UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE DIREITO

EDUARDA GUIZONI CARARA

OS LIMITES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS: UMA ABORDAGEM SOBRE O DIREITO FUNDAMENTAL E O LEGÍTIMO INTERESSE, À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO CONTEXTO BRASILEIRO

CRICIÚMA/SC

2024

EDUARDA GUIZONI CARARA

OS LIMITES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS: UMA ABORDAGEM SOBRE O DIREITO FUNDAMENTAL E O LEGÍTIMO INTERESSE, À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO CONTEXTO BRASILEIRO

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Direito da Universidade do Extremo Sul Catarinense, UNESC.

Orientadora: Profª Mª Mariana Mazuco Carlessi

CRICIÚMA

2024

EDUARDA GUIZONI CARARA

OS LIMITES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS: UMA ABORDAGEM SOBRE O DIREITO FUNDAMENTAL E O LEGÍTIMO INTERESSE, À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO CONTEXTO BRASILEIRO

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel no Curso de Direito da Universidade do Extremo Sul Catarinense, UNESC.

Criciúma, 04 de julho de 2024.

BANCA EXAMINADORA

Orientadora Profª Mariana Mazuco Carlessi - Mestra - (UNESC)

Prof. Dr. Gustavo Silveira Borges - Pós Doutor - (UNESC)

Prof. Dr – Maurício da Cunha Savino Filó - Doutor - (UNESC)

AGRADECIMENTOS

Primeiramente, agradeço a Deus por ter me dado força, sabedoria e a perseverança necessárias para concluir esta etapa importante da minha vida acadêmica. Sua presença constante foi meu alicerce em todos os momentos.

Aos meus pais, sou eternamente grata por todo amor, apoio e sacrifício. Vocês sempre acreditaram em mim, mesmo quando eu duvidava de minhas próprias capacidades. Seus exemplos de dedicação e coragem me inspiraram a seguir em frente e a nunca desistir dos meus sonhos. Este trabalho é, em grande parte, fruto de tudo o que aprendi com vocês.

Ao meu marido, minha profunda gratidão por sua paciência, compreensão e incentivo. Sua parceria inabalável e seu carinho foram fundamentais para que eu pudesse superar os desafios deste percurso. Obrigada por estar ao meu lado em cada passo, celebrando as vitórias e oferecendo conforto nas dificuldades.

À minha orientadora, Mariana, expresso meu sincero agradecimento por sua orientação e dedicação ao longo deste processo. Sua expertise, suas sugestões valiosas e seu constante encorajamento foram essenciais para a realização deste trabalho. Agradeço por acreditar no meu potencial e por contribuir significativamente para o meu crescimento acadêmico e pessoal.

Este trabalho é dedicado a todos vocês, que são minha fonte de inspiração e motivação.

“A menos que modifiquemos à nossa maneira de pensar, não seremos capazes de resolver os problemas causados pela forma como nos acostumamos a ver o mundo”.

Albert Einstein

RESUMO

Este trabalho tem como objetivo principal, analisar se o uso do legitimo interesse como hipótese de tratamento de dados, está em conformidade com a Lei Geral de Proteção de Dados, de forma a garantir os direitos fundamentais do titular. Utilizou-se o método dedutivo e teórico na pesquisa, partindo de princípios gerais por meio de referências bibliográficas, para se chegar a uma resposta específica do problema. Nesse sentido, o presente trabalho aborda a questão da privacidade e proteção de dados pessoais, como um direito fundamental na sociedade da informação, considerando o impacto da internet na coleta de dados e da sociedade de vigilância contínua. Além disso, analisa o desenvolvimento da legislação brasileira de proteção de dados, comparando-a com legislações estrangeiras e destacando a Lei Geral de Proteção de Dados Pessoais no Brasil, bem como a necessidade de bases legais para o tratamento de dados pessoais. Por fim, o estudo explora o conceito de legítimo interesse no tratamento de dados, examinando suas implicações legais, especialmente em relação aos dados sensíveis, e a responsabilidade dos agentes de tratamento em relação ao Relatório de Impacto.

Palavras-chave: Lei Geral de Proteção de Dados; Legítimo Interesse; Tratamento de Dados Pessoais; Relatório de Impacto.

ABSTRACT OU RESUMEN

This work's main objective is to analyze whether the use of legitimate interest as a data processing hypothesis is in compliance with the General Data Protection Law, in order to guarantee the fundamental rights of the holder. The deductive and theoretical method was used in the research, starting from general principles through bibliographical references, to arrive at a specific answer to the problem. In this sense, this work addresses the issue of privacy and protection of personal data, as a fundamental right in the information society, considering the impact of the internet on data collection and the society of continuous surveillance. Furthermore, it analyzes the development of Brazilian data protection legislation, comparing it with foreign legislation and highlighting the General Law for the Protection of Personal Data in Brazil, as well as the need for legal bases for the processing of personal data. Finally, the study explores the concept of legitimate interest in data processing, examining its legal implications, especially in relation to sensitive data, and the responsibility of processing agents in relation to the Impact Report.

Keywords: General Data Protection Law; Legitimate Interest; Processing of Personal Data; Impact Report.

LISTA DE ABREVIATURAS E SIGLAS

CC	Código Civil
CPC	Código de Processo Civil
COE	Conselho Europeu
GDPR	Regulamento Geral de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
STJ	Supremo Tribunal Federal

SUMÁRIO

1 INTRODUÇÃO

A privacidade e a proteção dos dados pessoais emergem como direitos fundamentais na era digital, marcando uma transformação significativa na sociedade da informação. O advento da internet trouxe consigo uma revolução na forma como os dados são coletados, armazenados e utilizados, tornando a privacidade uma questão central. No contexto atual, onde a coleta de dados é incessante e a vigilância é onipresente, torna-se imprescindível compreender o impacto da internet sobre a privacidade e os direitos de personalidade.

A internet, ao ampliar o acesso à informação e facilitar a comunicação, também abriu novas fronteiras para a coleta massiva de dados pessoais. Essa coleta muitas vezes ocorre de forma imperceptível para os indivíduos, gerando preocupações sobre a utilização desses dados e as possíveis violações à privacidade.

Nesse sentido, este trabalho terá como objetivo principal, analisar se o uso do legitimo interesse como hipótese de tratamento de dados, está em conformidade com a Lei Geral de Proteção de Dados, de forma a garantir os direitos fundamentais do titular. Já que, o direito à privacidade e a proteção dos dados pessoais se entrelaçam com os direitos de personalidade, que buscam resguardar a dignidade e a liberdade dos indivíduos. Esses direitos são fundamentais para garantir que cada pessoa tenha controle sobre suas informações e como elas são usadas, protegendo-as contra abusos e invasões indevidas. Pra se chagar a uma conclusão do problema apresentado, será utilizado o método dedutivo e teórico na pesquisa, permitindo de princípios gerais para a análise específica das questões, visando contribuir para o entendimento e a aplicação eficaz das normas de proteção de dados, promovendo um equilíbrio entre inovação tecnológica e respeito aos direitos fundamentais.

Para analisar o contexto, consta mencionar que, a sociedade contemporânea é frequentemente descrita como uma sociedade de vigilância, onde tecnologias avançadas permitem a monitoração contínua e detalhada das atividades individuais. A vigilância, seja ela estatal ou corporativa, levanta sérias questões éticas e legais, demandando um equilíbrio entre segurança, inovação e respeito aos direitos fundamentais. Neste cenário, o papel das legislações de proteção de dados se torna crucial para estabelecer normas claras e proteger os cidadãos contra abusos.

O desenvolvimento da legislação brasileira de proteção de dados reflete uma resposta a essa nova realidade. Inspirada por legislações estrangeiras sobre o

tema, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, o Brasil formulou a Lei Geral de Proteção de Dados Pessoais (LGPD) em 2018, no qual somente entrou em vigor em 2020. A LGPD representa um marco significativo ao definir diretrizes para o tratamento de dados pessoais e estabelecer direitos e obrigações para os envolvidos no processamento dessas informações. O surgimento dessa lei não só alinha o Brasil com padrões internacionais, mas também atende a uma necessidade crescente de regulamentação no campo da privacidade e proteção de dados.

A LGPD destaca a importância das bases legais para o tratamento de dados pessoais, fornecendo um conjunto de fundamentos que legitimam o processamento dessas informações. Entre essas bases, o legítimo interesse do controlador ou de terceiros surge como uma das mais discutidas. Analisar o legítimo interesse permite compreender como empresas e organizações podem processar dados sem o consentimento explícito do titular, desde que atendam a determinados critérios de necessidade e balanceamento de interesses. Essa abordagem é essencial para assegurar que o uso de dados seja justo e proporcional, respeitando os direitos dos indivíduos enquanto possibilita atividades empresariais legítimas e inovadoras. Além disso, o estudo do legítimo interesse contribui para a construção de práticas de *compliance* e governança em proteção de dados, promovendo a confiança e a transparência nas relações entre consumidores e organizações.

