela de oportunidade para recolocar o tema em pauta e garantir sua aprovação rápida (SAMPAIO, 2014. p. 04).

Com isso, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, foi promulgada com o objetivo de regular o uso da Internet e garantir o direito à privacidade dos usuários. Essa legislação representou uma inovação significativa, pois estabeleceu regras para o uso da Internet no país em um momento em que o acesso aos dados e o registro do comportamento dos usuários não eram adequadamente regulamentados. O artigo 3º, III, do Marco Civil da Internet, estabelece como um de seus princípios a "proteção dos dados pessoais, na forma da lei". O legislador deixou claro que esse dispositivo seria um prenúncio de uma legislação específica sobre proteção de dados, referindo-se à LGPD, que viria posteriormente.

O Marco Civil da Internet define, pela primeira vez, o consentimento como sendo livre, expresso e informado, adjetivos estrategicamente atribuídos para o posterior debate sobre a proteção de dados pessoais. O texto dispõe sobre o direito ao esquecimento e ao controle de dados, no entanto, é internacionalmente criticado pela previsão de armazenagem pelos provedores de internet dos denominados “metadados”. O art. 15 prevê

que o provedor de aplicações de internet deve manter os registros de acesso a aplicações de internet sob sigilo em ambiente controlado e seguro, pelo prazo de 6 (seis) meses.

Bioni (2018) afirma que o Marco Civil da Internet é taxativo no processo de controle do titular de seus dados. Independentemente da etapa e do fluxo, a lei define que o consentimento prevalece, desde a coleta, passando pelo compartilhamento até a exclusão. Nas palavras de Bioni "verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo Marco Civil para a proteção de dados pessoais" (BIONI, 2018, p. 132).

Em outubro de 2014, a Secretaria Nacional do Consumidor do Ministério da Justiça informou que o texto deveria ser revisto, em virtude de mudanças na conjuntura nacional trazidas pela aprovação de diversos marcos normativos significativos, como a Lei do Cadastro Positivo (Lei 12.414/2011), a Lei de Acesso à Informação (Lei 12.527/2011), a Lei dos Crimes Cibernéticos (Lei 12.737/2012) e o Marco Civil da Internet.

Naquele tempo, já havia vários debates sobre a criação de uma legislação específica para tutela dos dados pessoais. O anteprojeto foi apresentado em formato de Consulta Pública para incentivar a participação popular na elaboração da minuta da lei brasileira de proteção de dados pessoais que seria encaminhada à Câmara dos Deputados. A proposta visava assegurar ao cidadão uma série de direitos básicos sobre seus dados pessoais, armazenados tanto em território nacional, como em centrais fora do país.

A minuta objeto da Consulta Pública abordou também questões relativas ao vazamento e uso compartilhado de dados, além da responsabilidade daqueles que lidam com essas informações, exigiu clareza sobre os procedimentos adotados para garantir a segurança desses dados. O Projeto de Lei foi encaminhado ao Poder Legislativo em 2016, sob o nº 5.276, sendo objeto de debate e intensa participação dos setores ingressados no tema.

Enquanto a Lei Geral de Proteção de Dados brasileira ainda estava em fase de criação, em 2018 entrou em vigor o Regulamento Geral de Proteção de Dados europeu (RGPD), que influenciou outros países na implementação de legislação de proteção de dados, inclusive o Brasil. Conforme Bioni (2021) o RGPD é "reconhecido como a maior influência da LGPD", visto que se tornou, até o momento, o marco regulatório mais completo em termos de legais e estruturais de proteção de dados pessoais. Um dos motivos que fez o RGPD influenciar outros países na criação e implementação de leis de proteção de dados pessoais foi o fato de incluir em seu texto legal um critério para a manutenção dos fluxos de dados. Para que haja a transferência de dados pessoais da União Europeia para um país terceiro, devem ser observados os requisitos estabelecidos na RGPD e as garantias existentes de proteção de dados no país que irá receber e tratar os dados.

Voltando ao marco cronológico da criação da LGPD, até o final do ano de 2017 ainda não havia nenhuma perspectiva concreta de aprovação da Lei, após 13 audiências públicas com debates temáticos, um seminário internacional e diversas contribuições de diferentes setores, como da academia e de empresas de software (ABRASEM, ABRANET, Facebook), o projeto de Lei foi encaminhado à Câmara dos Deputados com requerimento de urgência. O Deputado Orlando Silva emitiu parecer destacando que buscou ouvir todas as partes interessadas e teve cuidado e rigor com a definição de dado pessoal e sensível. Segundo ele, buscou um conceito preciso, mas que não inibisse a inovação tecnológica.

Durante a tramitação, o texto recebeu 11 emendas, sendo que 6 foram acatadas pelo relator. No dia 29 de maio de 2018, a matéria foi aprovada na forma do substitutivo apresentado pelo deputado Orlando Silva, seguindo para o Senado Federal. A primeira Comissão a analisar o texto foi a de Assuntos Econômicos, tendo como relator o senador Ricardo Ferraço, que após intensa articulação teve seu relatório aprovado no dia 3 de julho de 2018, com 9 emendas a fim de aprimorar a técnica legislativa e garantir o equilíbrio entre a proteção à privacidade e a inovação tecnológica. Até que, em meados de 2018, vários fatores impulsionaram o Brasil à aprovação da Lei, como o escândalo da *Cambridge Analytica*.

Em 2018, a empresa de marketing inglesa *Cambridge Analytica*, especialista em analisar grandes quantidades de dados pessoais para construir estratégias mais eficazes a serem empregadas em campanhas publicitárias em diversos ramos, foi acusada de ter acesso aos dados de mais de 50 milhões de usuários do Facebook, dados esses utilizados em 2016 para conduzir e influenciar as eleições presidências norte americanas que resultaram na vitória do candidato Donald Trump. Os dados foram coletados por meio do aplicativo "*thisisyourdigitallife*" e, ao utilizarem o aplicativo, os usuários concordavam em ceder dados e informações pessoais que, posteriormente, foram repassadas para a *Cambridge Analytica*. Segundo explica Silas Martí:

> Tudo começou em junho de 2014, quando o professor Aleksandr Kogan, da Universidade Cambridge, no Reino Unido, criou um teste de personalidade no Facebook com o pretexto de conduzir um estudo psicológico de usuários. Mesmo que só 270 mil pessoas tenham feito o teste de Kogan, o sistema permitiu que sua equipe visse o perfil de 50 milhões de usuários, pois também captava as informações de todos os amigos delas. No ano seguinte, Kogan repassou essa informação à Cambridge Analytica, que então contratou outros especialistas, entre eles Christopher Wylie, que acabou revelando o esquema ao jornal britânico The Observer (a versão dominical do Guardian) para influenciar a eleição dos EUA (MARTÍ, 2018).

O vazamento de perfis teria ocorrido por conta de uma política flexível do Facebook com relação à entrega de informações de perfis a aplicativos de terceiros na rede social. Entre 2007 e 2014, a empresa ofereceu livremente dados de usuários a desenvolvedores de apps. No Reino Unido a rede social foi submetida ao pagamento de multas, razoavelmente baixas, no valor de 643.000 dólares, sob a égide da *Data Protection Actde* 1998, uma vez que os dados foram coletados em 2015. Se analisado este mesmo caso sobre a égide da RGPD o valor da multa poderia ser 30 vezes maior podendo chegar a 22 milhões de dólares.

No Brasil, o Ministério da Justiça e Segurança Pública, por meio do Departamento de Proteção e Defesa do Consumidor (DPDC) da Secretaria Nacional do Consumidor (SENACON), decidiu impor uma multa de R$ 6,6 milhões às empresas Facebook Inc. e Facebook Serviços Online do Brasil Ltda por meio de um processo administrativo. As investigações revelaram que aproximadamente 440.000 perfis pessoais de brasileiros foram coletados no caso Cambridge Analytica, o que foi considerado uma prática abusiva por parte do Facebook. A falta de transparência sobre as configurações de privacidade e a ausência de proteção dos dados pessoais dos usuários foram apontadas como fundamentos para essa decisão. É importante destacar que o valor da multa foi determinado com base nas normas do Código de Defesa do Consumidor (CDC), e se o caso ocorresse sob a vigência da LGPD, poderia chegar a 50 milhões de reais, além de implicar a suspensão, proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

Outros fatores que impulsionaram o Brasil para a aprovação da LGPD foram: I) a vigência do RGPD europeu, que atribuiu um critério para a manutenção do fluxo de dados – para que haja a transferência de dados da União Europeia para um terceiro país, deverão ser observadas as garantias existentes no país destinatário sobre a proteção de dados; II) o desejo expresso do Brasil de ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que exige, como boa prática, a regulamentação do uso de dados pessoais, assim como um órgão supervisor independente e autônomo; e III) uma articulação interna à Câmara dos Deputados para a aprovação das alterações na Lei do Cadastro Positivo, que envolvia a aprovação da Lei Geral de Proteção de Dados como condição indispensável.

Ainda de acordo com Bioni (2021), esses acontecimentos foram um "verdadeiro ultimato para a aprovação da Lei". Assim, em 14 de agosto de 2018, a LGPD foi sancionada pelo então presidente Michel Temer. O que representou um avanço significativo, visto que, pela primeira vez, o país teve uma legislação específica para a proteção dos dados pessoais.

No dia 10 de julho de 2018, a matéria, por requerimento de urgência, foi pautada em plenário e aprovada por unanimidade. Devido ao regime de urgência, o Senador Eduardo Braga proferiu parecer favorável nas Comissões de Ciência e Tecnologia (CCT) e Comissão de Constituição e Justiça (CCJ), defendendo a necessidade de aprovação do texto para estabelecimento de uma segurança jurídica na proteção de dados pessoais no Brasil. O relator da matéria Ricardo Ferraço afirmou em seu parecer que 60 entidades atuaram na construção coletiva do texto aprovado.

Após elaboração legislativa, a Lei de Proteção de Dados Pessoais foi sancionada e publicada no dia 14 de agosto de 2018, como Lei nº 13.709/2018, "que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)". A lei foi sancionada com alguns vetos, com destaque para os artigos que criavam a agência reguladora de dados pessoais (arts. 55 a 59), que estabeleciam regras de compartilhamento de dados entre a administração pública e empresas privadas. O texto que entrou em vigor em 2020 é considerado uma normativa harmônica com a legislação internacional e satisfatória para sua finalidade.

À semelhança de outras normas jurídicas, a Lei Geral de Proteção de Dados (LGPD) é composta por regras e princípios fundamentais. Em suas disposições preliminares, a lei estabelece como objetivo primordial a proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. É importante ressaltar que a LGPD representa um marco regulatório crucial para a proteção dos dados pessoais, independentemente de estes serem transmitidos pela Internet ou por outros meios.

Assim, quaisquer estabelecimentos que coletem dados pessoais – como farmácias, locadoras de carro, postos de gasolina – estão submetidos às suas disposições. Ainda nas disposições preliminares, o art. 2º traz os seus fundamentos, isto é, como o Estado deve interpretá-la diante de casos concretos, e materializa alguns dispositivos legais de direitos e garantias fundamentais dispostos na Constituição Federal:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I- o respeito à privacidade;
> II- a autodeterminação informativa;
> III- a liberdade de expressão, de informação, de comunicação e de opinião;
> IV- a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI -a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL,1988).

Os fundamentos da Lei Geral de Proteção de Dados (LGPD) representam a materialização legal de certos direitos e garantias fundamentais consagrados em nossa Constituição. O artigo 2º, inciso I, estabelece como primeiro fundamento o respeito à privacidade. Esse fundamento está em total harmonia com o inciso X do artigo 5º da Constituição Federal, que preconiza a inviolabilidade da intimidade e da vida privada, princípio replicado no inciso IV do mesmo artigo da LGPD. Isso demonstra que a proteção à privacidade está diretamente relacionada a um dos pilares do Estado Democrático de Direito, que é o respeito ao indivíduo. Embora possa parecer óbvio nos dias de hoje, essa concepção de indivíduo não era considerada em outras formas de organização estatal, sendo uma característica distintiva do Estado Moderno.

2.2 Princípios

Os princípios constituem indispensável elemento da interpretação dos textos legais, são mandamentos jurídicos primaciais e fundamentais, compostos de valores da cultura sociojurídica de uma sociedade, servindo de substrato a outras normas jurídicas que conjuntamente servirão como fundamento para solução de casos concretos.

Conhecer princípios equivale a conhecer a essência da matéria, facilitando, sobremaneira, a dissecação do objeto de estudo. Desconhecer os princípios, de maneira reversa, é caminhar laboriosamente por entre disposições e preceptivos, sem visão de largueza e amplitude, prejudicando, de maneira definitiva, a possibilidade de investigar e conhecer o objeto (PESTANA, 2014).

A Lei Geral de Proteção de Dados, dentre diversas disposições, voltou-se, cuidadosamente, a estabelecer os princípios que deverão ser respeitados por ocasião do tratamento de dados. Importa ressaltar que quando uma norma é denominada principiológica, significa que ela tem uma maneira específica de ser interpretada. Nesse sentido, define Alexy:

> O ponto decisivo na distinção entre regras e princípios é que princípios são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes. Princípios são, por conseguinte, mandamentos de otimização, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas. O âmbito das possibilidades jurídicas é determinado pelos princípios e regras colidentes (ALEXY, 2006, p. 90).