O tratamento de dados pessoais sensíveis, por sua vez, requer uma abordagem ainda mais rigorosa. Dados que revelam origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, entre outros, demandam proteções adicionais devido ao seu potencial de causar discriminação ou outros danos significativos. A LGPD estabelece critérios específicos para o tratamento desses dados, enfatizando a necessidade de bases legais sólidas e a implementação de medidas de segurança adequadas.

Para tanto, os agentes de tratamento de dados têm a obrigação de assegurar a conformidade com a LGPD, sendo responsáveis pela elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD). Esses relatórios são instrumentos fundamentais para avaliar os riscos associados ao processamento de dados e determinar as medidas necessárias para mitigá-los. Assim, a obrigatoriedade dos RIPDs reforça a transparência e a responsabilidade dos agentes de tratamento, promovendo uma cultura de proteção de dados mais robusta.

Por fim, ao explorar a privacidade e a proteção de dados pessoais como direitos fundamentais na sociedade da informação, este trabalho busca entender as implicações legais, éticas e sociais desse tema. A análise da legislação brasileira de proteção de dados, em comparação com modelos estrangeiros, e a discussão sobre o legítimo interesse no tratamento de dados pessoais, fornecem uma base para compreender como o Brasil está se posicionando frente aos desafios impostos pela era digital. A reflexão sobre esses aspectos é essencial para a construção de um ambiente digital mais seguro e respeitoso dos direitos individuais, contribuindo para uma sociedade mais justa e equitativa.

2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NA SOCIEDADE DA INFORMAÇÃO

Este capítulo tem o objetivo de explorar a relevância da privacidade e da proteção de dados pessoais como direitos fundamentais na sociedade contemporânea, especialmente no contexto da sociedade da informação. Inicialmente, será analisado o impacto da internet na coleta de dados, considerando as transformações e desafios gerados pela crescente digitalização da sociedade, incluindo práticas de coleta, armazenamento e uso de dados pessoais. Em seguida, será abordada a relação entre o direito à privacidade e a proteção dos dados pessoais em consonância com os direitos da personalidade. Serão exploradas as interseções entre esses conceitos fundamentais do direito, destacando a importância de garantir a integridade e autonomia do indivíduo no ambiente digital, bem como legislações e regulamentações pertinentes para proteger a privacidade e os dados pessoais dos cidadãos.

2.1 PRIVACIDADE E O IMPACTO DA INTERNET NA COLETA DE DADOS NO CONTEXTO DA SOCIEDADE DE INFORMAÇÃO

Na Era do *Big Data*, a privacidade é vista como o direito do cidadão de controlar suas próprias informações, em conformidade com o princípio da autodeterminação. Este princípio está enraizado na ideia de que as pessoas devem ter autonomia sobre suas vidas digitais e de como controlar suas próprias informações pessoais, podendo tomar decisões informadas sobre como esses dados serão coletados, utilizados e compartilhados (LEONARDI, 2011, p. 67-68). A autorregulação ganha importância em uma sociedade da informação, na qual a coleta e o fluxo de dados criam dinâmicas de poder, enfatizando sua relevância (RODOTÀ, 2008, p. 24-37).

Segundo Bioni (2021, p. 34), a análise de dados agora é feita não apenas em pequenas quantidades ou amostras, mas em todo o conjunto de dados disponíveis. Isso resulta em um aumento significativo no volume de dados processados, permitindo correlacionar diversos fatos e estabelecer padrões para inferir até mesmo probabilidades de eventos futuros.

Com a ascensão da internet e das novas tecnologias de informação e comunicação, impulsionaram o surgimento da era digital, também conhecida como sociedade da informação, promovendo uma modernização nas relações sociais e ampliando significativamente a transmissão de dados, conteúdos, imagens e informações. Isso ocorre porque os meios virtuais se adequam à nossa era, oferecendo velocidade e interatividade, o que facilita a disseminação de ideias e promove a união entre pessoas com interesses semelhantes (FORNASIER; LIMA, 2015, p. 5). O direito de acesso à internet é considerado um direito fundamental e que se origina dos princípios da dignidade da pessoa humana e da cidadania, conforme estabelecido nos incisos II e III do Artigo 1º da Constituição Federal de 1988 (BRASIL, 1998).

Para Pimentel e Cardoso (2015, p. 48) a internet não é apenas um meio de comunicação; ela se tornou parte integral da vida em sociedade, facilitando e mantendo as relações humanas. Esses dados se espalham quase como uma epidemia, atingindo grandes proporções tanto *online* quanto *offline* (RECUERO, 2009, p. 116).

A proteção de dados emergiu como uma questão política relativamente nova, especialmente em comparação com o estabelecido paradigma da privacidade. Sua importância aumentou devido à crescente disponibilidade de informações e ao precedente estabelecido pelo julgamento da Lei do Censo na Alemanha em 1983 (LEONARDI, 2011, p. 59). A questão é de natureza legal e está diretamente relacionada ao direito à privacidade. Além disso, é fundamental para a elaboração de políticas públicas que vão além do domínio jurídico, dada a dinâmica das tecnologias envolvidas no tratamento de dados pessoais (BENNET, 2018, p. 1-3).

Os dados pessoais são fundamentais para o funcionamento da economia, sobretudo devido à capacidade de processamento automatizado proporcionada pelas tecnologias. Atualmente, esses dados estão intimamente ligados à utilização da internet e outras formas de automação, exercendo influência em diversos modos, como a econômica, social e política. Os efeitos decorrentes do tratamento desses dados ultrapassam as fronteiras digitais e têm impacto no mundo físico (LIMBEGER, 2019, p. 563).

Devido à sua importância para o avanço econômico, é imprescindível reconhecer que o manuseio de dados pessoais também tem impactos na esfera da privacidade individual. Assim, torna-se necessário estabelecer mecanismos que

conciliem as estruturas de proibição, controle e processamento de dados, garantindo um equilíbrio adequado entre esses aspectos (RODOTÀ, 2008, p. 46-47).

Nesse sentido, Castells (2005, p. 24-25) já apontava que em todos os momentos ocorre a coleta de dados e as pessoas contribuem com suas informações para participar de uma sociedade em rede, na qual as redes sociais e os meios de comunicação promovem uma hiper conexão entre indivíduos e grupos. Esse contexto também é caracterizado como Sociedade da Informação. Vejamos:

> Nos últimos anos, a comunicação em ampla escala tem passado por profunda transformação tecnológica e organizacional, com a emergência do que denominei autocomunicação de massa, baseada em redes horizontais de comunicação multidirecional, interativa, na internet; e, mais ainda, nas redes de comunicação sem fio, atualmente a principal plataforma de comunicação em toda parte. Esse é o novo contexto, no cerne da sociedade em rede como nova estrutura social (CASTELLS, 2017, p. 153).

Assim, ao identificar as fontes de dados e descrever o processo de sua aquisição, também conhecido como coleta ou extração, torna-se evidente que o *Big Data* consiste na captura de *small data* (dados considerados individualmente), processados por computadores, coletados ao longo da vida dos indivíduos (ZUBOFF, 2018, p. 31).

Nas plataformas de comunicação, todos os dados são colhidos, desde curtidas, publicação de fotos, movimentações financeiras etc., sendo esses dados já alertados por Mendes e Doneda (2018, p. 469-483), que ao considerar o fluxo de dados, como aqueles relacionados a crédito e finanças para avaliar a capacidade de pagamento dos consumidores, bem como informações sobre saúde dos pacientes e padrões de comportamento coletados na internet, fica evidente a prevalência dos meios digitais.

A partir desse ponto, praticamente todos os dados pessoais de um indivíduo, obtidos através de suas interações digitais, são convertidos em informações e adquirem uma nova dimensão simbólica. A partir desse ponto, eventos, objetos, processos e pessoas se tornam visíveis, compreensíveis e compartilháveis de maneiras inéditas (ZUBOFF, 2020 p. 24).

A extração de dados mencionada, refere-se ao processo unilateral de coleta de dados pessoais dos usuários da internet. Esse processo ocorre sem que o indivíduo, necessariamente, esteja ciente da extração ou tenha dado consentimento para todos os fins a que esses dados serão destinados (ZUBOFF, 2020, p. 270).

Diante disso, o Ministro Ruy Rosado de Aguiar afirma: O cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo” (BRASIL, STJ, 1995, p.6119)

Pois, a análise de dados refere-se ao processo no qual os dados coletados são transformados em informações correspondentes, permitindo a visualização de comportamentos e características individuais ou de grupos, assim como a identificação de padrões (predição comportamental), sendo este processo necessário para tal análise onde os cientistas de dados precisam ter domínio sobre os novos métodos relacionados à análise preditiva, mineração de dados da realidade e análise de padrões de vida (ZUBOFF, 2018, p. 40).

Neste contexto, os novos métodos de análise preditiva e mineração da realidade envolvem algoritmos complexos. Algoritmos, em termos simples, são sequências pré-definidas de comandos automatizados que, a partir de dados, geram conclusões que podem influenciar ou não uma ação. Doneda e Almeida (2018, p. 141-148) corroboram essa definição, destacando que os algoritmos são conjuntos de instruções para uma determinada tarefa, resultando em uma saída específica.

Destaca Frazão (2021, p. 1) que o desafio de compreender, inclusive, torna-se quase impossível, uma vez que os algoritmos, geralmente, são como caixas pretas, apresentando um alto nível de complexidade e centenas ou milhares de etapas que são incompreensíveis para o homem comum e até mesmo para os programadores.

Diante disso, em meio à crescente digitalização e ao avanço das tecnologias de coleta e análise de dados, torna-se imperativo estabelecer políticas e regulamentações robustas que assegurem o respeito à privacidade e a proteção dos dados pessoais, dos quais veremos nos próximos capítulos deste trabalho. O equilíbrio entre a inovação tecnológica e a preservação dos direitos individuais torna-se, portanto, um desafio de extrema importância para a construção de uma sociedade justa e democrática, onde os indivíduos possam usufruir plenamente dos benefícios da era digital sem comprometer sua intimidade e segurança.

2.2 DIREITO À PRIVACIDADE E A PROTEÇÃO DE DADOS EM RELAÇÃO AOS DIREITOS DE PERSONALIDADE

De acordo com Doneda (2006, p. 126-127), a privacidade tem sido historicamente entendida através da distinção entre público e privado. O direito à privacidade baseava-se em concepções sobre quais atividades deveriam ocorrer na esfera pública e quais deveriam ser reservadas ao espaço privado dos indivíduos, sendo limitado pela ideia de que a residência dos indivíduos seria um local de proteção contra o escrutínio público. Nesse contexto, Arendt (2010, p. 77-85) considera o direito à privacidade como um fundamento democrático, pois acredita que, ao escapar da "pressão social", os indivíduos podem vivenciar e explorar suas subjetividades no espaço privado.

A privacidade pode ser vista como um direito baseado na liberdade negativa do seu titular, que tem o poder de decidir quais aspectos de sua vida estão inseridos em sua esfera privada e, consequentemente, são protegidos por esse direito (RODOTÀ, 2012, p. 320). Atualmente, não se pode analisar os desafios da privacidade de maneira tão simples, dividindo apenas entre "se esconder" e "se expor", ou entre pessoas que guardam segredos e aquelas que não têm nada a esconder. As ideias de valorizar a privacidade individual ou favorecer as interações sociais também não são mais tão práticas. Essas abordagens estão se tornando cada vez mais abstratas, pois não capturam totalmente a complexidade da privacidade, que precisa ser entendida de forma mais ampla do que apenas o indivíduo (RODOTÀ, 2008, p. 25).

Portanto, os direitos da personalidade são aqueles direitos que se relacionam com aspectos tangíveis e intangíveis que definem e distinguem uma pessoa. Entre os exemplos mais comuns listados no Código Civil, estão o direito ao nome, à honra, à integridade física e psicológica. Assim, considerando a diversidade entre as pessoas, o Direito nos resguarda contra violações à nossa individualidade (TEPEDINO, 2004, p. 29).

Através das informações reunidas sobre um indivíduo, é viável compreender, influenciar e até mesmo manipular seu comportamento, frequentemente sem o seu consentimento ou consciência. Com o aumento do uso da internet e das tecnologias inteligentes, identificar quem de fato possui o controle dessas informações torna-se uma tarefa desafiadora. No mundo virtual, embora o acesso seja generalizado, a vigilância é facilmente realizada, dependendo apenas do manejo das informações coletadas, o que coloca em evidência a complexidade de garantir a privacidade na era digital (FOUCAULT, 2005, p. 8-10).

A origem dos direitos da personalidade reside na percepção da importância de proteger os valores que vão além do patrimônio e são essenciais para a vida humana, juntamente com suas características e princípios associados, conforme explicado por Pereira (2010, p. 202), em sua doutrina:

> A concepção dos Direitos da Personalidade sustenta que, a par dos direitos economicamente apreciáveis, ditos patrimoniais, outros há, não menos valiosos, merecedores de amparo e proteção da ordem jurídica. Admite a existência de um ideal de justiça, sobreposto à expressão caprichosa de um legislador eventual. Atinentes à própria natureza humana, ocupam eles posição supraestatal, já tendo encontrado nos sistemas jurídicos a objetividade que os ordena, como poder de ação, judicialmente exigíveis.

Conforme a visão de Tepedino (2004, p. 47), os direitos da personalidade não necessitam ser tratados como um único direito subjetivo, nem serem categorizados em várias classificações diferentes. A abordagem mais adequada consiste em proteger de forma abrangente a pessoa em todos os seus aspectos. Por outro lado, a dignidade humana é considerada uma cláusula geral de proteção das pessoas, estando intimamente relacionada aos direitos fundamentais. Ambos funcionam em conjunto no cerne do discurso jurídico constitucional, sendo componentes essenciais e inseparáveis para qualquer sistema jurídico verdadeiramente democrático (PASQUALINI, 1999, p. 80-81).

No Brasil, após a promulgação da Constituição Federal de 1988, os direitos da personalidade foram formalmente integrados ao sistema jurídico nacional, fazendo parte do conjunto de Direitos e Garantias Fundamentais, garantindo assim sua proteção e eficácia, presente no Art. 5º, inc. X, da CF/88 que dispõe: “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).

Com o avanço da ciência e da tecnologia, as invasões à intimidade e à vida privada das pessoas tornaram-se mais frequentes e intensas (SZANIAWSKI, 2005, p. 118-119). Para Diniz (2016, p. 133-134), a personalidade não é em si um direito, portanto não seria correto dizer que as pessoas têm um direito à personalidade. Na verdade, a personalidade é a base dos direitos e deveres que surgem dela. É tratada como um objeto de direito e é considerada como o primeiro bem da pessoa, essencial para que ela possa ser quem é, sobreviver e se adaptar ao ambiente em que vive. Serve como um critério para avaliar, adquirir e organizar outros bens.

O doutrinador Bittar (2008, p.7-8), entende que os “direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, a honra, a intelectualidade e outros tantos”.

Em complemento, acerca da classificação dos direitos da personalidade, no entendimento de Pereira (2010, P. 202), incluem, portanto, o “direito à vida, à liberdade, ao próprio corpo, à incolumidade física, à proteção da intimidade, à integridade moral, à preservação da própria imagem, ao nome, às obras de criação do indivíduo e tudo mais que seja digno de proteção, amparo e defesa na ordem constitucional, penal, administrativa, processual e civil”.

Nesse sentido, Bittar (2008, p. 49) apresenta uma classificação dos direitos da personalidade em três categorias distintas: direitos físicos, psíquicos e morais. Os direitos físicos dizem respeito aos aspectos materiais do corpo humano, como a integridade corporal e a imagem. Já os direitos psíquicos englobam elementos intrínsecos à personalidade, como a liberdade e a intimidade. Por fim, os direitos morais abrangem atributos valorativos da pessoa na sociedade, como a identidade, a honra e as expressões intelectuais.

Numa sociedade onde as informações circulam constantemente, o direito à privacidade precisa se estender além da proteção da vida íntima. Ele também deve garantir que as pessoas tenham controle sobre seus dados pessoais. Às vezes, a exposição dos dados, mesmo que pareça inofensiva ao preencher um formulário ou acessar um site, pode ser tão prejudicial quanto invadir a privacidade de alguém em sua casa. O uso indevido desses dados pode causar diversos problemas para a pessoa envolvida (SCHREIBER, 2013, p. 135-136).

Conforme argumentado por Bioni (2021, p. 91), o direito à proteção dos dados pessoais deve ser reconhecido como um novo tipo de direito da personalidade. O autor adverte que, caso contrário, há o risco de esse direito não se desvincular das ideias tradicionais e da dinâmica do direito à privacidade, o que poderia impossibilitar a criação de uma legislação adequada para regular o fluxo de informações como um fator promotor da dignidade da pessoa humana (BIONI, 2021, p. 107).

Os dados pessoais são uma manifestação essencial da nossa identidade, refletindo nossas características individuais e nosso papel na sociedade. Portanto, é fundamental reconhecer a proteção dos dados pessoais como um direito da

personalidade, uma medida que está sendo considerada para inclusão em nossa gama de direitos fundamentais (COSTA; OLIVEIRA, 2019, p. 32).

Nesse sentido, Rodatà (2008. p. 23-24), ressalta que o desafio para garantir o direito à privacidade na era moderna é diferente de períodos históricos anteriores. Atualmente, o debate não gira mais em torno de proteger a privacidade contra invasões de terceiros. A perspectiva atual está em compreender o cenário atual da distribuição de poder, onde a infraestrutura de informação desempenha um papel fundamental como um de seus principais componentes.