Isto posto, os princípios elencados no artigo 6º da LGPD têm importância significativa na compreensão e aplicação das normas. No *caput* deste artigo vê-se que, além dos princípios, deve-se observar a boa-fé, que, neste contexto é objetiva, pois trata de relações jurídicas em que interessam as repercussões de determinadas condutas, principalmente em relação àquelas de caráter obrigacional (LÔBO, 2017). Assim, passamos a analisar brevemente, cada princípio individualmente.

2.2.1 Finalidade

O primeiro princípio, previsto no art. 6°, inciso I, da LGPD, é o da finalidade, definido pelo normativo como a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Conforme Doneda:

> Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade) (DONEDA, 2006, p. 216).

O princípio da finalidade estabelece a importância da concordância entre as partes sobre o propósito do tratamento de dados. Nesse contexto, pretende-se dar ao titular dos dados a prerrogativa de analisar se a coleta daquele dado específico tem uma justificativa válida. Considerando que os dados só podem ser tratados com a autorização do titular, é essencial garantir que não haverá desvio da finalidade acordada para a coleta e tratamento dos dados no contrato.

Dessa forma, o controlador e o operador estão vinculados à finalidade previamente acordada, evitando o uso de artifícios para destinar os dados a usos não autorizados. Isso cria uma obrigação de aderir estritamente ao pacto, de modo que os controladores devem definir claramente, desde a concepção do projeto, para quais finalidades os dados serão utilizados.

Por outro lado, esse princípio também qualifica tais propósitos, exigindo que sejam legítimos, específicos, explícitos e informados ao titular. Na verdade, isso representa a concretização da boa-fé, juntamente com os adjetivos que devem orientar uma manifestação de vontade plenamente válida. Em outras palavras, impede que as cláusulas sejam obscuras ou

dúbias no que se refere à finalidade, considerando que o titular deve avaliá-las para concordar com a operação.

2.2.2 Adequação

Com o intuito de garantir a tutela dos direitos do titular de dados pessoais, o legislador apontou no artigo 6º, II, da LGPD, o princípio da adequação. Ele estabelece que os dados pessoais tratados devem ser compatíveis com a finalidade informada pelo agente e de acordo com o contexto de tratamento.

Por exemplo, se a empresa solicitar dados para envio de boletim informativo e depois quiser gerar uma pontuação para a pesquisa qualitativa de algum produto, ela terá que buscar uma nova autorização. Além disso, o uso deve ser adequado ao propósito do relatório original. Mesmo que não haja uma nova finalidade, o uso indevido de informações produzirá desconformidades. MACHADO; MARCONI, 2020, p. 2608).

A adequação refere-se, portanto, ao nexo de pertinência lógica de conformidade que se estabelece entre o tratamento, a finalidade objetivada e a comunicação transmitida ao titular.

2.2.3 Necessidade

Previsto no inciso III do artigo 6º, da LGPD, o princípio da necessidade consubstancia-se na limitação do tratamento de dados pessoais ao mínimo necessário para realização da finalidade objetivada, com abrangência dos dados pertinentes e proporcionais.

Isso implica que os agentes de tratamento devem utilizar apenas os dados estritamente necessários para alcançar a finalidade previamente delimitada e quando aplicável, aprovada pelo titular dos dados. A coleta e o uso dos dados devem ser limitados ao que for imprescindível para atingir essa finalidade. Qualquer desvio desse princípio seria inadequado, uma vez que seria impróprio tratar dados impertinentes ou excessivos.

2.2.4 Livre Acesso

Este princípio, disposto no art. 6º, inciso IV, é reforçado no art. 9º da LGPD, o qual estipula que além de assegurar clareza sobre a forma e a duração do tratamento, se garanta também a integridade dos dados do titular. Assim, deve-se garantir aos titulares a

“consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”.

Isto é, deve haver um canal para que o titular tenha acesso às suas informações tuteladas pelo controlador. Este princípio gera uma obrigação para o controlador, que deve possibilitar ao titular o acesso aos seus dados para que ele possa avaliar se o tratamento está sendo feito de maneira adequada.

Além disso, as informações devem ser fornecidas de forma clara, adequada e óbvia sobre os seguintes pontos: i) finalidade específica do tratamento; ii) identificação do controlador; iii) informações de contato do controlador; iv) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; v) responsabilidades dos agentes que realizarão o tratamento (MACHADO; MARCONI, p. 2608-2609). Em suma, garante ao titular dos dados a transparência sobre suas informações.

2.2.5 Qualidade dos Dados

Conforme o inciso V, do art. 6º, a qualidade de dados é a “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”. Contudo, para isso, é imprescindível que eles sejam atualizados, claros e exatos, caso contrário, o titular dos dados poderá ser prejudicado. Maldonado e Blum explicam:

> Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico, recusa de crédito, vedação de participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta (MALDONADO; BLUM, 2019, p. 149).

Portanto, tal princípio consubstancia-se na garantia de exatidão, clareza, relevância e atualização desses dados. Desse modo, é essencial a atualização em banco de dados, tendo em vista que o contrato entre o titular e os agentes de tratamento pode perdurar por anos.

2.2.6 Transparência

Previsto no art. 6º, inciso VI da LGPD, o princípio da transparência visa garantir aos titulares de dados a prestação clara e acessível de informações sobre o tratamento e os respectivos agentes, resguardados os segredos industriais e comerciais.

Segundo Vainzof (2021, p.156), entende-se que este é essencial para atingir o objetivo da legislação, que é proteger a privacidade e o livre desenvolvimento da personalidade, pois sem que o titular tenha fácil acesso as informações claras e precisas sobre o tratamento dos seus dados, não há como garantir a referida tutela.

Este princípio deve, notadamente, ser observado desde antes do fornecimento do consentimento, por parte do titular. É importante destacar que a transparência não se refere apenas aos processos que envolvem os dados do titular, mas, também, a informações sobre a identidade do responsável pelo tratamento de dados e suas respectivas características.

Assim, a transparência do tratamento de dados deve acontecer desde a fase inicial, a de coleta, até a fase final, de eliminação dos dados de maneira clara e sem barreiras técnicas.

> O titular dos dados carece de ampla informação sobre o tratamento dos seus dados para que consiga enxergar, cristalinamente, a legalidade, a legitimidade e a segurança do tratamento de acordo com o seu propósito, adequação e necessidade. Assim, terá condições para refletir sobre o tratamento e tomar decisões de acordo com os seus direitos. A transparência deve ser diretamente proporcional ao poder do tratamento dos dados pessoais (qualitativo e quantitativo) e à capacidade de assimilação dos titulares dos novos e dinâmicos produtos e serviços apresentados para o seu uso (MALDONADO e BLUM, 2019, p. 150).

É factível verificar isso em situações anteriores à entrada em vigor da LGPD. O primeiro passo das autoridades é questionar informações que foram negadas aos usuários, as quais, se tivessem sido disponibilizadas previamente, poderiam ter influenciado sua decisão de consentir. Além disso, diante do não cumprimento, só é possível responsabilizar os culpados quando há informações detalhadas sobre o processo.

Por conseguinte, pode-se afirmar que a principal força da LGPD e de outras legislações reside no sistema de *accountability* (responsabilização) formado por suas regras e princípios. No que tange às regras, destacam-se os artigos 9º, 18 e 19, os quais essencialmente estipulam que o titular dos dados tem o direito de acessar as informações pertinentes de forma simplificada. O objetivo é que o titular seja o principal fiscal das atividades dos controladores de dados.

2.2.7 Segurança

O princípio da segurança, conforme estabelecido no artigo 6º, inciso VII, compreende a implementação de medidas técnicas e administrativas destinadas a proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Esse princípio, em conjunto com o princípio da prevenção, tem como objetivo central preservar um ambiente seguro, utilizando e aprimorando constantemente as técnicas de segurança para mitigar e prevenir possíveis incidentes.

O tratamento de dados pessoais requer a implementação de medidas técnicas e administrativas para protegê-los de acesso não autorizado, bem como de destruição, perda, alteração, comunicação ou difusão acidentais ou ilícitas. Esse princípio visa garantir a segurança dos dados em um ambiente protegido, utilizando técnicas de segurança contemporâneas e procedimentos aprimorados, especialmente para entidades jurídicas que realizam o tratamento.

É essencial ressaltar que, independentemente da causa (voluntária ou acidental), o responsável pelo tratamento deve prever e se precaver contra todas as possíveis situações de acesso indevido aos dados. No entanto, os titulares dos dados têm direito a acessar seus dados tratados de forma autorizada, com cautelas procedimentais e técnicas constantemente atualizadas.

2.2.8 Prevenção

O princípio da prevenção é um pilar fundamental no contexto da proteção de dados pessoais, embora entendamos que ele se encontra inserido no princípio anteriormente examinado, resolveu o legislador prestigiar de maneira expressa a prevenção, visando antecipar e mitigar potenciais riscos associados ao tratamento de dados, antes mesmo que tais incidentes ocorram. Em sua essência, ele demanda a implementação proativa de medidas técnicas e administrativas destinadas a evitar violações de segurança e garantir a integridade, confidencialidade e disponibilidade dos dados.

Sob uma perspectiva jurídica, o princípio da prevenção implica o dever das organizações de adotar políticas, processos e controles que assegurem o cumprimento das normas de proteção de dados desde o início do ciclo de vida dos dados. Ademais, sob a ótica técnica, esse princípio exige a utilização de tecnologias e práticas avançadas de segurança da

informação, como criptografia, autenticação multifatorial e monitoramento contínuo, a fim de proteger os dados contra ameaças internas e externas.

Em suma, o princípio da prevenção na LGPD representa um compromisso contínuo e abrangente com a proteção dos dados pessoais, estabelecendo uma cultura organizacional voltada para a segurança e a conformidade com a legislação de proteção de dados.

2.2.9 Não Discriminação

Segundo o princípio da não discriminação, previsto no art. 6º, inciso IX, é vedada a utilização de dados pessoais com fins discriminatórios considerados ilícitos ou abusivos, sendo que esses dois aspectos são confluentes para caracterizar certas condutas como discriminatórias.

De acordo com Mulholand (2018), é possível o tratamento diferenciado de dados, mas desde que respeitado o princípio da boa-fé, mencionada no *caput*, do art. 6º da lei em análise. Nesse sentido:

> Aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas. Assim, por exemplo, seria legítimo a um operador de dados que esteja realizando a precificação de um serviço de seguros de automóveis, tratar de maneira diferenciada os dados de mulheres entre 35 e 45 anos e mães, com a finalidade de oferecimento de um valor que reflita os riscos de danos usualmente ocasionados ou sofridos por esse grupo determinado de pessoas (MULHOLLAND, 2018, p. 163-164).

Assim, é imperioso observar que no momento do tratamento dos dados pessoais, é proibida a exclusão de informações específicas relacionadas às características individuais, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde, ou orientação sexual, sob pena de transgressão ao princípio da boa-fé.

2.2.10 Princípio da Responsabilização e Prestação de Contas

O princípio da responsabilização e prestação de contas, consagrado no artigo 6º, inciso X da Lei Geral de Proteção de Dados (LGPD), estabelece que os agentes de tratamento de dados devem ser responsáveis pela conformidade com as disposições legais e

regulamentares relativas à proteção de dados pessoais. Isso implica que tais agentes devem adotar medidas eficazes para garantir o cumprimento das normas de proteção de dados em todas as fases do tratamento, desde a coleta até a exclusão dos dados. Nesse sentido:

> Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos. (MALDONADO; BLUM, 2019, p. 166-167).

É relevante ressaltar que, segundo Rosenvald (2017), o conceito de responsabilidade civil transcende sua função meramente restaurativa, desempenhando também um papel preventivo e civilizatório. Nesse contexto, o princípio da prestação de contas assume uma importância significativa para este estudo.

Essa abordagem visa promover uma cultura de transparência e responsabilidade no tratamento de dados pessoais, garantindo que os agentes de tratamento assumam a responsabilidade pelo manejo adequado e seguro dos dados sob sua custódia. Isso não apenas protege os direitos dos titulares de dados, mas também fortalece a confiança na gestão e proteção de dados em conformidade com a Lei Geral de Proteção de Dados.

2.3 Categorias de Dados Pessoais

No inciso I do artigo 5º, da LGPD, temos a definição de dado pessoal como qualquer "informação relacionada à pessoa natural identificada ou identificável" (BRASIL, 2018). Observe que este dispositivo veio complementar o artigo 7º do Marco Civil da Internet (MCI), especificamente em seu inciso um, que já estabelecia como direito do usuário a "I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação".

Há duas classificações de dados pessoais: a reducionista e a expansionista. Segundo a teoria reducionista, dado pessoal consiste em uma informação que deve estar associada a algo específico, ou seja, deve possuir um vínculo direto e inequívoco com seu titular. Por exemplo, um determinado número de CPF está vinculado diretamente a um titular específico. Em contrapartida, a visão expansionista, amplamente adotada, define dado pessoal de forma mais abrangente. Nesta perspectiva, a necessidade de uma associação direta entre dado e titular é desconsiderada. De acordo com essa teoria, dado pessoal pode ser qualquer

tipo de informação que permita a potencial identificação do seu titular, mesmo que não haja um vínculo direto com a informação (BIONI, 2020, p. 16). Assim, conforme sintetiza Bioni (2020):

> Ainda que divergentes, tais teorizações detêm o mesmo centro gravitacional. Ambas demandam uma análise contextual donde está inserido um dado, aferindo-se o seu grau de "identificabilidade" para, então, desencadear a compreensão se uma determinada informação está relacionada a uma pessoa identificada ou identificável. (SCHWARTZ; SOLOVE, 2011, apud BIONI, 2020, p. 17).

O mesmo artigo 5º da LGPD define, ainda, o que é dado pessoal sensível, dado pessoal anonimizado, banco de dados e anonimização de dados, conforme se observa a seguir, *in literis*:

> II - **dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - **dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - **banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; (...) XI - **anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. (BRASIL, 2018).

Há, portanto, três categorias de dados pessoais, a seguir analisaremos cada uma delas e seus aspectos-chaves.

2.3.1 Dados Pessoais *Lato Sensu*

Os Dados Pessoais *Lato Sensu* englobam informações referentes a uma pessoa física identificada, bem como um conjunto de informações distintas que, em conjunto, podem levar à identificação dessa pessoa. Exemplificativamente, incluem-se nesta categoria o nome, apelido, data de nascimento, endereço de *Internet Protocol* (IP), imagens obtidas por sistemas de "videovigilância" e gravações de chamadas telefônicas. Ademais, conforme o § 2º do art. 12 da Lei Geral de Proteção de Dados (LGPD), serão igualmente considerados como dados pessoais aqueles utilizados para a formação do perfil comportamental de determinada pessoa natural, desde que identificada. Contrariamente, não se enquadram como dados pessoais, por exemplo, o Número de Identificação do Registro de Empresas (NIRE), que se aplica a pessoas jurídicas e, portanto, não permite a identificação direta de indivíduos.

2.3.2 Dados Pessoais Sensíveis

Seguindo essa linha de raciocínio, a segunda categoria é a de Dados Pessoais Sensíveis, esses dados estão relacionados a questões mais subjetivas e comportamentais, e devido ao seu potencial de causar danos mais significativos, seu tratamento deve obedecer às regras mais rigorosas, uma vez que dizem respeito a direitos personalíssimos, como raça, opinião política e vida sexual, conforme discutido anteriormente. Portanto, é necessário obter o consentimento específico e destacado do titular para o seu tratamento.

Cabe destacar que, durante o debate de construção da lei, alguns setores trabalharam para a retirada dos dados genéticos ou biométricos do conceito. Porém o texto original do PL 5276/2016 não faz essa vinculação a uma pessoa natural. A Associação Brasileira de Marketing de Dados (ABEMD) foi um dos grupos que articulou por uma definição que vinculasse expressamente os dados sensíveis à identificação de uma pessoa natural.

Em sua contribuição ao texto, Vitor Moraes de Andrade, assessor da ABEMD indicou a seguinte definição para dados sensíveis:

> III - dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos. salvo quando a utilização destes últimos for exclusivamente para identificação de pessoas naturais, hipótese em que o dado será considerado pessoal, nos termos do inciso I (ANDRADE, 2022).

O grupo argumenta que o texto original considerava indiscriminadamente informações biométricas sem levar em conta a finalidade de seu uso. Para eles, isso poderia resultar em restrições desnecessárias na utilização desses dados. Assim como a Associação Brasileira de Marketing de Dados (ABEMD), o Facebook, a Associação Brasileira das Empresas de Software (ABES) e a Câmara Americana de Comércio (AMCHAM) foram grupos que defenderam essa definição correlacionada a essa perspectiva.

Conforme exposto, a Lei 13.709/2018 (LGPD) regula como dados pessoais sensíveis aqueles que relacionados a sete categorias específicas, a saber: origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso, filosófico ou político; dados referentes à saúde ou à vida sexual; e dados genéticos ou biométricos quando vinculados a uma pessoa natural. Essas informações são consideradas

sensíveis e são protegidas pela lei de forma especial, garantindo o Princípio da Não-Discriminação e a privacidade dos indivíduos.

Entretanto, mesmo quando o dado pessoal é classificado como sensível, a legislação brasileira de proteção de dados pessoais permite o tratamento desse tipo de informação em certas circunstâncias. Tais circunstâncias são delineadas no artigo 11, sendo a primeira delas estabelecida pelo consentimento do titular. No entanto, o texto prevê uma série de exceções para o tratamento desses dados sem a necessidade do consentimento do titular. São sete situações que se concentram na execução de políticas públicas, realização de pesquisas e estudos, proteção da vida e tutela da saúde, além de garantir a prevenção à fraude.

2.3.3 Dados Anonimizados

Por fim, o último conceito é o de Dados Anonimizados, sendo esse um dos mais debatidos no processo de formulação da lei. O texto final admitiu a possibilidade de anonimização e de existência de tais dados, definindo-os como aquele dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Em seu art. 12, a lei dispõe que os dados anonimizados não serão considerados dados pessoais, ou seja, caso os dados sejam anonimizados em sua totalidade deixarão de ser tutelados pela LGPD, no entanto, deve-se garantir que os dados não sejam passíveis de reversão, ou seja, que não seja possível reidentificar o indivíduo a partir dos dados.

A definição de dado anonimizado envolve três critérios essenciais: (I) a impossibilidade de se atribuir identidade ao indivíduo; (II) a inexistência de uma forma conhecida e sistemática de (re)identificar os dados; e (III) a incapacidade de conectar dois ou mais registros de uma mesma pessoa.

Os métodos comuns de anonimização existentes são: (I) a supressão, em que os valores são completamente removidos ou substituídos por um valor fictício, como um asterisco (*), sendo normalmente aplicável, aos identificadores explícitos; (II) a generalização, consistente na modificação da escala ou ordem, como uma data de nascimento; (III) a permutação, que divide os dados em grupos e os embaralha; (IV) e por fim, a perturbação, que diz respeito à substituição de valores removendo o *link* ao dado original, mas mantendo suas propriedades estatísticas.

No contexto atual, a dificuldade está em avaliar se os métodos disponíveis de anonimização produzem, de fato, dados que são legitimamente anônimos. De acordo com

Bioni (2020), o dado anônimo seria a antítese de dado pessoal, ao impedir a identificação da pessoa natural. Neste sentido, qualquer dado anonimizado possui o risco inerente de se tornar um dado pessoal, haja vista que sua identificabilidade é remota e não imediata.

Desse modo, torna-se prudente entender a anonimização e o conceito de dados anonimizados como um processo, mutável e por meio do qual se torna possível manter a utilidade de um banco de dados, e não como um artifício para esgueirar-se do regulamento de proteção de dados e das obrigações que este impõe.

2.4 Consentimento

Em um Estado Democrático de Direito, a regulação jurídica do tratamento de dados está amparada na ideia de que o indivíduo goza de autodeterminação informacional, ou seja, "tem o poder para controlar livremente a revelação e a utilização dos seus dados pessoais na sociedade, preservando, assim, sua capacidade de livre desenvolvimento de sua personalidade" (MENDES, 2014, p.60).

Assim, para que o indivíduo possa exercer sua autodeterminação informativa, torna-se necessário um instituto jurídico que o permita expressar sua vontade de autorizar ou não o processamento e tratamento de seus dados. Em seu artigo 5º, inciso XII, a LGPD define o consentimento como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados para uma finalidade determinada" (BRASIL, 2018).

Em complemento ao artigo 5º, o artigo 7º da LGPD, elenca o consentimento como uma das dez bases legais para o tratamento de dados:

> CAPÍTULO II
> DO TRATAMENTO DE DADOS PESSOAIS
> Seção I
> Dos Requisitos para o Tratamento de Dados Pessoais
> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular; (BRASIL, 2018)

Ademais, o artigo 8º também da LGPD estabelece que o consentimento deverá ser fornecido por escrito ou por qualquer outro meio que ateste a manifestação de vontade do titular e, caso fornecido por escrito, deverá constar em cláusula destacada das demais.

Cabe ao controlador de dados o ônus da prova de que o consentimento foi obtido dentro dos limites legais. Outra previsão legal é a de que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular. Outrossim, a LGPD

veda o tratamento de dados pessoais mediante vício de consentimento, além de ater-se ao dever respeitar finalidades já determinadas, sendo consideradas nulas as autorizações genéricas.

Insta salientar que no §1º do art. 9º da LGPD é estabelecido que, caso as informações fornecidas ao titular, quando o consentimento for requerido, tenham conteúdo enganoso ou abusivo ou que sua apresentação não tenha sido com transparência, de maneira clara e inequívoca, o consentimento será considerado nulo.

Apesar disso, quando se observa a realidade dos titulares de dados, usuários de aplicativos, sites e plataformas digitais sequer leem os termos de política e privacidade e de uso dos respectivos controladores e, quando o fazem, acabam muitas vezes não entendendo o texto pelo linguajar técnico.

> Mais do que isso, caso o usuário não concorde com os termos apresentados, é comum que sua única opção seja não desfrutar de importantes produtos e serviços online. Entretanto, assim fazendo, acaba enfrentando elevados custos sociais (MENDES; FONSECA, 2020, p. 352).

Nesse cenário, é evidente que o titular de dados encontra-se em uma situação de vulnerabilidade perante os controladores, visto que resta presente uma relação assimétrica de poder entre quem disponibiliza e quem obtém esses dados, isso porque o consentimento não é a única base legal capaz de assegurar a autodeterminação informativa, devendo haver uma conjugação de princípios e dispositivos legais favoráveis aos titulares de dados, a fim de que seu direito à proteção de dados seja devidamente observado e respeitado.

2.5 Proteção dos Dados Pessoais à luz da Constituição Federal

O ordenamento jurídico brasileiro estabelece uma série de regras a condutas a serem observadas com o fim de garantir proteção aos direitos do titular dos dados durante todo o processo de tratamento. Dentre os direitos fundamentais assegurados pela lei, destacam-se de maneira pertinente ao presente estudo o direito à liberdade, à privacidade e o livre desenvolvimento da pessoa humana.

O direito fundamental à liberdade encontra escopo no art. 5º, *caput*, da Constituição Federal. Esse dispositivo, estabelecido como cláusula geral, deu abertura para a interpretação de liberdades fundamentais especiais, como a de manifestação de pensamento,

liberdade de expressão, religiosa, entre outras, que embora não nominadas derivam implicitamente da ordem jurídica.

Referente à matéria de dados pessoais, A promulgação da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, marcou um momento histórico no ordenamento jurídico brasileiro ao incluir, no rol de direitos e garantias fundamentais, a proteção de dados pessoais. O inciso LXXIX do artigo 5º da Constituição Federal passou a dispor que "*é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais*."

A partir desse cenário de vigilância constante em que os indivíduos estão inseridos, o direito fundamental à liberdade garante, como regra, a escolha de disponibilizar ou não seus dados a outrem, não sendo constrangido a fazê-lo.

No tocante ao direito à privacidade, tutelado no art. 5º, X da Constituição Federal com a seguinte redação "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988). Ainda, o art. 21 do Código Civil reforça esse entendimento e traz um fundamento jurídico de seguridade ao indivíduo que tem sua privacidade violada, garantindo-lhe acesso ao judiciário a fim de que ele tome medidas para cessar ou impedir tal violação.

O conceito preliminar de direito à privacidade sofreu algumas modificações ao longo dos anos. A Constituição Imperial (1824), limitava-se a abranger apenas o direito à propriedade e o sigilo de correspondências, ou seja, à inviolabilidade da propriedade e das comunicações.

Com o advento da sociedade da informação, ocasionado pelos avanços tecnológicos e a facilidade de adquirir e transmitir informações, foi imperioso modificar e ampliar a abrangência do direito à privacidade. Um artigo publicado na Haverd Law Review, denominado "*The Rightto Privacy*", argumentava a necessidade de um conceito de direito à privacidade mais abrangente, chegando-se à conclusão de que a privacidade seria um "direito de ser deixado só" (BRANDEIS; VAZ, 1890, p.193).

Assim, a tutela da privacidade, em sua nova acepção, não se resume ao dever geral de abstenção à vida íntima de outrem, impondo, também, deveres de caráter positivo, como o de solicitar autorização para a inclusão de determinada pessoa em um cadastro de dados. Desse modo, é imprescindível que outros direitos sejam analisados, como a autodeterminação informativa, que foi trabalhada em tópicos anteriores do presente estudo.

Em relação ao livre desenvolvimento da personalidade, jurisprudencial e doutrinariamente entende-se que Tal inclusão evidencia a crescente relevância da proteção de dados no cenário nacional e internacional, consolidando a ideia de que os dados pessoais são uma extensão da personalidade do indivíduo e, portanto, merecem proteção jurídica robusta.