Portanto, para garantir o direito essencial à privacidade no contexto digital, além de proteger a intimidade e a vida privada, é fundamental ampliar o conceito de privacidade para incluir outras formas desse direito, como a segurança e a proteção dos dados pessoais armazenados na internet por indivíduos ou coletados por organizações públicas e privadas.

2.3 A SOCIEDADE DE VIGILÂNCIA NA CONTEMPORANEIDADE

Na era da sociedade da informação, a vigilância constante está presente, embora nem sempre seja óbvia, devido à ampla distribuição do monitoramento resultante do avanço tecnológico. Por exemplo, ao navegar na internet ou usar serviços online, as pessoas agem tranquilamente sem perceber exatamente como estão sendo monitoradas, por quem e com qual objetivo (GUARDIA, 2020, p. 494).

Existe, portanto, uma preocupação crescente sobre a perspectiva do fim da privacidade na sociedade da vigilância, devido à enorme quantidade de dados pessoais que são coletados e transformados em informações sobre a personalidade e a intimidade de seus titulares. Esses dados são usados por empresas para analisar o comportamento das pessoas (RODOTÀ, 2008, p. 13).

No contexto histórico, considera-se que ocorreu após os eventos do atentado de 11 de setembro nos Estados Unidos, pois, observou-se um progressivo declínio da privacidade e de outras garantias fundamentais, impulsionado pela crescente demanda por transparência. Isso abriu uma oportunidade para diversas empresas coletarem, analisarem e categorizarem dados pessoais visando o controle de indivíduos (RODOTÀ, 2008, p. 14).

A diminuição do direito à privacidade na sociedade contemporânea evoca a ideia da sociedade de vigilância, concebida primeiramente por Foucault (1999, p.

88), como uma sociedade disciplinar inserida em uma estrutura de poder hierárquica, que descreve a implementação de dispositivos de vigilância destinados ao controle dos observados, caracterizando uma forma de vigilância centralizada.

Conforme observado por Han (2018, p. 65-66), a sociedade da transparência possui uma íntima ligação estrutural com a sociedade da vigilância, uma vez que pode obter informações com facilidade, seguindo a lógica da eficiência. Nesse contexto, cada clique é armazenado, a maioria dos passos é rastreável e há rastros digitais por toda parte. Assim, a vigilância e o controle tornam-se elementos intrínsecos à comunicação digital, onde todos observam e monitoram uns aos outros.

Na atual era da informação total, a vigilância permeia todos os ângulos, sem uma centralização definida. Apesar de muitos sentirem-se completamente livres, a evolução de técnicas conduz à hipercomunicação, desenhando assim o panorama do panóptico digital (HAN, 2018, p. 60). Nesse contexto, todos contribuem ativamente para a manutenção desse sistema ao se exporem e exporem os outros de forma contínua, como apontado pelo autor:

> Os caçadores digitais de informação estarão sempre andando com os seus Google Glass. Esses óculos de dados substituem as lanças, os arcos e as flechas dos caçadores paleolíticos. O Google Glass liga o olho humano diretamente à internet. Seus usuários, por assim dizer, veem a tudo. Eles introduzem a era da informação total (HAN, 2018, p. 43).

Nesse contexto, observa-se que a extração de dados se assemelha a uma prática predatória, sempre visível e abarcada pela perspectiva global, ressaltando assim a vitalidade da informação na sociedade contemporânea. Assim, o indivíduo na sociedade contemporânea não se expõe por pressão externa, mas por uma escolha própria, impulsionado por uma necessidade que ele mesmo cria. Movido pelo receio de perder sua esfera privada e íntima, ele cede à necessidade de exposição, sem restrições (HAN, 2017, p. 60).

O conceito elaborado por Zuboff (2020) exemplifica o que a autora denomina de capitalismo de vigilância, uma ideia intimamente relacionada ao avanço tecnológico na sociedade de consumo. Alguns argumentam que na internet os sujeitos que fornecem seus dados são a mercadoria em si. No entanto, essa interpretação precisa ser reconsiderada, de acordo com Zuboff, pois os sujeitos não são simplesmente objetos; eles são, na verdade, os objetos cuja coleta de dados pessoais representa o novo capital (ZUBOFF, 2020. p. 22).

Ainda, salienta a autora (2020, p. 23-24) que o capitalismo de vigilância representa a nova ordem global que o capitalismo contemporâneo adquiriu, originando-se no Vale do Silício, onde os dados pessoais emergiram como os ativos mais preciosos do mercado, extrai-se:

> Os capitalistas de vigilância descobriram que os dados comportamentais mais preditivos provêm da intervenção no jogo de modo a incentivar, persuadir, sintonizar e arrebanhar comportamento em busca de resultados lucrativos. Pressões de natureza competitiva provocaram a mudança, na qual processos de máquina automatizados não só conhecem nosso comportamento, como também moldam nosso comportamento em escala. Com tal reorientação transformando conhecimento em poder, não basta mais automatizar o fluxo de informação sobre nós; a meta agora é nos automatizar (ZUBOFF, 2020 p. 24).

Nesse sentido, consta mencionar que a internet, mesmo sendo uma novidade relativa, tem sido um catalisador de muitas mudanças sociais significativas. Pode ser vista como um espaço de comunicação global devido à interconexão de computadores em todo o mundo. Ela não é apenas a estrutura física da comunicação digital, mas também um vasto reservatório de informações, onde os seres humanos navegam e contribuem para esse universo, como observado por Levy (LEVY, 1999, p. 29).

Entretanto, apesar dos benefícios proporcionados por essas inovações, surgem também preocupações profundas relacionadas à privacidade e ao consentimento. Ainda no conceito de Zuboff (2020, p. 19), a sociedade de vigilância atual está profundamente ligada ao capitalismo de vigilância, que utiliza todas as nuances da experiência humana, desde vozes até emoções, presentes nos nossos dados pessoais. Esses dados são controlados e transformados em informações comportamentais valiosas para diversos mercados. Eles são adquiridos de forma gratuita através dos nossos rastros digitais, deixados em nossas atividades online, como pesquisas na internet e registros de compras online.

A estrutura da sociedade contemporânea, caracterizada pela constante vigilância e busca incessante por dados, deu origem à necessidade de regular as interações no ambiente digital, com foco especial na proteção dos dados pessoais. As leis passaram a acompanhar e controlar as novas dinâmicas da internet, com o objetivo de preservar principalmente os dados compartilhados e a privacidade, assim como outros direitos inerentes a essa nova era tecnológica.

Nesse contexto, a promulgação da Lei Geral de Proteção de Dados Pessoais em 2018 no Brasil surgiu para estabelecer diretrizes de proteção de dados, inclusive no âmbito digital, e salvaguardar direitos fundamentais, como será discutido mais detalhadamente no próximo tópico.

3. O DESENVOLVIMENTO DA LEGISLAÇÃO BRASILEIRA DE PROTEÇÃO DE DADOS

No âmbito do desenvolvimento da legislação brasileira sobre proteção de dados, é imprescindível analisar as abordagens adotadas por outras nações no que diz respeito à privacidade e proteção de dados.

Essa compreensão do panorama internacional oferece insights valiosos para a formulação de políticas eficazes no Brasil, alinhadas com as melhores práticas globais e os padrões internacionais de proteção de dado, como por exemplo a influência do Regulamento Geral de Proteção de Dados (GDPR).

Posteriormente, será examinado o surgimento e a evolução da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, onde serão abordados os principais aspectos dessa legislação, como seus fundamentos, objetivos e impactos esperados na sociedade. Além disso, será discutida a importância de estabelecer bases legais sólidas para o tratamento de dados pessoais, destacando a LGPD como um marco normativo essencial para garantir a proteção da privacidade e a segurança dos dados dos cidadãos brasileiros.

3.1 LEGISLAÇÕES ESTRANGEIRAS SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS

É notável a influência da GDPR em várias regulamentações nacionais sobre dados pessoais, uma vez que ela foi uma pioneira nesse campo. Até o momento, é considerada o marco regulatório mais abrangente, tanto em termos legais quanto estruturais, no que diz respeito às questões de privacidade virtual. Uma das principais bases legais de seu regimento é o consentimento expresso e inequívoco dos usuários, que deve ser claro, explícito e fornecido antes da coleta e uso dos dados pessoais, podendo ser revogado a qualquer momento (OLIVEIRA; GUERRA, 2020, p. 75-83).

Para Mendes (2019, p. 39) a importância de elevar o patamar de segurança dos dados pessoais e a proteção desses dados, representa uma extensão da identidade individual e, portanto, merece ser salvaguardada pela jurisdição.

Diante disso, a difusão da legislação de proteção de dados teve início mundialmente em meados de 1970 na Alemanha, pois desde essa década, os países

têm trabalhado juntos para criar regras sobre como lidar com dados pessoais na internet. Isso envolve princípios básicos para proteger esses dados em um mundo cada vez mais conectado digitalmente (MENDES; FONSECA, 2020, p. 512).