Um exemplo é o direito que o titular dos dados tratados tem de demandar a correção de dados inexatos, incompletos ou desatualizados. Tal proteção é mandamental, pois, em se tratando de uma sociedade de vigilância, as informações de cunho pessoal associadas à personalidade de um indivíduo em específico, podem não apenas identificá-lo, mas também impactar o exercício de sua cidadania.

Dessa forma, para salvaguardar esses direitos fundamentais, que é o objetivo da lei através da regulamentação do procedimento de tratamento de dados, deve ser observado pelo as normas impostas, caso contrário, deverão responder pelos prejuízos causados aos titulares de dados.

2.6 Crimes Digitais e Mercantilização dos Dados

Durante a pandemia de Covid-19, o número de usuários na internet aumentou exponencialmente devido ao isolamento social, que forçou muitos a trabalharem em *home office* e a realizarem transações bancárias *online*. Embora a tecnologia tenha agilizado muitas tarefas, também levou a um aumento significativo de crimes digitais no Brasil, resultando em consequências muitas vezes irreparáveis, incluindo danos psicológicos.

Com o passar do tempo e a evolução das tecnologias novas formas de acessar os dados e cometer diferentes crimes foram surgindo, sendo necessária atenção legislativa e meios eficazes de investigação no meio digital, pois muitos dos autores delitivos valem-se do anonimato para não deixar rastros, sendo impossível identificá-los.

É certo que com o passar dos anos o número de cidadãos com dados coletados sem sua autorização, senão quando vazados, aumenta de forma exacerbada. Em 2021 a sociedade empresária PSAFE, responsável por detectar vazamento de dados, constatou o vazamento de mais de 200 milhões de dados brasileiros no início do ano, esses estavam sendo comercializados em grupos de criminosos cibernéticos, expondo assim a vulnerabilidade do sistema de proteção dos dados pessoais (PECSEN, 2021).

Segundo o Ministro do Superior Tribunal de Justiça (STJ) Humberto Martins, em entrevista ao seminário virtual de criminalidade em tempos de Covid-19:

> Cabe ao Estado brasileiro aprimorar seu arcabouço normativo para impedir que esses crimes sejam praticados, evitando prejuízos financeiros e patrimoniais às pessoas, às empresas e ao próprio poder público", declarou, pois os criminosos passaram a praticar fraudes eletrônicas ao perceber o uso intenso da internet no período da pandemia (MARTINS, 2022).

A maioria dos golpes quando aplicados nascem a partir de fraudes, seja por envio de comprovantes falsos de depósito e boletos de pagamento de lojas falsas, aquisição de *login* e senha dos usuários para realizar compras em seu nome e anúncios falsos. Uma pesquisa feita por empresas que atuam no comércio online e apresentada na terceira edição da Semana de Segurança revelou que o Brasil é o segundo país com mais crimes digitais na América Latina, ficando atrás apenas do México.

De acordo com a pesquisa, entre janeiro e setembro de 2023 ocorreram cerca de 80mil golpes na compra e venda online de produtos, uma média de 9mil golpes por mês, resultando num prejuízo de cerca de R$ 529 milhões. O estudo também apontou que a maioria das vítimas de fraudes são homens (73%), e desses, 71% têm até 31 anos, sendo a região Sudeste a que mais teve fraudes.

2.6.1 *Phishing*

Um dos golpes mais comuns em crimes cibernéticos é o *Phishing*, que visa roubar dados pessoais, como nome, CPF, RG, além de informações bancárias e senhas, para realizar extorsões. O termo *phishing* vem do inglês "pescar" e se refere à prática de enviar e-mails com links ou anexos maliciosos que, quando clicados, instalam vírus no dispositivo da vítima, permitindo acesso a todos os dados nele contidos. Esses criminosos exploram a ingenuidade e o desconhecimento dos usuários sobre tais fraudes. Com o aumento do número de usuários na internet, muitos desconhecem esses perigos e acabam clicando em links suspeitos, permitindo que os criminosos "pesquem" suas informações.

2.6.2 *Smishing*

Smishing envolve o envio de mensagens persuasivas via torpedos ou SMS, em que os criminosos se passam por sua operadora de celular ou por lojas renomadas, afirmando que você ganhou um prêmio e solicitando que clique em um link para reivindicá-lo. Ao clicar no link, todos os seus dados são roubados.

2.6.3 *Pharming*

O termo *Pharming* é uma combinação de "phishing" e "farming" e tem a mesma finalidade de roubar dados pessoais dos usuários da internet, mas de uma forma diferente. No *Pharming,* o tráfego de um site é manipulado para redirecionar o indivíduo de um site legítimo para um site malicioso, onde são instalados softwares maliciosos, ou "vírus", no dispositivo, possibilitando o roubo de dados pessoais.

2.6.4 Man in The Middle Attack

Esse é um dos ataques mais difíceis de detectar, pois o invasor se passa por uma das partes que recebe a informação. O objetivo é o mesmo dos outros ataques: roubar dados. Nesse golpe, o invasor intercepta o tráfego da internet antes que ele chegue ao destinatário. Por exemplo, ao acessar "www.google.com.br", o tráfego passa por diversos roteadores até chegar ao Google. O invasor se faz passar por um desses roteadores, recebendo a informação. Ele pode atuar como um ponto de Wi-Fi falso, nomeado como um roteador público, e se posicionar entre você e suas transações bancárias online, seus e-mails de trabalho ou seus chats. Dessa forma, o dispositivo da vítima acaba "conversando" com um impostor disfarçado do site real, permitindo ao invasor acessar e roubar todas as informações enviadas ou recebidas, incluindo dados pessoais.

Visto na exemplificação os quatro dos mais famosos e comuns crimes digitais da atualidade, pode-se exprimir que os titulares de dados são alvos constantes desses crimes, estando em situação de vulnerabilidade com pouca segurança efetiva e, mesmo com a LGPD, é necessário que ela seja atualizada de maneira ágil para prevenir a prática e minimizar os danos.

3 RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO

A noção da responsabilidade pode ser extraída da etimologia da própria palavra, que vem do latim *respondere,* responder a alguma coisa, ou seja, a necessidade de que o indivíduo seja responsabilizado por seus atos danosos. No âmbito do direito obrigacional, a responsabilidade civil é um conceito fundamental, pois está vinculado ao

reconhecimento e à proteção dos direitos pessoais. Quando o ordenamento jurídico estabelece direitos, ele visa regular as relações entre indivíduos e prevenir a violação desses direitos.

Os artigos 186 e 187 do Código Civil definem o que é ato ilícito:

> **Art. 186**. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito (BRASIL, 2002).
>
> **Art. 187.** Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes (BRASIL, 2002).

Por sua vez, o artigo 927 do Código Civil trata do dever de reparação:

> **Art. 927.** Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo (BRASIL, 2002).

No contexto do direito civil, uma violação é considerada um ato ilícito que acarreta a obrigação de reparação. Consequentemente, estabelece-se um vínculo jurídico que confere a uma parte o direito de exigir da outra o cumprimento de uma determinada obrigação ou prestação. Nesse sentido, a doutrina brasileira se ocupou em classificar certos aspectos da responsabilidade civil, culminando nas teorias da responsabilidade civil subjetiva e objetiva, na qual seus fundamentos passam a ser expostos a seguir.

3.1 Responsabilidade civil subjetiva

A teoria da responsabilidade civil subjetiva teve origem na Lei Aquiliana e foi adotada pelo sistema jurídico brasileiro no Código Civil de 1916, com sua revogação e a vigência do atual Código Civil de 2002, a responsabilidade civil subjetiva passou a ser tratada no já trazido artigo 186 do Código Civil, tendo como pressuposto para a imputabilidade do agente que causa dano a outrem a existência de culpa. Portanto, aquele que descumpre um dever legal estabelecido na norma jurídica ou viola um dever de cuidado agindo de maneira negligente, imprudente ou imperita fica obrigado a reparar o dano.

Para Pontes de Miranda:

> [...] a culpa é defeito que se pode apontar na vontade. Supõe-se que o agente, no que quis, passou o limite em que sua atividade ou a sua omissão seriam sem defeito, [...] a culpa em sentido amplo, abrange a culpa; porque é culpado quem pratica ato, ou deixa de o praticar, com dolo (MIRANDA, 1958).

O artigo 186 do Código Civil determina a existência de ato ilícito quando há ação ou omissão voluntária, na ação voluntária é mais fácil verificar a culpa do agente, pois ela é um comando nítido do agente, já no caso da omissão o exercício para aferição da culpa é diferente, devendo ser feito o questionamento se a pessoa poderia ou deveria ter agido para evitar o resultado, ou ainda, se a omissão foi determinante para o dano causado a terceiro.

Nesse sentido entende Pontes de Miranda que "a abstenção, omissão, ou ato negativo, também pode ser causa de dano. Se o ato cuja prática teria impedido, ou, pelo menos, teria grande probabilidade de impedir o dano, foi omitido, responde o omitente" (MIRANDA, 1958, p. 193). No âmbito do direito público, a omissão do Estado também é relevante para o estudo, segundo Yussef Said Cahali:

> [...] desde que exigível da administração a execução da obra ou a prestação do serviço que teriam prevenido ou evitado o evento danoso sofrido pelo particular, identifica-se na conduta omissiva estatal a causa bastante para determinar a responsabilidade objetiva14 do Estado por sua reparação: no simples conceito de descumprimento de obrigação exigível já está embutida a ideia de culpa, só elidível se não demonstrada a excludente da inexigibilidade do ato omitido, posto como causa do dano, se demonstradas as exceções convencionais do caso fortuito, da força maior ou do ato próprio do ofendido (CAHALI, 2007).

Conforme se depreende do texto do artigo 186 do Código Civil, a imputabilidade do ato ilícito não se condiciona apenas à verificação da culpa, mas também a existência de um dano propriamente dito, seja patrimonial, seja moral ou ambos, além destes, deve estar presente o nexo de causalidade entre o dano e a conduta ilícita do agente.

3.2 Responsabilidade civil objetiva

A responsabilidade civil objetiva tem escopo legal no artigo 927 do Código Civil, que dispõe:

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

O fundamento teórico da responsabilidade objetiva não é a culpa, mas o dever de cuidado do agente, ou seja, ele é responsável, *a priori*, porque não observou o dever de

cuidado que lhe era imanente. Um exemplo é a responsabilidade do Estado, por meio dos impostos os cidadãos tem a garantia de uma boa prestação de serviços públicos e, esse dever se considera inobservado quando, dos serviços estatais, advenha algum dano.

Cabe ressaltar que as excludentes da responsabilidade objetiva recaem somente quando há quebra do nexo de causalidade, que pode ser por caso fortuito ou força maior e fato exclusivo da vítima ou de terceiro. São exemplos de responsabilidade civil objetiva as decorrentes das relações de consumo, do abuso de direito, do estado de necessidade e do risco integral.

Um marco intransponível no que tange a responsabilidade civil e sua influência para a LGPD é o Código de Defesa do Consumidor, Lei nº 8.078 de 1990. A Constituição, ao determinar que o Estado promovesse a defesa do consumidor, reconheceu a vulnerabilidade deste e, consequentemente, no Código de Defesa do Consumidor, a responsabilidade pelos danos causados em decorrência da relação de consumo independe de prova de culpa, salvo a responsabilidade dos profissionais liberais.

Fato é que, a evolução tecnológica tem levado a uma mudança significativa na forma como os fatos jurídicos e institutos do direito são tratados, adaptando-os para abarcar novas peculiaridades. Nesse contexto, novas perspectivas de responsabilidade civil se estabelecem, com a crescente ampliação das hipóteses de responsabilidade civil objetiva, a jurisprudência tem avançado na ampliação das hipóteses de indenização pelos danos presumidos.

No que tange às disposições da LGPD, uma vez em posse (legítima e consentida) dos dados pessoais ou sensíveis, os agentes de tratamento têm a liberdade para tratá-los, desde que observados os princípios e limites estabelecidos pela legislação e regulação oriunda da Autoridade Nacional de Proteção de Dados. A não observância dessas diretrizes resulta em responsabilidade civil, tema que será abordado nos próximos tópicos.

4. RESPONSABILIDADE CIVIL E A LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados regula o tratamento de dados pessoais, tanto digitais, quanto analógicos, realizados por indivíduos ou entidades públicas e privadas, com o objetivo de proteger os direitos fundamentais à liberdade, privacidade e ao desenvolvimento pessoal.

No Capítulo VI, Seção III, da lei 13.709/2018, que aborda a responsabilidade e a compensação por danos causados pelos agentes de tratamento, o artigo 42 estabelece que

agentes de tratamento, controladores ou operadores devem reparar danos patrimoniais, morais, individuais ou coletivos se realizarem o tratamento de dados em desacordo com a legislação. Embora o artigo não mencione diretamente a culpa, também não a exclui explicitamente, exigindo que a reparação seja feita quando o tratamento de dados for lesivo e violar a legislação.

A responsabilidade é fundamentada em dois critérios principais: a realização da atividade de tratamento de dados e a violação da legislação aplicável. O inciso I do §1º do artigo 42 prevê que o operador pode ser solidariamente responsável se violar a lei ou agir em desacordo com as instruções do controlador, visando garantir a reparação dos danos.

Além disso, o inciso II do §1º do artigo 42 estabelece que os controladores também podem ser responsabilizados solidariamente se estiverem diretamente envolvidos no tratamento que causou danos ao titular dos dados, refletindo a complexidade das operações de dados compartilhados entre entidades públicas e privadas.

Marcos Gomes da Silva Bruno (2019) afirma que a LGPD não é clara quanto à aplicabilidade da responsabilidade subjetiva ou objetiva. A menção à responsabilidade objetiva foi retirada do texto de um dos projetos que ensejaram a redação atual da LGPD, conforme explicam Gustavo Tepedino, Aline Terra e Gisela Guedes:

> A versão inicial do Projeto de Lei nº 5276 trazia no capítulo sobre Transferências Internacionais de Dados, uma regra geral expressa de responsabilidade solidária e objetiva desses agentes pelos danos causados em virtude do tratamento de dados (artigo 35). Além disso, na seção sobre Responsabilidade e Ressarcimento de danos, havia uma abordagem ampla sobre os sujeitos obrigados a reparar o dano (“todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais causar dano a outrem”) (art. 42), e outra regra igualmente ampla prevendo a solidariedade entre todos os agentes da cadeia de tratamento, sem qualquer distinção entre controlador e operador. Diferentemente desse primeiro texto, todas as versões subsequentes do projeto, até a versão finalmente sancionada, passaram a não mais mencionar, como regra geral um regime de solidariedade ou objetividade na responsabilidade pelos danos decorrentes do tratamento de dados (TELEPEDINO, TERRA, GUEDES, 2021).

A inexatidão terminológica da lei confere ao intérprete a possibilidade de responsabilização a depender do agente de tratamento, se pessoa física ou jurídica de direito privado ou pessoa jurídica de direito público.

4.1 Controlador sendo um ente público

Ao ente público, a Lei Geral de Proteção de Dados destinou o capítulo IV “Do tratamento de dados pessoais pelo Poder Público”, com diversas particularidades em seu sistema de responsabilidade civil. Dispensou a ele uma série de deveres específicos em decorrência do tratamento de dados pessoais e delineou normas reguladoras do uso compartilhado de suas bases de dados entre órgãos da administração pública e entre entes privados.

Contrariamente, o legislador não tratou especificamente a responsabilidade civil dos entes públicos quando da verificação de danos decorrentes do tratamento de dados, a lei deixou a cargo do intérprete proceder sua interpretação. Nesta hipótese, a responsabilidade civil do ente público pode ser aferida por meio da teoria do risco administrativo, que se baseia no risco que a atividade pública oferece ao administrado, não aceitando excludentes na responsabilidade da administração, devendo o Estado suportar, independentemente de culpa, os danos sofridos por terceiros em quaisquer hipóteses.

O artigo 37, §6 da Constituição Federal prevê que nenhum particular deve suportar o dano decorrente de atividades voltadas para o interesse social da coletividade. Esta previsão adquire especial relevância nos tempos atuais em que se espera do poder público um planejamento capaz em garantir a eficiência e segurança de sua atuação, cabendo ressaltar a lição expendida por Odete Medauar:

> Informada pela ‘teoria do risco’, a responsabilidade do Estado apresenta-se hoje, na maioria dos ordenamentos, como ‘responsabilidade objetiva’. Nessa linha, não mais se invoca o dolo ou culpa do agente, o mau funcionamento ou falha da Administração. Necessário se torna existir relação de causa e efeito entre ação ou omissão administrativa e dano sofrido pela vítima. É o chamado nexo causal ou nexo de causalidade. Deixa-se de lado, para fins de ressarcimento do dano, o questionamento do dolo ou culpa do agente o questionamento da licitude ou ilicitude da conduta, o questionamento do bom ou mau funcionamento da Administração. Demonstrado o nexo de causalidade, o Estado deve ressarcir (MEDAUAR, 2005).

Dessa forma, é certo que a responsabilidade civil objetiva não se reveste de caráter absoluto, pois admite abrandamento e até mesmo a exclusão da responsabilidade estatal em algumas hipóteses excepcionais, como no caso fortuito, força maior e a culpa atribuível à própria vítima. Cabe destacar, neste ponto, o entendimento do ministro Celso de Mello do Supremo Tribunal Federal é de que:

> os elementos que compõem a estrutura e delineiam o perfil da responsabilidade civil objetiva do Poder Público compreendem (a) a alteridade do dano, (b) a causalidade material entre o “eventus damni” e o comportamento positivo (ação) ou negativo (omissão) do agente público, (c) a oficialidade da atividade causal e lesiva imputável a agente do Poder Público, que, nessa condição funcional, tenha incidido

> em conduta comissiva ou omissiva , independentemente da licitude, ou não, do seu comportamento funcional (RTJ 140/636) e (d) a ausência de causa excludente da responsabilidade estatal (RTJ 55/503 – RTJ 71/99 – RTJ 91/377 – RTJ 99/1155 – RTJ 131/417) (STF, 2018).

Portanto, a responsabilidade estatal no âmbito do tratamento de dados pessoais é analisada seguindo os critérios da responsabilidade objetiva para atos comissivos, como o tratamento e compartilhamento irregular de dados e, por outro lado, seguindo uma ótica subjetiva em se tratando de atos omissivos, como, por exemplo, a não observância das normas de prevenção e de segurança da informação.

4.2 Controlador sendo pessoa natural ou pessoa jurídica de direito privado

Quando o controlador for pessoa física ou pessoa jurídica de direito privado, o sistema de configuração da responsabilidade civil observa, não somente o critério pessoal, mas também a relação jurídica subjacente. Nesse sentido, é pertinente analisar os dispositivos que aludem à responsabilidade civil dos agentes de tratamento de dados na LGPD conforme dois critérios hermenêuticos.

4.2.1 Interpretação sistemática

Quando o legislador excepcionou a regra da responsabilidade civil subjetiva no direito privado, o fez de maneira expressa e inequívoca, a exemplo do emprego da expressão “independentemente de culpa”, como cláusula geral no artigo 927, parágrafo único do Código Civil. Na Lei Geral de Proteção de Dados não há qualquer artigo que se valha dessa expressão, assim não há indicação que o regime jurídico adotado seja o da responsabilidade objetiva.

Outro argumento é de que a lei 13.709/2018 (LGPD) foi bastante detalhista na imposição de uma série de deveres de ação e abstenção aos agentes de tratamento, como a observância cumulativa e intencional de todos os princípios de proteção de dados (art. 6º), abstenção de coleta de dados desnecessários (art. 14, §4º), a divulgação ostensiva da identidade e das informações de contato do encarregado (art. 41, §1º), entre outros.

É evidente que tais regras não são meras recomendações, mas sim um padrão de conduta que o legislador cobra o cumprimento. Assim, caso o sistema de responsabilidade civil fosse objetiva, elencar de maneira exaustiva e detalhada esses deveres teria sido algo absolutamente inócuo, pois de nada adiantaria o cumprimento dos deveres se, qualquer que fosse o incidente, a responsabilidade independeria de culpa. Em reforço a essa concepção o artigo 43 da lei prevê hipóteses excludentes de responsabilidade:

> **Art. 43.** Os agentes de tratamento **só não serão responsabilizados quando provarem**:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (BRASIL, 2018).

De forma contrária, não pode ser tido como irregular o tratamento que observou a lei e que, simultaneamente, proveja a segurança que dele se espera. Dessa forma, a reparação pelos danos advindos de atos ilícitos somente se dá por expressa disposição legal, nesse caso seria equivocado adotar a responsabilidade objetiva, cuja caracterização independe de negligência, imprudência, imperícia ou da violação de qualquer dever jurídico por parte do agente.

4.2.2 Interpretação teleológica

Teleológica é a interpretação que visa compreender a lei de acordo com o objetivo para o qual foi criada. Com a finalidade de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural como a Lei Geral de Proteção de Dados enunciou em seu artigo 1º.

A adoção, como regra, do sistema da responsabilidade civil objetiva resultaria num desincentivo à observância dos deveres específicos de proteção, prevenção e segurança impostos aos agentes de tratamento, desprestigiando a ideia de um adequado fluxo informacional como solução para um desenvolvimento econômico e tecnológico baseado em dados.

4.3 Regulamentação da responsabilidade civil dos agentes de tratamento de dados na LGPD

O artigo 42 da LGPD estabelece a responsabilidade dos agentes de tratamento de dados pessoais, destacando que tanto o controlador quanto o operador podem ser responsabilizados por danos causados a terceiros em decorrência do tratamento de dados pessoais, especialmente em caso de violação das normas da LGPD. Essa responsabilidade abrange danos de natureza moral, patrimonial, individual ou coletiva.

O inciso I do §1º do artigo 42 da LGPD equipara a o operador ao controlador de dados pessoais para fins de responsabilização nas hipóteses de descumprimento à legislação de proteção de dados ou a inobservância das instruções do controlador para a operação de tratamento de dados. Nas hipóteses de equiparação o operador responderá solidariamente com este pelos danos causados.

O inciso II do §1º do artigo 42, por sua vez, estabelece a responsabilidade solidária entre controladores envolvidos no tratamento de dados, ponto favorável ao titular de dados pessoais, pois é demasiadamente custoso imputar ao titular de dados o ônus de identificar o agente fomentador do dano causado em si em razão de descumprimentos legais.

Os parágrafos conseguintes do artigo 42 não abordam diretamente pressupostos para responsabilização civil dos agentes de tratamento de dados pessoais. O §2º trata do direito de regresso contra os corresponsáveis do reparador do dano ao titular, enquanto o §3º trata da tutela coletiva de direitos e o §4º dispõe sobre distribuição ao encargo probatório.

Magro e Andrade (2024) reputam que o obstáculo ensejador das discordâncias acerca do regime de responsabilidade civil na LGPD advém da insuficiência redacional do art. 42 da norma de proteção de dados, considerado elementar à sistemática de responsabilidade e ressarcimento de danos na LGPD. Para os autores, a interpretação gramatical do dispositivo é inserível ao assentamento de um regime de responsabilidade civil dos agentes de tratamento.

Para Fernando Antônio Tasso, a LGPD não ignorou a coerência interna com o sistema de responsabilidade civil do Código Civil e do Código de Defesa do Consumidor, mesmo que objetiva, de regular as relações jurídicas de direito privado baseadas no tratamento de dados pessoais:

> A despeito dos embates doutrinários, verifica-se que a Lei Geral de Proteção de Dados elegeu o sistema de responsabilidade civil subjetiva em perfeito alinhamento com o Código Civil, inserindo-se de forma harmoniosa no mosaico legislativo, o mesmo ocorrendo em relação ao Código de Defesa do Consumidor que, dado o tratamento Constitucional da defesa do consumidor, atrai para seu sistema de responsabilidade objetiva os fatos jurídicos dessa natureza (TASSO, 2020, p. 113).

O artigo 45 da LGPD, positiva os microssistemas de proteção de dados e de defesa do consumidor no que tange à responsabilidade civil na hipótese em que a violação dos direitos do titular de dados pessoais opera-se em relações de consumo. Nessa hipótese, na circunstância de que o titular de dados também é consumidor, nos termos da legislação respectiva, subsiste a viabilidade de invocar o sistema de responsabilidade prevista no Código de Proteção e Defesa do Consumidor, a qual é a responsabilidade objetiva.

5. ENTENDIMENTO DOUTRINÁRIO SOBRE O REGIME DE RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

No âmbito doutrinário, considerando-se a atualidade e pertinência do tema, o entendimento acerca do regime de responsabilidade dos agentes de tratamento de dados pessoais foi dividido em três linhas de pensamento: (I) responsabilidade objetiva; (II) responsabilidade subjetiva e (III) um sistema *sui generes*, nominado responsabilidade proativa.

5.1 Responsabilidade Objetiva

A corrente doutrinária que defende adoção do sistema de responsabilidade objetiva tem como fundamento a teoria do risco, com o intento de aplacar efetivamente o risco de vazamento de dados pessoais, o legislador objetivou restringir ao máximo as hipóteses nas quais o tratamento é juridicamente protegido.

Andrade e Magro (2022) fazem menção ao estudo elaborado por Danilo Doneda e Laura Mendes e, 2018, considerado percursor da concepção de que o risco é o parâmetro prevalecente para imputação do dever de indenizar no âmbito da proteção de dados, o que conduz, portanto, à responsabilização objetiva dos agentes de tratamento de dados.

A avaliação acerca da responsabilidade civil demanda análise sistemática da LGPD, não se cingindo à seção concernente a esse assunto. Dessa forma, a estruturação da LGPD indica que, em regra, o tratamento de dados condiciona-se à observância das bases legais elencadas no artigo 7º, de que a coleta e processamento de dados devem atender à consecução de sua finalidade (princípios da necessidade e finalidade), além da adoção de uma conduta de eliminação de dados quando encerrado o tratamento, devendo o agente considerar o risco presente no tratamento de dados.

O cerne desta corrente reside na convicção de que a atividade de tratamento de dados pessoais apresenta riscos imanentes aos respectivos titulares de dados, conclusão amparada na interpretação sistemática da LGPD, com o intento de "minimizar as hipóteses de tratamento àqueles que sejam, em um sentido geral, úteis e necessárias" (ANDRADE, MAGRO, 2022, p. 216).