Na linha cronológica de Doneda (2020, p. 192), dispõe que no ano de 1980, a (OCDE), estabeleceu um comitê de ministros e emitiu diretrizes que delinearam princípios fundamentais sobre a proteção de dados e o intercâmbio de informações entre países com legislações próprias, alinhadas aos princípios estabelecidos nas diretrizes. No entanto, apesar dessas diretrizes, não havia uma força vinculativa para estabelecer um padrão, levando a interpretações variadas e à criação de diversas leis em várias nações. Isso resultou em cada país adotando sua própria abordagem em relação à proteção de dados (OCDE, 2002, p. 2).

Após, no ano de 1981, Freire e Dissenha (2021, p. 5-6), evidenciam que a Comissão Europeia aprovou a Convenção nº 108, que se tornou um instrumento legal internacional primário. Essa convenção foi projetada para proteger os indivíduos contra o uso indevido e a coleta abusiva de dados pessoais, proibindo o processamento de informações confidenciais relacionadas à raça, política, saúde, religião, vida sexual, antecedentes criminais e outras. Além disso, a convenção garantiu o direito dos indivíduos de saber quais informações estão sendo armazenadas sobre eles e, se necessário, corrigi-las (COE, 1981, p.18).

Nesse contexto, acerca da Convenção nº 108, complementa Doneda (2020, p. 194):

> […] a Convenção deixa claro que a proteção de dados pessoais se refere diretamente à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para esse campo a disciplina, evidenciando sua deferência ao artigo 8° da Convenção Europeia para os Direitos do Homem.

Em 1983, uma decisão de grande relevância foi proferida pelo Tribunal Constitucional Alemão, que reconheceu o direito à autodeterminação da informação. O tribunal declarou que a Lei do Censo era inconstitucional no que diz respeito às obrigações dos cidadãos de fornecer dados, incluindo a imposição de multas e a permissão para o compartilhamento desses dados entre órgãos públicos federais (ARANHA; FERREIRA, 2020, p. 1)

Para Mendes (2008, p. 50), a decisão da Corte Constitucional estabeleceu um direito à autodeterminação da informação, o que influenciou as leis nacionais e europeias sobre proteção de dados. Ela reconheceu que as pessoas têm um direito

fundamental sobre seus dados e devem ter controle sobre eles, tornando o indivíduo central no processo de tratamento de dados. Isso limita o poder legislativo, que deve respeitar esse direito ao formular leis relacionadas à proteção de dados pessoais.

Ainda, segundo Mendes (2019, p. 43-44), acerca da linha temporal da proteção de dados no Brasil, destaca-se o ano de 1990, pela criação do Código de Defesa do Consumidor, estabelecido na Lei nº 8.078/90, que regula o uso de bancos de dados de consumidores e estabelece regras sobre o acesso a informações pessoais e de consumo arquivadas sobre o consumidor, permitindo correções em caso de imprecisões.

Em 1996, a Lei de Interceptação Telefônica e Telemática, Lei nº 9.296/96, no art. 10, reconheceu o direito à privacidade ao limitar o uso desses recursos apenas com autorização judicial para investigações específicas (BRASIL, 1996).

No ano seguinte, em 1997, diante das sociedades civis marcadas pelo trauma do uso autoritário da informação, surgiu a necessidade de um instrumento para requisitar informações pessoais em posse do poder público. Isso era desejado e crucial tanto para proteger os direitos fundamentais quanto para promover uma cultura democrática. Foi nesse contexto que o *habeas data* Lei nº 9.507/97, foi concebida, proporcionando aos cidadãos um meio direto de acessar e, se necessário, corrigir as informações sobre si mesmos armazenadas em bancos de dados (DONEDA, 2020, p. 272).

Para Lugati e Almeida (2020, p. 2), salientam que na Europa, no ano de 1995, a União Europeia aprovou e sancionou a Diretiva nº 46, uma legislação abrangente voltada para a proteção de dados pessoais. Essa diretiva foi amplamente discutida em todo o mundo até a aprovação do GDPR, já que a criação dessa legislação serviu como catalisador para outros países.

Embora a diretiva não tivesse força legal vinculativa para os países membros, ela serviu como referência para as legislações nacionais, e muitos de seus princípios fundamentais foram mantidos no GDPR. Sob essa diretriz, os princípios de proteção devem ser aplicados a todas as atividades de tratamento de dados pessoais, com as atividades dos controladores de dados sendo regidas pelo Direito Comunitário. Além disso, é observado o princípio de excluir o tratamento de dados realizado por indivíduos no exercício de atividades exclusivamente pessoais ou domésticas, como por exemplo as correspondências ou listas de endereços (UE, 2016, p. 2).

No contexto da evolução das normas de proteção de dados no Brasil, várias outras leis também abordaram a proteção de dados pessoais, incluindo o Código Civil (Lei 10.406/2002), a Lei do Cadastro Positivo (Lei 12.414/2011) e a Lei de Acesso à Informação Pública (Lei 12.527/2011), conforme destaca Mendes (2019, p. 44).

Diante disso, para Salomão (2016, p. 7-8), o Marco Civil da Internet foi a Lei 12.965/14, de 2014, tem três pilares fundamentais, sendo a neutralidade da rede, liberdade de expressão e privacidade, dos quais estabelece diretrizes para a doutrina e para a atuação dos Tribunais, onde seu objetivo principal é manter o caráter aberto da internet, presente no artigo 3º, no qual enumera princípios como a proteção da privacidade e dos dados pessoais, e no artigo 7º, que garante direitos como a inviolabilidade e sigilo do fluxo de comunicações, bem como das comunicações privadas armazenadas, exceto por ordem judicial. Já no artigo 10º, § 1º, destaca a proteção específica dos registros, dados pessoais e comunicações privadas, deixando claro que tais dados podem ser fornecidos mediante ordem judicial, exigindo que o responsável pela guarda os disponibilize nesses casos.

Em 27 de abril de 2016, foi aprovado o Regulamento Geral de Proteção de Dados (GDPR), que substituiu a Diretiva 95/46/CE. O GDPR mantém os mesmos princípios da diretiva anterior, como aponta Malheiros (2017, p. 10). Esse regulamento foi elaborado com o objetivo de estabelecer diretrizes e normas para proteger os direitos das pessoas físicas em relação ao tratamento e circulação de seus dados pessoais. Adicionalmente, foi exigido que países mantivessem legislação compatível com o GDPR para manter relações comerciais com a União Europeia (UE, 2016, p. 2).

E finalmente, no ano de 2018 a Lei nº 13.709/2018 foi promulgada, nomeada como Lei Geral de Proteção de Dados (LGPD), que somente entrou em vigor em 2020 (BRASIL, 2018)

Por fim, cabe destacar que as leis de outros países referentes à privacidade e proteção de dados têm evoluído para acompanhar os avanços tecnológicos e atender às crescentes preocupações com a segurança das informações pessoais. Desde os primeiros marcos regulatórios até as mais recentes medidas, como o GDPR na União Europeia, essas regulamentações buscam encontrar um equilíbrio entre a inovação tecnológica e a salvaguarda dos direitos individuais. Para tanto, criou-se a necessidade da LGPD no Brasil, do qual será abordado no capítulo seguinte.

3.2 O SURGIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A promulgação da LGPD, Lei nº 13.709/2018, representa um marco significativo no Brasil, visando principalmente regulamentar as relações que envolvem dados pessoais. Seu principal objetivo é proteger os titulares desses dados diante da constante ameaça de compartilhamento ilegal na sociedade da informação.

Apesar de ter sido promulgada em 14 de agosto de 2018, a LGPD só entrou em vigor em setembro de 2020, com a aplicação de sanções iniciando apenas em agosto de 2021 (BRASIL, 2018). Foi amplamente reconhecido que era necessário um período de adaptação à nova legislação, especialmente para as empresas, devido à complexidade das novas regras e ao volume de dados a serem ajustados para garantir a conformidade (TEIXEIRA, 2020, p.27).

Além de ser crucial para regulamentar as relações envolvendo dados, a promulgação da LGPD posicionou o Brasil entre os países considerados adequados em proteção da privacidade e dos dados pessoais. Isso coloca o país ao lado de outras nações que possuem legislações semelhantes de proteção de dados (SARLET, 2021, p. 305).

A LGPD é considerada uma lei de caráter principiológica, destacando-se por sua missão de proteger as relações que envolvem dados pessoais, com especial atenção aos direitos do titular de dados (PINHEIRO, 2020, p. 40).

Nos primeiros artigos, a lei destaca seu propósito de proteger direitos fundamentais de liberdade e privacidade, fundamentando-se nos direitos humanos, na dignidade e no exercício da cidadania pelas pessoas. Além disso, ressalta a autodeterminação informativa, a liberdade de expressão, de informação, comunicação, opinião, entre outros (BRASIL, 2018).

Para Doneda (2020, 161), acerca da autodeterminação informativa consoante a Lei, vejamos:

> Tanto a doutrina da autodeterminação informativa quanto a da liberdade informática foram fundamentais para o desenvolvimento dos atuais sistemas de proteção de dados pessoais e para o próprio direito à privacidade, em um sentido mais amplo. Não obstante, uma crítica baseada em seus pressupostos e no estágio atual da tecnologia, bem como da doutrina, nos sugere estarmos atentos a alguns aspectos de sua enunciação.