Para Mulholland (2020) dados pessoais:

> Tais danos se caracterizam por serem quantitativamente elevados e qualitativamente graves, ao atingirem direitos difusos, o que, por si só, já justificaria a adoção da responsabilidade civil objetiva, tal como nos casos de danos ambientais e dos danos causados por acidentes de consumo (MULHOLLAND, 2020).

Não obstante, a omissão legislativa que resultou na ausência de critérios preestabelecidos para definição da modalidade de responsabilidade civil dos agentes de tratamento de dados resulta, a priori, na integração desta à regra estabelecida no *caput* do artigo 927 do Código Civil, a qual é a de responsabilidade subjetiva, dado que para incidência da cláusula geral de responsabilidade objetiva, prevista no parágrafo único do artigo 927, a conduta antijurídica ensejadora de reparação, independentemente de culpa, deve ter expressa previsão legal ou resultar de atividade cujo risco é inerente à atividade por sua própria natureza.

Para Gondim (2021) o exercício da atividade de tratamento de dados é de risco, seja em dados pessoais gerais, seja em dados pessoais sensíveis, o que amolda o regime de responsabilidade objetiva, prescindido da culpa, devido à cláusula geral de responsabilidade objetiva prevista no *caput* do art. 927 do Código Civil.

Há quem entenda que a estrutura de excludentes de responsabilidade elencadas no artigo 43 da LGPD revela a problemática originada na ausência de estabelecimento concreto do regime de responsabilidade civil objetivo ou subjetivo na norma de proteção de dados, imputando aos agentes de tratamento responsabilidade objetiva, a qual será afastada somente quando provarem:

> I- que não realizaram o tratamento de dados que lhes é atribuído
> II- que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III- que o dano é decorrente de culpa exclusiva do titular de dados ou de terceiro (BRASIL, 2018).

Andrade e Magro (2022) consideram, ainda, ao exporem as distintas correntes de pensamento, que se faz possível a imputação de regime de responsabilidade objetiva ao

operador e ao controlador em face da convergência entre a LGPD e o CDC (Código de Defesa do Consumidor) devido à proximidade redacional e sistemática constatada entre as normas.

A adoção do modelo objetivo é medida facilitadora do exercício dos direitos inerentes ao titular de dados pessoais no curso de ação judicial com a finalidade de reparar danos por si suportados devido à irregularidade no tratamento de seus dados, uma vez que é flagrante a dificuldade de demonstração do dano na tutela do direito à proteção de dados, reconhecendo-se, neste aspecto, sua hipossuficiência em face do agente de tratamento de dados pessoais.

5.2 Responsabilidade Subjetiva

O entendimento de que o regime de responsabilidade civil adotado na LGPD foi subjetivo resulta de três fundamentos intrínsecos à própria estruturação da referida norma. O primeiro alude ao histórico de tramitação legislativa que culminou a LGPD. O segundo aos padrões de conduta a serem seguidos pelos agentes de tratamento de dados. O terceiro refere-se à excludente de responsabilidade preconizada no inciso II do artigo 43 da Lei Geral de Proteção de Dados.

Andrade e Magro (2022) discorrem, sobre o primeiro fundamento, que:

> Ao longo do processo de maturação dos projetos que originaram a LGPD, notadamente o PL nº5.276, foi-se retirada a única disposição acerca de responsabilidade objetiva em capítulo atinente à transferência internacional de dados (MAGRO, ANDRADE, 2022, p.222).

Nas versões subsequentes do projeto de lei até a versão sancionada na LGPD, não subsistiu menção no sentido de adoção, como regra geral, de regime objetivo de responsabilidade civil pelos danos causados por agentes no exercício do tratamento de dados, de forma que a referência à responsabilidade civil foi completamente suprimida do texto legal, o que permite concluir que o legislador, a despeito da omissão legislativa, optou pelo regime subjetivo, assim defendem Gisela Guedes e Rose Meireles.

Bioni e Dias (2020, p. 04), destacam que os quase dez anos de debates que conduziram a atual redação do diploma normativo de proteção de dados “deixaram pistas hermenêuticas valiosas e possibilidades analíticas a partir dos trabalhos preparatórios da lei”.

O segundo fundamento se firma na positivação do capítulo VII da LGPD destinado à Segurança e Boas Práticas. Segundo Guedes e Meireles (2019) a lei trouxe uma

série de padrões de conduta a serem compulsoriamente seguidos pelo operador e pelo controlador, notando-se a atenção conferida pelo legislador à conduta de agentes de tratamento, inclusive ao cumprimento de procedimentos, políticas internas, padrões técnicos e outros mecanismos a serem supervisionados.

Destaca-se ainda, que o artigo 6º, inciso X, da LGPD positiva os princípios da responsabilização e da prestação de contas, pelos quais é imprescindível a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive, da eficácia dessas medidas" (BRASIL, 2018).

Nessa perspectiva, as autoras afirmam que não há coerência em impor aos agentes o dever de adotar tais condutas, se, em havendo incidente que ocasione danos ao titular de dados, será responsabilizado independentemente de ter cumprido, na íntegra, os deveres de segurança preconizados na legislação, sendo a modalidade subjetiva apropriada à responsabilização dos agentes de tratamento.

Guedes e Meireles (2019, p.123) ao procederem também à interpretação sistêmica da norma de proteção de dados, fundamentam seu posicionamento na noção hodierna de "culpa normativa [...] a partir da ideia de desvio de conduta, que leva em conta apenas o comportamento exigível diante das especiais circunstâncias do caso concreto" (GUEDES, MEIRELES, 2019).

O terceiro fundamento presente na LGPD que indica a adoção da responsabilidade subjetiva está na excludente de responsabilidade prevista no inciso II do artigo 43 da norma de proteção de dados, pelo qual os agentes serão isentos de responsabilidade quando, embora tenham realizado o tratamento de dados pessoais que lhes foi atribuído, não houve violação à LGPD. Dessa forma, em contraposição aos incisos I e III, que preceituam a exclusão da responsabilidade com fundamento no rompimento do nexo de causalidade, o inciso II remete à culpa como fundamento para constatar a responsabilidade do agente e a subsequente indenização pelo dano.

Assim, ainda que manifesto o nexo de causalidade entre a conduta do agente e o dano alegado pelo titular, não haverá responsabilização quando o operador ou controlador de dados se escusar do ônus de provar o efetivo cumprimento dos deveres preceituados na LGPD ao demonstrar que tomou as medidas de segurança recomendadas, hipótese em que o agente demonstrará que a ocorrência do dano não se deu por inobservância de deveres em alguma conduta sua.

Guedes, Telepedino e Terra (2022, p. 293), por fim, no que concerne às similitudes entre o CDC e a LGPD, que podem ser usadas para justificar a adoção do regime de responsabilização objetiva dos agentes, asseveram que, enquanto no CDC há expressa indicação, em menos dois artigos (artigos 12 e 14), se valendo da expressão "independentemente de culpa", que deixa evidenciada a opção do legislador pela responsabilidade objetiva. Inexiste na LGPD previsão análoga.

Em conclusão, o inciso II do artigo 43, o capítulo VII e o artigo 6º, X, todos da LGPD, bem como o histórico do trâmite legislativo da norma, refletem que a modalidade de responsabilidade a ser seguida é a subjetiva, pois encontra-se intrinsecamente relacionada ao elemento "culpa", motivação pela qual, segundo os autores citados ao longo deste subcapítulo, o reconhecimento do regime da responsabilidade civil subjetiva aos agentes de tratamento de dados.

5.3 Responsabilidade Proativa

Além das correntes de responsabilidade objetiva e subjetiva, há também quem defenda que, com a vigência da LGPD, instituiu-se um regime diferenciado de responsabilidade civil, aplicável exclusivamente aos agentes de tratamento de dados pessoais, fundamentado no dever de segurança trazido no artigo 44 da LGPD, o qual assemelha-se à noção consumerista de defeito no produto ou serviço, bem como no dever de prestação de contas trazido, também como um princípio, no artigo 6º, X da LGPD.

Moraes e Queiroz (2019, p. 125/126) defendem que a LGPD inaugurou um sistema especial de responsabilidade civil denominado "proativo", que se caracteriza pela reunião dos conceitos de responsabilidade e prestação de contas. Os autores sustentam que considerando a prevenção de danos como valor máximo a ser alcançado, os agentes de tratamento não devem apenas se preocupar em cumprir a lei, mas também prevenir a ocorrência de danos aos titulares, adotando medidas eficazes e demonstrando sua segurança, devendo provar:

> I- que avaliou e, se necessário, redesenhou adequadamente o processamento de dados pessoais; II- que as medidas de segurança implementadas são adequadas e eficazes; III- que se aplica uma política de privacidade interna com obrigações claras, ações concretas vinculadas a cada uma e que foram designados os responsáveis pelo cumprimento; IV- que nomeou um encarregado e que exige esse mesmo cumprimento responsável de seus funcionários e na sua cadeia de terceirização (MORAES; QUEIROZ, p. 129).

A responsabilidade civil na Lei Geral de Proteção de Dados, tal qual no modelo europeu, articula-se em torno de três requisitos cumulativos, sendo a existência de dano, a violação da legislação de proteção de dados por parte do operador ou do controlador e, por fim, a reparação do dano.

O regime Proativo depreende que o dano seja ocasionado pelo tratamento irregular de dados pessoais por parte dos agentes de tratamento, seja por violação direta a LGPD ou algum dever legal de segurança dele esperado, comprovados esses dois requisitos advém a obrigação de ressarcir o dano à parte lesada. Dresch (2020) leciona que o "enunciado normativo chave" para fundamentar essa corrente é o artigo 44 da LGPD, que preceitua um dever geral de segurança, cuja violação ensejará a responsabilização civil.

Na LGPD o ilícito geral trata-se da inobservância do dever de segurança, o que ocorre com o tratamento irregular de dados pessoais, assim o dever geral de segurança e o tratamento irregular são os parâmetros que esteiam a responsabilidade civil dos agentes de tratamento de dados, devendo ser feita análise minuciosa dos padrões de conduta para se avaliar se o tratamento forneceu ou não a segurança esperada.

Dessa forma, o fundamento da responsabilidade civil na LGPD ocorre pela violação à lei, não estando centrada na culpa, o que afasta a incidência de responsabilidade subjetiva, de igual modo não se centra no risco, afastando a responsabilidade civil objetiva, de forma que se pode estabelecer um regime de responsabilidade *sui generes*. Ressalta-se que nas hipóteses em que a violação à legislação ocorre em relação de consumo, subsiste a incidência do CDC.

Assim, a noção de responsabilidade proativa indica que além de cumprir os imperativos legais da LGPD, os agentes de tratamento devem demonstrar o cumprimento, mapeando todas as atividades que envolvem dados pessoais, bem como seus riscos e as medidas de segurança adotadas para evitar danos, demonstrar também a capacitação dos operadores e controladores de dados, para que estes aprendam as formas adequadas de proteção de dados.

6. ESTUDO DE CASOS

Tendo em vista a contextualização realizada acerca do assunto objeto desta monografia, será feita uma colocação em análise de alguns casos que levaram para as pautas do Judiciário a discussão em relação à responsabilidade civil no âmbito da Lei Geral de Proteção de Dados.

6.1 Caso Cyrela

O primeiro caso emblemático envolvendo a Lei Geral de Proteção de Dados envolveu a sentença proferida em processo que condenou a construtora Cyrela a pagar indenização por danos morais ao consumidor Fabrício Vilela Coelho, vítima de suposto vazamento indevido de dados pessoais. A decisão proferida pela juíza da 13ª Vara Cível de São Paulo determinou que a empresa pagasse uma indenização de R$10.000,00 (dez mil reais) à Fabrício pelo compartilhamento de seus dados sem prévia autorização.

Em novembro de 2018, o requerente comprou um apartamento da construtora e pouco tempo depois passou a receber ligações indesejadas de instituições financeiras e empresas de decoração oferecendo serviços associados à aquisição do imóvel. Conforme entendimento da magistrada, a conduta da Cyrela infringiu normas da LGPD, bem como direitos previstos no CDC e na Constituição Federal.

> Isto posto, a **responsabilidade da ré é objetiva** (arts. 14, caput, CDC e 45, LGPD). Inexiste suporte para a exclusão de responsabilidade (art. 14, §3º, I a III, CDC), de sorte que caracterizado o ato ilícito relativo à violação de direitos de personalidade do autor, especialmente por permitir e tolerar 9conduta omissiva) ou mesmo promover (conduta comissiva) o acesso indevido a dados pessoais do requerente por terceiros (BRASIL, 2020).

Até então, o caso servia de parâmetro a ser levado em consideração, mas em agosto de 2021 a sentença foi reformada e Cyrela inocentada, sob o argumento de que não houve provas suficientes que comprovassem que o compartilhamento de dados do autor foi feiro pela construtora e especialmente porque à época da compra do imóvel a LGPD ainda não estava em vigor.

Além de apontar a insuficiência de provas, a nova decisão que inocentou Cyrela também classificou o encaminhamento de mensagens genéricas via e-mail ou WhatsApp como mero aborrecimento, insuscetível de dano moral.

Em entrevista à CNN Business, o escritório Vilela Coelho, responsável pela acusação, afirmou que pretendia recorrer da decisão, “como o consumidor vai provar que foi Cyrela? Só se tiver acesso à base de dados dela ou se ela confessar”, disse o advogado Mario Filipe Santos (2021). De acordo com este critério, quando a alegação do consumidor tem aparência de verdadeira, cabe ao juiz inverter o ônus da prova e exigir que a empresa

demonstrasse não ser responsável pelo que o consumidor alega. Para Bruno Bioni e Daniel Dias (2020):

> [...] caso a alegação da vítima seja verossímil, ou haja hipossuficiência para produção de provas, ou a produção seja excessivamente onerosa, o juiz poderá inverter o ônus da prova em relação a esses três últimos elementos. Como resultado, a vítima não precisará propor nenhum elemento de responsabilidade, ficando a cargo dos agentes de tratamento o ônus de provar sua não ocorrência (BIONI; DIAS, 2020).

O caso Cyrela, em que pese ter sido o primeiro e ainda de ter acontecido em um momento de transição para a Lei Geral de Proteção de Dados, não pode servir como parâmetro para reclamações de outros consumidores no futuro, pois a jurisprudência sobre LGPD ainda está em formação, com a lei de proteção de dados em plena vigência, o consumidor tende a ganhar de maneira mais automática proteções que, no julgamento desta lide, pesaram em favor de Cyrela.

6.2 Caso Eletropaulo

Ao apreciar o agravo em recurso especial (AResp) 2130619/SP, com julgamento em 07/09/2023 (sete de março de dois mil e vinte e três), e como relator o ministro Francisco Falcão, decidiu a segunda turma do Superior Tribunal de Justiça que o dano moral no caso de danos morais não é presumido.

Trata-se, na origem, de ação de indenização proposta por Maria Edite de Souza em face da concessionária de energia elétrica Eletropaulo pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiro, de seus dados pessoais, tendo a vítima recebido inúmeras mensagens e ligações indevidas de terceiros. Foram vazadas informações como nome, CPF, RG, números de telefone, e-mail, endereço residencial e data de nascimento.

A sentença de primeiro grau julgou improcedentes os pedidos do autor, tendo a Corte Estadual (Tribunal de Justiça de São Paulo), reformulado a decisão para condenar a concessionária ao pagamento da indenização com fundamento em vazamento de dados de pessoa idosa.

A empresa ré interpôs recurso especial, no qual aduziu a negativa aos artigos 42, 43, II e III, 46 e 48 da LGPD, em razão da comprovada postura da empresa quanto à

segurança reservada aos dados sob sua responsabilidade, sendo o vazamento causado por terceiro alheio à relação entre as partes, o que justificaria uma excludente de responsabilidade.

No voto do relator Ministro Francisco Falcão, no que concerne a alegação de ofensa aos artigos supramencionados da LGPD, vinculados à tese de culpa exclusiva de terceiro, verificou-se que o Tribunal *a quo*, em nenhum momento abordou as questões referidas nos dispositivos legais, mesmo após a oposição de embargos de instrumento, incidindo, na hipótese, a súmula 211 do STJ, que inadmite recurso especial em relação à questão que, em embargos de declaração, não foi apreciada pelo tribunal *a quo. In casu*, não se falou em prequestionamento ficto (art.1.025/CPC), pois caberia à parte arguir tais questões explicitamente, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração.

Em relação a alegada ofensa ao artigo 5º, II, da LGPD, entendeu o julgador que o dispositivo dispõe de forma taxativa quais dados são considerados dados pessoais sensíveis, e que dados de natureza comum, mas não íntimos, passíveis apenas de identificação da pessoa natural, não podem ser classificados como sensíveis, que embora tenha ocorrido o vazamento, não restou comprovada qualquer lesão aos direitos da personalidade do autor que justificasse a condenação da ré ao pagamento de indenização por danos morais.

A ementa do agravo em recurso especial aborda que:

> PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDAD. NECESSIDADE DE COMPROVAÇÃO DO DANO. [...] 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 de dados comprove eventual dano decorrente da exposição dessas informações (STJ, 2023).

Ao final, no inteiro teor, a menção é de que o caso se trata de mero inconveniente desacompanhado de comprovação do dano, portanto incabível de indenização por danos morais presumidos. A presente decisão denota um posicionamento contrário ao defendido por doutrinadores, como a professora Caitlin Mulholland, que leciona ser o rol do artigo 5º, II, da LGPD exemplificativo, pois outros dados além dos trazidos no artigo merecem a qualificação como dados sensíveis, a exemplo dados de geolocalização.

A natureza dos dados não deveria ser critério para reconhecer se há um dano moral (presumido ou não) em situação de vazamento de dados, pois a LGPD tem entre seus fundamentos a privacidade, intimidade e autodeterminação informativa, princípios que

permeiam todas as categorias de dados, sensíveis ou não. Quando se trata de dano, a LGPD não diferencia situações envolvendo dados comuns e dados sensíveis, sendo a natureza do dado um elemento a ser analisado, e não requisito para cabimento de ação.

Em recente estudo feito por Daniel Solove (2023), professor na George Washington University Law School, ele critica leis de proteção de dados que estabelecem dois níveis de proteção, um para dados comuns e outro para dados sensíveis. Classificar a sensibilidade de uma informação depende do contexto em que o titular de dados está inserido, para vítimas de perseguição, por exemplo, o endereço onde residem pode ser considerada uma informação sensível.

Portanto, a individualização é necessária não apenas para assegurar as particularidades de cada caso, mas também para que se possa arbitrar uma indenização compatível com a dimensão do dano moral configurado.

6.3 Caso SERASA

O caso em tela trata-se de ação de obrigação de fazer c/c indenização por danos morais ajuizada por Aira Alves Pereira Tavares Freitas, a requerente em sua inicial alega a comercialização de dados pela instituição SERASA EXPERIAN S/A sem prévio consentimento da consumidora. Diante disso, Aira requereu que o réu se abstivesse de divulgar, permitir o acesso, gratuito ou pago, bem como compartilhar informações a respeito da renda mensal, endereço e telefones pessoais, com consequente indenização em valor não inferior a R$11.000,00 (onze mil reais) pelos danos morais.

Em primeiro grau, a sentença julgou improcedentes os pedidos formulados na inicial, no Tribunal Estadual de São Paulo foi negado provimento à apelação interposta por Aira por entenderem que os dados da recorrente disponibilizados pela recorrida não se tratavam de dados sensíveis, fundamentando que a LGPD admite o tratamento de dados pessoais para proteção de crédito independente de prévio consentimento do titular (art. 7º, X, da Lei nº 13.709/18) e que a súmula 550/STJ dispõe ser desnecessário o consentimento do consumidor quando à utilização de escore de crédito.

Em recurso especial interposto ao STJ, Aira alega violação dos artigos s. 43, §§1º e 2º do CDC; 7º, I e X, 8º e 9º da LGPD; 3º, §§ 1º e 3º, I, 4º e 5º, VII, da Lei 12.414/2011; e 5º, X, da CRFB/1988, fundamentando que o consentimento e comunicação dos titulares é dever e não mero ato de liberalidade e que a disponibilização de dados pessoais

em bancos de dados de fácil acesso a terceiros enseja indenização por danos morais, pelo sentimento de insegurança experimentado pelo indivíduo.

O recurso especial, distribuído sob o nº 2115461, tendo como relatora a Ministra Nancy Andrighi teve início afastando a aplicação da súmula 550/STJ, pois o caso em comento diz respeito à comercialização de dados pessoais da consumidora e não à divulgação de análise de crédito feita a partir de referidos dados. Em segundo, foi dito que não se pode aplicar de forma genérica que o gestor de banco de dados pode disponibilizar, sem consentimento prévio do titular, dados pessoais dos cadastrados, pois existe um tratamento diferenciado para cada situação, a depender da atividade do gestor e dos dados em si.

No exame do mérito recursal destacaram-se algumas teses e fundamentos, dentre eles:

> 48. Em síntese, embora o gestor de banco de dados para proteção do crédito possa realizar o tratamento de dados pessoais e abrir cadastro sem prévio consentimento do cadastrado, a Lei nº 12.414/2011 **(I)** restringe o compartilhamento das informações cadastrais a outros bancos de dados – que são geridos por pessoas devidamente autorizadas pelo BACEN; e **(II)** em relação aos consulentes, apenas autoriza a disponibilização **(a)** da pontuação de crédito; e **(b)** do histórico de crédito, desde que autorizado previamente pelo cadastrado, em observância ao modelo de autorização do Decreto nº 9.936/2019. 49. Desse modo, se um terceiro consulente tem interesse em obter as informações cadastrais do cadastrado, ainda que sejam dados pessoais não sensíveis, deve ele obter o prévio e expresso consentimento do titular, com base na autonomia da vontade, pois não há autorização legal para que o gestor de banco de dados disponibilize tais dados (STJ, 2024).

À despeito da comunicação quanto à abertura do cadastro em banco de dados e sobre os agentes de tratamento de dados o entendimento foi que:

> 67. Em síntese, embora não seja exigido o consentimento prévio para a abertura do cadastro pelo gestor de banco de dados, é necessária a comunicação ao cadastrado, inclusive sobre os demais agentes de tratamento (terceiros que obtém acesso aos dados), destacando-se que o cadastrado pode exigir o cancelamento a qualquer momento, jamais podendo o gestor manter um cadastro contra a vontade expressa do cadastrado (STJ, 2024).

Com relação ao dano moral pela disponibilização indevida de dados a terceiros, de acordo com o artigo 16 da Lei nº 12.414/2011 o banco de dados, a fonte e o consulente são responsáveis objetiva e solidariamente pelos danos morais que causarem ao cadastrado, nos termos do CDC. De igual forma foi mencionada a responsabilidade e ressarcimento de danos previstos no artigo 42 da LGPD, Andrighi:

> 73. Nesse sentido, como já reconhecido por esta Turma, disponibilização indevida (em ofensa aos limites legais) de dados pessoais pelos bancos de dados para terceiros caracteriza dano moral presumido *(in re ipsa*) (REsp 1.758.799/MG, Terceira Turma, DJe 19/11/2019) (STJ, 2024).

O entendimento da relatora foi que a sensação de insegurança não pode ser considerada como mero dissabor, assim, a inobservância dos deveres associados ao tratamento dos dados do consumidor – que deve ser informado – faz nascer para este a pretensão de indenização pelos danos causados. Assim, o gestor de banco de dados que disponibiliza para terceiros consulentes o acesso aos dados do cadastrado que somente poderiam ser compartilhados entre bancos de dados deve responder pelos danos morais causados ao cadastrado, que decorrem, sobretudo, da sensação de insegurança gerada pela disponibilização indevida dos seus dados.

Por fim, o dispositivo do acórdão conheceu o recurso especial e deu-lhe parcial provimento, condenando a ré a se abster de disponibilizar dados da autora (informações cadastrais e de adimplemento), sem sua prévia autorização, para terceiros consulentes e a pagar o valor de R$11.000,00 a título de indenização por danos morais.

6.4 Caso Seguradora de Vida

O caso em tela envolve um segurado que contratou seguro de vida da empresa Prudential do Brasil Seguros de Vida S/A. Em outubro de 2020, o segurado recebeu um e-mail da seguradora informando sobre um incidente de *cibersegurança* em seu sistema de proposta para contratação de seguros de vida individuais, no qual foi identificado acesso não autorizado a parte dos dados das propostas, contendo informações como nome, CPF, endereço, dados sobre saúde, bens e beneficiários e até números de conta corrente e agência bancária.

Do acórdão que julgou a presente demanda pode se extrair fundamentos e assuntos abordados nesta pesquisa.

> APELAÇÃO – AÇÃO DE REPARAÇÃO DE DANOS E OBRIGAÇÃO DE FAZER – VAZAMENTO DE DADOS E INFORMAÇÕES PESSOAIS DO AUTOR – RESPONSABIILADE OBJETIVA DA RÉ SEGURADORA – CONSOANTE DIRETRIZES DA LEI GERAL DE PROTEÇÃO DE DADOS E CÓDIGO DE DEFESA DO CONSUMIDOR – DANO MORAL CONFIGURADO – VALOR MAJORADO. I- Falha na prestação de serviços executados pela seguradora ré que permitiu acesso a Dados pessoais do autor e terceiros. Responsabilidade objetiva. Dever de indenizar. [...] as informações vazadas dizem respeito, dentre outros, às informações de saúde, bens e beneficiários do autor, plenamente enquadráveis, portanto, dentro do conceito de dados sensíveis [...] III-

> Dano moral configurado de natureza *in re ipsa*, cuja existência se presume a partir do mero vazamento dos dados pessoais, sendo prescindível a existência de demonstração de que o episódio resultou algum tipo de efeito deletério para o autor. Indenização cujo valor majorado para R$15.000,00 (BRASIL, 2023).

O entendimento firmado foi de que a responsabilidade nesse caso é objetiva de acordo com a LGPD, além disso configura também responsabilidade por fato do serviço, sujeita ao regramento do artigo 14 do CDC. No Caso restou evidente que a seguradora violou os princípios da finalidade e transparência no tratamento de dados pessoais.