Nesse sentido, o artigo 5º, inciso I, a LGPD define dados pessoais como "informação relacionada a pessoa natural identificada ou identificável", e ainda distingue e define os dados pessoais sensíveis no inciso II do mesmo artigo (BRASIL, 2018).

Os dados pessoais sensíveis, descritos no inciso II do artigo 5º da LGPD, são considerados dados suscetíveis de gerar preconceito, pois podem ser utilizados com a finalidade de discriminação, incluindo informações como origem étnica ou racial, dados genéticos ou biométricos (RODOTÀ, 2008, p. 96).

Da mesma forma, a legislação proporciona uma camada extra de proteção aos dados pessoais de crianças e adolescentes, como descrito no artigo 14. Isso reflete um cuidado mais detalhado com os dados sensíveis e a salvaguarda dos interesses coletivos e difusos (BRASIL, 2018). Pois, em cada ordenamento jurídico, o regime adotado em relação aos dados sensíveis varia de acordo com as concepções a este respeito. É necessário ter em conta que a diferenciação conceitual dos dados sensíveis atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior. Reconhecemos, porém, que há situações nas quais a discriminação pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos (DONEDA, 2020, p. 144-145).

É crucial destacar que, de acordo com o artigo 7º, inciso I, a lei enfatiza a importância do consentimento do titular de dados pessoais. Define-se o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", conforme descrito no artigo 5º, inciso XII (BRASIL, 2018).

Ressalta-se que o consentimento passou a ser empregado como um instrumento de expressão da vontade do indivíduo, podendo evidenciar tanto o aspecto da autodeterminação quanto o da legitimação (DONEDA, 2006, p. 56).

Acerca do consentimento, no artigo 2o, alínea h, da lei, pode-se ainda observar a conceituação do consentimento, sendo trazido como “qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento”. Ademais, na alínea a do artigo 7o, vê-se que o consentimento é colocado como fundamental no tratamento de dados, excluídos os casos de dispensa, o que se assemelha inclusive com a disposição feita pela LGPD (BRASIL, 2018)

A legislação, no entanto, também descreve situações específicas em que o consentimento não é necessário, como para a realização de estudos por órgãos de pesquisa, desde que os dados pessoais sejam anonimizados sempre que possível; para a proteção da vida ou da integridade física do titular ou de terceiros; para o cumprimento de obrigações legais ou regulatórias pelo controlador, entre outros casos (BRASIL, 2018).

Nesse contexto, com o surgimento da Lei Geral de Proteção de Dados Pessoais no Brasil reflete a resposta à crescente preocupação com a privacidade em meio ao avanço tecnológico. A legislação busca garantir maior controle e transparência no tratamento de informações pessoais, incluindo o tema do tratamento de dados, a ser abordado adiante.

3.3 A NECESSIDADE DE BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados do Brasil (LGPD - Lei nº 13.709/18) foi promulgada para estabelecer uma base legal específica para o tratamento de dados (TEFFÉ; VIOLA, 2019, p. 1-38).

Esse cenário destacou a necessidade de uma legislação específica para proteger os direitos fundamentais de privacidade, liberdade e dados pessoais do indivíduo. O objetivo é fornecer ao titular dos dados os instrumentos legais necessários para uma proteção abrangente de seus dados e direitos, permitindo algum controle sobre o fluxo das informações tratadas. A privacidade também é entendida como o direito à autodeterminação informativa (BUCHAIN 2019, p. 209-229).

Na análise de Teixeira e Guerreiro (2022, p. 31) sobre a lei, é ressaltado que a LGPD, como exposto no item 3.2, não visa prioritariamente proteger a propriedade dos dados, mas sim o titular dos mesmos. O primeiro artigo da lei reitera essa abordagem, enfatizando sua aplicabilidade às pessoas naturais e introduzindo conceitos como o do titular de dados, que desempenha um papel central na legislação.

Ainda para Teixeira e Guerreiro (2022, p. 32), destaca que na era da informação, a utilização de dados pessoais se torna essencial, porém a lei estabelece limites para garantir a preservação desse direito fundamental ao indivíduo. A individualidade do titular precisa ser reavaliada para ser incorporada ao bem comum.

O legislador enfatiza que a titularidade dos dados pertence à pessoa natural, exigindo que qualquer tratamento respeite as normas legais e reconheça o direito do titular sobre seus dados, mesmo que dispersos em múltiplos bancos de dados pelo mundo.

Atualmente, a privacidade envolve também conceder ao titular de dados o controle sobre o fluxo e os usos de suas informações pessoais, dada a gravidade das consequências que um tratamento indiscriminado de dados pode acarretar (PEIXOTO, 2016, p. 358).

Em outras palavras, o titular de dados deve ter o controle sobre o fluxo de suas informações, tanto online quanto offline (RODOTÀ, 2008, p. 97-98). Privacidade também significa ter o direito à autodeterminação informativa, permitindo que o titular controle sua própria vida e evite abusos por parte dos responsáveis pelo tratamento de dados. Estes não devem ter permissão para usar os dados de forma indiscriminada ou para finalidades não autorizadas ou desconhecidas pelo titular. Isso poderia prejudicar o livre desenvolvimento da personalidade individual, já que os dados fazem parte da identidade do indivíduo e são intrínsecos a ele, e não fatores separados (DANTAS; COSTA, 2020, p. 69-89).

Segundo Reis (2021, p. 157) essa distinção de forma clara em sua obra, destacando que os dados refletem a personalidade de uma pessoa. Portanto, tanto os dados comuns quanto as sensíveis possuem um valor significativo para o mercado, uma vez que, com o tratamento adequado, é possível obter informações específicas sobre várias facetas do titular, permitindo a indução de comportamentos presentes e futuros.

Conforme Mendes (2014, p 55-56) esclarece que as técnicas computacionais disponíveis atualmente, proporcionaram habilidades antes inimagináveis para gerar conhecimento a partir de dados. Ela destaca que o valor das informações obtidas não está apenas na capacidade de armazenar grandes volumes de dados, mas, principalmente, na capacidade de obter novos elementos informativos sobre os cidadãos através do tratamento desses dados.

Nesse interim, o tratamento de dados, segundo a LGPD, engloba todo o ciclo de manipulação dos dados, desde sua coleta até seu processamento e eventual transmissão. Essa abordagem está alinhada com a natureza dos dados, uma vez que a simples digitalização de informações coloca esses dados na linha de produção de conhecimento característica do ambiente virtual (DONEDA, 2020, p. 140),

Conforme estabelece o artigo 5º, X da LGPD, o tratamento de dados é:

> (...) toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

A LGPD estabelece deveres e responsabilidades para aqueles que realizam o tratamento de dados pessoais. Atuando de maneira horizontal, abrangendo os setores econômicos, tanto o privado quanto o público (TEPEDINO; TEFFÉ, 2019, p. 287-322).

Cabe as empresas ou entidades que lidam com dados pessoais devem ser transparentes quanto ao uso desses dados e assegurar a segurança daqueles que são armazenados e processados. De acordo com a seção II do Capítulo VI da lei, é estipulado que as empresas designem um responsável pelo tratamento de dados pessoais, cujo papel principal é fornecer informações às autoridades governamentais e tomar medidas para garantir a conformidade com a LGPD (Brasil, 2018). Em suma, o responsável pelo tratamento de dados pode ser considerado como um agente de aplicação da lei, atuando como intermediário entre os titulares de dados, as empresas e a Autoridade Nacional de Proteção de Dados (ANPD).

Diante disso, as bases legais que permitem o tratamento de dados estão enumeradas nos incisos do artigo 7º da lei, em uma lista exaustiva.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).

Ainda, cumpre destacar que no artigo 11 da LGPD, está elencado as bases legais, no tocante aos tratamentos de dados pessoais sensíveis. Esses dados recebem uma proteção adicional devido à sua natureza mais íntima, estando mais próximos da privacidade do indivíduo. Geralmente, são dados que podem potencialmente resultar em situações discriminatórias para o indivíduo, como opiniões políticas ou religiosas, por exemplo. Ainda, outra observação relevante, é que as bases legais não possuem hierarquia entre si; ou seja, nenhuma é considerada mais importante do que a outra (LEONARDI, 2019, p. 71-85).

Ademais, a fim de garantir a legitimidade do tratamento, basta a aplicação de uma das bases legais listadas, sendo também possível que um tratamento de dados seja autorizado por mais de uma base legal (LIMA, 2019, p. 179-188).

Ao realizar o tratamento de dados, o agente deve estar respaldado por pelo menos uma das bases legais listadas na lei, as quais fundamentam sua atividade. Caso contrário, o tratamento de dados será considerado irregular, sujeitando o agente a possíveis sanções administrativas e/ou judiciais (OLIVEIRA; CORTS, 2020, p. 50).

No tocante ao definir o que seria um “tratamento irregular de dados pessoais”, a lei afirma no art. 44 da LGPD os critérios, quais sejam:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
>
> I - o modo pelo qual é realizado;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;
>
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
>
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (BRASIL, 2018).

Nota-se a partir deste artigo acima indicado, que a legislação não define minuciosamente o que constituiria um "tratamento irregular", entretanto, apenas apresenta uma cláusula geral de proteção, utilizando conceitos jurídicos indeterminados que podem ser adaptados para novas técnicas que surjam no futuro (DALLARI; MONACO, 2020, p. 5)

Nesse contexto, observou Albers (2016, p. 43), de que é difícil prever completamente o tratamento de dados e as decisões resultantes, mostrando que o direito de proteção de dados deve se concentrar mais na regulamentação dos riscos do que no controle absoluto. Extrai-se:

> Em contraposição aos conceitos originais de proteção de dados, de fato não é possível prever com facilidade o tratamento de dados e informações pessoais, o conhecimento gerado a partir deles e as decisões daí resultantes. A ideia de que esses processos pudessem ser quase completamente previstos, planejados e controlados por meios jurídicos mostrou ser demasiado simples. O processamento de dados e informações, a geração de informação e conhecimento, a tomada de decisões com base em informação e conhecimento incluem certa dinâmica e incerteza em muitos pontos. Isso se aplica com mais razão ainda com vistas ao uso de tecnologias. Consequentemente, é menos a ideia de controle que caracteriza ou deveria caracterizar o direito referente à proteção de dados do que, de modo semelhante ao direito ambiental, a ideia de regulamentação dos riscos.

Portanto, é crucial a importância das bases legais para o tratamento de dados pessoais. Em um cenário onde a tecnologia permeia cada aspecto das vidas das pessoas, garantir a conformidade com regulamentos e leis de proteção de dados é fundamental para preservar a privacidade e a dignidade dos indivíduos. A existência de estruturas legais sólidas não apenas protege os direitos dos cidadãos, mas também promove a confiança nas instituições e nos serviços digitais, contribuindo para um ambiente mais seguro e ético de troca de informações.

4. O LEGÍTIMO INTERESSE NO TRATAMENTO DE DADOS PESSOAIS

Neste capítulo, serão discutidos diversos aspectos relacionados ao conceito de legítimo interesse no tratamento de dados pessoais. Primeiramente, será explorada a base legal que permite aos controladores ou terceiros utilizarem o legítimo interesse como justificativa para o tratamento de dados, bem como o tratamento para o uso dos dados sensíveis. Além disso, serão abordadas as responsabilidades dos agentes de tratamento em relação ao Relatório de Impacto, sob a perspectiva da Lei Geral de Proteção de Dados (LGPD). Ao compreender esses pontos, será possível ter uma visão mais clara sobre os limites e obrigações relacionados ao uso do legítimo interesse na gestão de informações pessoais.

4.1 LEGÍTIMO INTERESSE: UMA PERSPECTIVA LEGAL PARA O TRATAMENTO DE DADOS DO CONTROLADOR OU TERCEIROS

Conforme o Parecer 06/2014, formulado pelo “Grupo de Trabalho do Artigo 29”, constituído pelas Autoridades de Proteção de Dados na União Européia do qual atuou até 2016, quando o EDPB assumiu essa função, chamado de Comité Europeu para a Proteção de Dados (*European Data Protection Board*), descreveu a palavra "legítimo" na Diretriz que tanto o propósito do tratamento dos dados quanto o interesse almejado. Desta forma, o mesmo adjetivo é frequentemente empregado na LGPD para estabelecer a base legal do tratamento de interesse legítimo (UNIÃO EUROPEIA, 2014, p.36)

Segundo Silva (2019, p. 87), é fundamental estabelecer um escopo claro do que se entende por "interesse legítimo" para evitar cenários de manipulação inadequada de dados.

Nesse sentido, o interesse legítimo é uma maneira legal ampla e maleável para lidar com informações. Às vezes, os responsáveis ou outros interessados o usam como uma forma de tornar mais flexível o sistema rigoroso de proteção de informações, tanto no Brasil quanto na Europa (BIONI 2019, p. 248-249).

A criação de um sistema rígido de proteção é adequada, uma vez que o Direito não acompanha a mesma velocidade de atualização das inovações tecnológicas (BENNET, 2018, p.5), que busca um equilíbrio entre as estruturas proibitivas de controle, coleta e tratamento de dados e as bases legais para esses

processamentos, por meio de instrumentos de flexibilização. Assim, a interpretação das bases que flexibilizam esse processo, como o legítimo interesse, se adaptam às alterações tecnológicas, sociais, culturais e contextuais (RODATÀ, 2008, p. 41-47).

No entanto, a intervenção dos controladores de dados ou terceiros interessados deve ser possível em determinados casos, utilizando instrumentos regulatórios mais resilientes e flexíveis, que ao mesmo tempo garantam a proteção dos direitos estabelecidos pelas normas sobre o tema (BENNET, 2018, p.5-6).

Assim, a legislação brasileira, por meio do inciso IX do artigo 7 da LGPD, estabeleceu uma previsão legal abrangente o bastante para permitir a flexibilização da proibição de tratamento de dados pessoais. A regulação do legítimo interesse é também contemplada nos artigos 10 e 37, conforme segue abaixo:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> (...)
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de
> prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
>
> Art. 10 O legítimo interesse do controlador somente poderá fundamentar tratamento de dados
> pessoais legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> I - apoio e promoção de atividades do controlador; e
>
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços
> que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades
> fundamentais, nos termos desta Lei.
>
> §1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados
> pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
>
> §2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados
> em seu legítimo interesse.
>
> §3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de
> dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados
> os segredos comercial e industrial.

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de
> dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (BRASIL, 2018).

Segundo o entendimento de Bioni (2021, p.22) sobre a Lei, o termo "legítimo" é utilizado junto à definição do princípio da finalidade, bem como ao se enunciar a base legal contida no Art. 7º, IX, o legítimo interesse. Apesar de sua recorrência, sua função varia. No primeiro caso, refere-se a uma análise restrita, indicando que a atividade de tratamento de dados não deve ser proibida por lei ou norma infralegal. Já no segundo caso, o termo é usado para avaliar se um interesse atende às condições estabelecidas no Art. 10 para ser considerado legítimo. É importante considerar essa distinção de escopo e alcance do termo.

Nesse ínterim, deve ser conduzida uma avaliação para confirmar a compatibilidade do interesse legítimo do controlador ou de terceiros com as consequências para o titular dos dados. Caso as consequências predominem para o titular, o interesse legítimo do controlador não será prioritário. Isso ocorre porque as normas de proteção de dados visam proteger o titular dos dados enquanto regulam as atividades dos demais agentes envolvidos na relação, preservando, desse modo, um bem social (FERRETTI, 2014, p. 884-850).

Para preservar a integridade do legítimo interesse, uma ferramenta destinada a flexibilizar o sistema rígido, é crucial evitar sua aplicação generalizada em todos os casos de tratamento de dados. Caso contrário, sua ampla aplicabilidade poderia suplantar as demais bases legais para o tratamento de dados, resultando em seu esvaziamento. Entretanto, não se deve deixar de invocar o legítimo interesse, mesmo que sua definição seja complicada devido à necessidade de avaliar seus impactos nos direitos e liberdades do titular (DIRETIVA, 95/46/CE, p. 5-9).

O legítimo interesse não deve ser a última opção nem a preferência do controlador dos dados, mas deve ser usado como base legal para o tratamento de dados de forma estrita e em conformidade com outras bases legais, considerando que todas têm a mesma importância hierárquica (DIRETIVA, 95/46/CE, p. 9-10).

Ainda, o interesse é o objetivo pelo qual o responsável pelo tratamento pode buscar ou o benefício resultante para o próprio responsável ou para terceiros, incluindo outras pessoas físicas ou jurídicas, ou até mesmo a sociedade como um todo. O Parecer 06/2014 lista vários exemplos de interesses legítimos para o

tratamento de dados pessoais, porém, esses exemplos devem ser analisados caso a caso em relação aos direitos e liberdades fundamentais do titular dos dados. Essa lista não é considerada exaustiva ou permanente, pois um interesse legítimo deve ser, na prática: (i) lícito; (ii) claro e específico; e (iii) representar um interesse real, não meramente especulativo (UNIÃO EUROPEIA, 2014, p. 40).

Além do interesse do controlador ou de terceiros, é imprescindível que esse interesse seja legítimo. Existem diversas naturezas de interesses que o controlador pode ter e, quanto mais clara e óbvia for a demonstração desse interesse, maior será a probabilidade de ser considerado legítimo (DIRETIVA, 95/46/CE, p. 36).