A decisão proferida foi de extrema importância para o posicionamento jurídico acerca da responsabilidade objetiva das empresas no que diz respeito à proteção de dados pessoais de seus consumidores.

7 CONCLUSÃO

A conclusão deste trabalho visa consolidar as principais considerações a respeito da responsabilidade civil no âmbito da Lei Geral de Proteção de Dados (LGPD). A análise demonstrou que a legislação brasileira, ao se inspirar no modelo europeu de proteção de dados, buscou equilibrar a proteção dos direitos fundamentais à privacidade, liberdade e ao desenvolvimento da personalidade com o tratamento de dados pessoais. Nesse contexto, a responsabilidade civil dos agentes de tratamento de dados assume papel central.

O entendimento predominante nos tribunais tem sido pela adoção da responsabilidade civil objetiva em muitos casos que envolvem o tratamento de dados pessoais. Esse tipo de responsabilidade se baseia na teoria do risco, ou seja, a simples atividade de tratamento de dados, por si só, envolve riscos aos titulares dos dados. Dessa forma, o agente de tratamento — seja ele controlador ou operador — tem o dever de garantir a segurança e o cumprimento das normas impostas pela LGPD, sendo responsabilizado mesmo sem a necessidade de comprovação de culpa.

O artigo 42 da LGPD reforça essa visão, determinando que tanto os controladores quanto os operadores podem ser responsabilizados pelos danos causados em decorrência do tratamento de dados pessoais, especialmente quando há violação das normas da legislação. Tal responsabilidade abrange tanto danos morais quanto materiais, sejam de natureza individual ou coletiva, refletindo a gravidade das possíveis infrações cometidas pelos agentes de tratamento.

A aplicação da responsabilidade objetiva é justificada pela dificuldade que os titulares de dados enfrentam em demonstrar a ocorrência de falhas no tratamento de seus dados. Essa vulnerabilidade, associada ao caráter muitas vezes difuso dos direitos envolvidos, reforça a necessidade de se aplicar um regime que prescinda da comprovação de culpa, facilitando, assim, o acesso à reparação dos danos sofridos. Ademais, o reconhecimento da hipossuficiência do titular de dados em face dos agentes de tratamento reforça a adoção desse modelo, conforme previsto pelo Código de Defesa do Consumidor (CDC), que também influencia o entendimento da LGPD.

Todavia, é preciso ponderar os riscos da adoção irrestrita da responsabilidade objetiva. Tal modelo, apesar de proteger o titular, pode provocar um efeito inverso, desestimulando a inovação, especialmente em pequenas e médias empresas, que podem não ter os recursos necessários para lidar com a rigidez de um sistema objetivo, mesmo adotando boas práticas e investindo em segurança da informação. A responsabilização automática pode gerar um cenário de insegurança jurídica e incentivar o ajuizamento de ações infundadas.

Contudo, ainda existem debates doutrinários sobre a aplicabilidade de um regime de responsabilidade subjetiva ou proativa em alguns casos, principalmente quando a violação dos deveres previstos na LGPD não for evidenciada. A divergência ocorre devido à ausência de uma previsão expressa sobre a modalidade de responsabilidade a ser aplicada. Apesar disso, o fato de o risco estar intrinsecamente ligado ao tratamento de dados e as recentes decisões jurisprudenciais que favorecem a aplicação da responsabilidade objetiva indicam que este tem sido o entendimento predominante nos tribunais.

Diante disso, este trabalho defende a adoção preferencial da responsabilidade subjetiva, com a exigência de comprovação de culpa, nos moldes tradicionais do Código Civil, ao menos como regra geral. A subjetivação da responsabilidade civil permite uma análise mais criteriosa das circunstâncias do caso concreto, ponderando se houve efetivamente falha no dever de cuidado, dolo ou negligência por parte dos agentes de tratamento.

Além disso, a responsabilidade subjetiva está mais alinhada ao princípio da proporcionalidade e ao próprio texto da LGPD, que admite hipóteses de exclusão de responsabilidade, permitindo ao agente demonstrar que adotou todas as medidas cabíveis para evitar o dano. Trata-se de uma abordagem que garante maior equilíbrio entre os interesses dos titulares e os direitos e deveres dos agentes econômicos, estimulando a conformidade e a maturidade institucional no tratamento de dados.

Em conclusão, embora a responsabilidade civil no contexto da proteção de dados deva assegurar a efetiva reparação dos danos e a prevenção de novas violações, ela também deve respeitar os limites da razoabilidade, da segurança jurídica e da boa-fé objetiva.

O fortalecimento da cultura de proteção de dados no Brasil passa não apenas pela rigidez normativa, mas também por uma aplicação sensata e ponderada das regras de responsabilidade, capaz de proteger direitos sem comprometer o desenvolvimento tecnológico e a liberdade econômica.

REFERÊNCIAS

AIME, Leonardo da Silva; OBREGÓN, Marcelo Fernando Quiroga. Inspiração internacional: influências da General Data Protection Regulation na Lei Geral de Proteção de Dados brasileira. **Derecho y Cambio Social**. n. 60, Peru, abr./jun. 2020.

ALVES, Paulo. Facebook e Cambridge Analytica: sete fatos que você precisa saber. **TechTudo**, 24 mar. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml . Acesso em: 9 maio 2024.

ANDRADE, Vitor Moraes de. **Cartilha de Proteção de Dados Pessoais**. 2022. Disponível em: https://abemd.org.br/LGPD/Cartilha.pdf. Acesso em 18 maio 2024.

ANDRADE, Landolfo; MAGRO, Américo Ribeiro. **Manual de Direito Digital**. 2. ed. rev., atual e ampl. Salvador: JusPodivm, 2022.

BIONI, Bruno Ricardo; RIELLI, Mariana Marques. A construção Multissetorial da LGPD: história e aprendizados. In: BIONI, Bruno; (Org.); LEITE, Jessica Silveira (Coord.) **Proteção de Dados**: **contexto, narrativas e elementos fundantes**. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BOFF, Salete Oro; FORTES, Vinícius Borges. Internet e proteção de dados pessoais: uma análise das normas jurídicas brasileiras a partir das repercussões do caso NSA vs. Edward Snowden. **Qualis B1**. v. 11, n. 1, p. 340-370. Rio Grande do Sul, 2016.

BRANDEIS, Louis; WARREN, Samuel. The right to privacy. **Harvard Law Review**. v. 4, n. 5, p. 193-220. dez. 1890.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

BRASIL. Superior Tribunal da Justiça. **Súmula 385, STJ**. Da anotação irregular em cadastro de proteção ao crédito, não cabe indenização por dano moral, quando preexistente legítima inscrição, ressalvado o direito ao cancelamento. Diário de Justiça Eletrônico, 8 jun. de 2009. Disponível em

BRASIL, Superior Tribunal de Justiça. **Agravo em recurso especial nº 2.130.619/SP**. Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravada: maria Edite de Souza. Relator: Ministro Francisco Falcão, 07 mar. 2023.

BRASIL, **Supremo Tribunal Federal**, (2. Turma). *Ag. Reg. No Recurso Extraordinário com agravo 1.116.698.* Relator Min. Celso de Mello, 04/06/2018. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=747648001. Acesso em 15 setembro 2024.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a banco de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 09 maio 2024.

BRASIL. Tribunal de Justiça do Estado de São Paulo. Procedimento Comum Cível 1080233-94.2019.8.26.0100; relator(a): tonia Yuka Korok; foro Central Cível – 13ª Vara Cível; Data do Julgamento: 29/09/2020; Data de Registro: 30/09/2020.

CAHALI, Youssef Said. **Responsabilidade Civil do Estado**. 3ª ed. São Paulo: Revista dos Tribunais, 2007. P. 221.

CAVALCANTE, Pedro Peres. **Privacidade e proteção de dados pessoais:** uma análise comparativa dos quadros regulatórios brasileiro e europeu. Trabalho de Conclusão de Curso (Graduação em Direito). 62f. Universidade Federal de Pernambuco. Recife, 2018

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. (coords.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais.** 1. ed. Rio de Janeiro: Forense, 2021. p. 3-20. ISBN 978-85-309-9151-7.

ENTENDA o caso de Edward Snowden, que revelou espionagem dos EUA. **PortalG1**. 02 jul. 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 08 maio 2024

LÔBO, Paulo. **Direito Civil: parte geral**. 6. ed. São Paulo: Saraiva, 2017.

LUCIO, Amanda. **No Brasil, 80mil pessoas já foram vítimas de golpes online em 2023**. 27 out. 2023. E-Commerce Brasil. Disponível em: https://www.ecommercebrasil.com.br/noticias/no-brasil-80-mil-pessoas-ja-foram-vitimas-de-golpes-online-em-2023. Acesso em 28 maio 2024.

MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. Estudos preliminares sobre os princípios aplicados ao tratamento de dados pessoais na lei 13.709/2018 – LGPD, Anais. **Encontro Nacional de Ensino, Pesquisa e Extensão**.2603-2613. Presidente Prudente, out. 2020

MALDONADO, V. N.; BLUM, R. O. **LGPD:** Lei Geral de Proteção de Dados comentada. 1. ed. São Paulo: Revista dos Tribunais, 2019.

MARTÍ, Silas. Entenda o escândalo do uso de dados do Facebook. **Folha de S. Paulo.** 22 mar. 2018. Disponível em: https://www1.folha.uol.com.br/mercado/2018/03/entenda-o-escandalo-do-uso-de-dados-do-facebook.shtml. Acesso em: 08 maio 2024.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. Proteção de dados pessoais e democracia: *fake news*, manipulação do eleitor e o caso da Cambridge Analytica, **Revista Eletrônica Direito e Sociedade**. v. 7, n. 3, p. 135-148. Canoas, 2019.

MEDAUAR, Odete. **Direito Administrativo Moderno**, p. 430, item n. 17.3, 9ª ed., 2005, RT. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/despacho247855/false. Acesso em 15 setembro 2024

MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor**. **Linhas gerais de um novo direito fundamenta**l. São Paulo: Editora Saraiva, 2014.

MENDES, L.S.; FONSECA; G.C.S. da. **Proteção de Dados Para Além do Consentimento: Tendências de Materialização**. Tratado de proteção de dados pessoais. São Paulo: Gen-Forense, 2020.

MJSP multa Facebook em R$ 6,6 milhões. **Ministério da Justiça e Segurança Pública**. 30 dez. 2019. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-multa-facebook-em-r-6-6-milhoes. Acesso em: 09 maio 2024.

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?** Migalhas. [S.I.], 30 jun. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidadecivil/329909/algpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-dedadospessoais-culpa-ou-risco Acesso em: 10 out. 2024

PECSEN, Thaisy. Leva**ntamento mostra que número de vazamentos de dados em 2021 deve superar 2020, aponta PSafe**. PSAFE, 13 jul. 2021. Disponível em:

https://www.psafe.com/blog/levantamento-mostra-que-numero-de-vazamentos-de-dados-em-2021-deve-superar-2020-aponta-psafe/. Acesso em: 28 maio 2024.

PESTANA, Marcio. **Direito Administrativo Brasileiro**, São Paulo: Ed. Atlas, 4ª ed., 2014.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à Lei n. 13.709/2018 LGPD. 2. ed., São Paulo: Saraiva Educação, 2020. [versão digital])

PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de direito privado: parte especial**. Tomo XXII. Direito das obrigações: obrigações e suas espécies. Fontes e espécies de obrigações. Rio de Janeiro: Borsoi, 1958.

ROSENVALD, Nelson. **As funções da responsabilidade civil: a reparação e a pena civil**. 3. ed. São Paulo: Saraiva, 2017.

SAMPAIO Apud ANDRADE, Simone Caixeta de. Trajetória legal do marco civil. **ComCiência**, n. 158, p. 0-0. Campinas, mai. 2014.

SCHWARTZ, Paul; M. SOLOVE, Daniel J. **The PII Problem: Privacy and a New Concept of Personally Identifiable Information**. Review law 86N.Y.U.L.Q. Rev. 1814, 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366. Acesso em 17 de maio 2024.

SOLOVE, Daniel J. Data is what data does: regulating use, harm, and risk instead of sensitive data. Northwestern University Law Review, v 118, jan 2023, p. 35-36.

TELEPEDINO, Gustavo (Org.); TERRA, Aline de Miranda; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil: Responsabilidade Civil.** 2 ed. V 4. Rio de Janeiro: Forense, 2021. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2131/tde-28092022-105418/publico/11182092MIC.pdf. Acesso em 14 setembro 2024.

UNIÃO EUROPEIA. **Diretiva 95/46/CEdo Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046. Acesso em: 09 maio 2024.

UNIÃO EUROPEIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002**. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058. Acesso em: 09 maio 2024

UNIÃO EUROPEIA. **Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006**. Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32006L0024. Acesso em: 09 maio 2024

VAINZOF, Rony. Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados comentada**. São Paulo: Revista dos Tribunais, 2019.

ZIALCITA, Paolo. Facebooks Pays $643,00 Fine For Role In Cambridge AnalyticaScanda. Disponível em: https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal . Acesso em: 10 maio 2024.