A legitimidade pode abranger uma ampla gama de interesses, desde que não seja contraditória com o restante do sistema jurídico ao qual o sujeito está sujeito. Portanto, os possíveis legítimos interesses do controlador são diversos, sendo mais desafiador comprovar que o caso específico é vantajoso também para o titular dos dados. Para caracterizar essa legitimidade, é importe que o objeto passe por um processo de validação e ganhe confiança (MAJCHER, 2018, p. 587).

Embora os discursos jurídicos muitas vezes associem a legitimidade à legalidade, é importante considerar a legitimidade em um sentido mais amplo, abrangendo tanto as definições sociais quanto morais. Por exemplo, a expectativa do titular dos dados sobre o uso de suas informações pelo controlador está diretamente ligada ao conceito de legitimidade social e pode justificar o tratamento dos dados pessoais (MAJCHER, 2018, p. 587-588).

No que tange ao controlador, o conceito é definido na legislação brasileira, no inciso VI do artigo 5º, como "pessoa natural ou jurídica de direito público ou privado, responsável pelas decisões relacionadas ao tratamento de dados pessoais" (BRASIL, 2018).

Ao contrário do RGPD, a legislação brasileira não fornece uma definição clara de quem seria considerado um terceiro, nem quando esse terceiro se enquadra na categoria de destinatário, tornando ainda mais desafiadora a interpretação do alcance da base legal do legítimo interesse de terceiros na LGPD. Portanto, é uma prioridade urgente da Autoridade Nacional de Proteção de Dados (ANPD) abordar essa questão. Exemplos de terceiros em uma relação de tratamento de dados pessoais incluem tanto pessoas físicas quanto jurídicas, bem como a sociedade em geral. É aconselhável distinguir essas diferentes categorias de terceiros, uma vez que apresentam diferentes riscos para os titulares dos dados, além de destacar que o uso

da base legal deve ser sempre contextual. Nesse sentido, cabe ao próprio controlador avaliar se o interesse desse terceiro é genuinamente legítimo (BIONI; KITAYAMA; RIELLI, 2021, p. 6)

Considerando que tanto a LGPD quanto a RGPD exigem a demonstração de proporcionalidade entre as categorias de "legítimo interesse" e os "direitos e liberdades fundamentais", é fundamental que a interpretação ampla da primeira categoria também seja aplicada nas considerações sobre a última (FERRETTI, 2014, p. 859-863). Ainda, o uso do termo "direitos e liberdades fundamentais" evidencia a amplitude que deve ser atribuída a esse conceito (BENNET, 2018, p. 33)

Teffé e Viola (2021, p. 146) concluem que o legítimo interesse pode ser a base mais apropriada em várias situações, sendo aplicável quando não for possível ou desejável conceder ao titular dos dados total controle, ou quando o controlador preferir evitar incomodá-lo com solicitações de consentimento para tratamentos que provavelmente seriam aceitos pelo titular. Portanto, desde que os requisitos legais para o interesse legítimo sejam cumpridos, o controlador poderia optar por utilizar o legítimo interesse em vez do consentimento.

Diante disso, no próximo tópico, será abordado como o legítimo interesse do controlador ou de terceiros influencia o tratamento dos dados sensíveis do titular, e como garantir que isso seja feito com responsabilidade e transparência, em conformidade com as regulamentações de proteção de dados.

4.2 O LEGÍTIMO INTERESSE E O TRATAMENTO DOS DADOS PESSOAIS SENSÍVEIS

A percepção da importância dos dados sensíveis surgiu da compreensão de que seu manuseio inadequado dos dados pode resultar em danos significativos ao titular. A avaliação objetiva da sensibilidade desses dados é desafiadora, sendo necessário considerar percepções subjetivas para identificá-los como sensíveis. (BENNET, 2018, p. 31-32).

O tratamento diferenciado de dados sensíveis respeita o princípio da isonomia, pois a discriminação é o dano inerente à noção de dado sensível. É importante considerar que dados que resultam em danos graves devem ser abordados de forma distinta daqueles que facilitam o fluxo de informações na Era do Big Data, mas com consequências menores para os titulares (BIONI, 2019, p. 85-86).

Primeiramente, cumpre destacar que os dados sensíveis são definidos como uma categoria de dados pessoais que apresentam uma tipologia distinta devido ao seu conteúdo, que proporciona uma vulnerabilidade especial, sujeita à discriminação (BIONI, 2018, p. 84). Conforme esse conceito, é mais relevante constatar a potencialidade discriminatória no tratamento de dados pessoais do que identificar a sua natureza própria ou conteúdo, como descrito no artigo 5º, II, LGPD (BRASIL, 2018).

Segundo Doneda (2005, 160-161), compreende que os dados sensíveis são considerados como certos tipos de informações que, se conhecidas e processadas, poderiam ser utilizadas potencialmente de forma discriminatória ou particularmente prejudicial.

Tais informações sensíveis, devido ao nível de intimidade nelas presentes, podem gerar inúmeros danos quando tratadas inadequadamente, ou seja, sem o consentimento do titular e sem observar as cautelas necessárias. Isso porque podem ser utilizadas para promover a intolerância, o preconceito ou a discriminação, violando direitos e garantias fundamentais dos titulares (MACHADO, 2018, p. 53).

O avanço tecnológico e os mecanismos cada vez mais ágeis para obtenção e coleta de informações tornam as violações de dados pessoais uma preocupação tanto no âmbito público quanto no privado. Um exemplo marcante disso foi o vazamento de dados do Facebook, onde informações foram utilizadas de forma irregular para influenciar campanhas eleitorais nos Estados Unidos. Esse incidente afetou milhares de usuários e evidenciou a capacidade de empresas de manipular eleitores através de propaganda eleitoral e disseminação de fake news. Esse escândalo serviu de alerta para a comunidade internacional (COÊLHO, 2019, p. 34-35).

Quando ocorrem essas intromissões indevidas na privacidade dos titulares, há uma violação a essas informações sensíveis, resultando em afronta a princípios como o da dignidade da pessoa humana, conforme explicado por Sarlet (2013, p. 20), extrai-se:

> [...] a dignidade, como qualidade intrínseca da pessoa humana, é irrenunciável e inalienável, constituindo elemento que qualifica o ser humano como tal e dele não se pode ser destacado, de tal sorte que não se pode cogitar na possibilidade de determinada pessoa ser titular de uma pretensão a que lhe seja concedida a dignidade. Esta, portanto, compreendida como qualidade integrante e, em princípio, irrenunciável da própria condição humana, pode (e deve) ser reconhecida, respeitada, promovida e protegida,

> não podendo, contudo (no sentido ora empregado) ser criada, concedida ou retirada (embora possa ser violada), já que existe – ou é reconhecida como tal – em cada ser humano como algo que lhe é inerente.

Diante disso, no artigo 5º, inciso II, a LGPD estabeleceu que dado pessoal sensível é toda informação que permite identificar 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 (BRASIL, 2018).

Nesse sentido, os dados pessoais sensíveis, por tratarem da intimidade do titular, exigem uma proteção judicial mais robusta. O vazamento ou uso indiscriminado desses dados pode causar graves problemas em diversas áreas da vida do indivíduo, comprometendo suas garantias e liberdades fundamentais. Portanto, o uso desses dados só será permitido com o consentimento específico e destacado do titular, ou quando a utilização for em benefício do próprio titular ou da sociedade, casos em que o consentimento pode ser dispensado, diferentemente do que ocorre com dados comuns (TEIXEIRA; GUERREIRO, 2022, p. 25). Nesse contexto, a LGPD dedicou um artigo específico aos procedimentos que devem ser seguidos:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiros;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9o desta Lei e exceto no caso

> de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
>
> § 1o Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
>
> § 2o Nos casos de aplicação do disposto nas alíneas a e b do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.
>
> § 3o A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
>
> § 4o É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto, nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5o deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
>
> I – a portabilidade de dados quando solicitada pelo titular; ou
>
> II – as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.
>
> § 5o É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários (BRASIL, 2018).

No entanto, cumpre destacar que a LGPD vedou o tratamento de dados sensíveis a partir da base de legitimação “legítimo interesse”, podendo justificar a vedação do processamento de informações pessoais com base no "legítimo interesse" tanto pela norma brasileira quanto pela lei geral europeia de proteção de dados pessoais, devido à preocupação das jurisdições com a possibilidade de danos ao titular decorrentes do tratamento de dados sensíveis (BENNET, 2018, p. 31-32).

Consta mencionar, que durante a pandemia de COVID-19, a sociedade utilizou dos dados pessoais sensíveis dos cidadãos. Esses dados foram valiosos na saúde pública, contribuindo para soluções em crises e para avanços em pesquisas científicas. No entanto, mesmo em situações excepcionais, deve-se agir com boa-fé, respeitando a privacidade dos titulares e cumprindo as leis, detalhando o processo de tratamento dos dados, sua duração e os propósitos da coleta (CANEDO, 2021, p. 6).

Fica evidente que, a avaliação da sensibilidade dos dados deve ser realizada individualmente, mesmo com as proteções estabelecidas por leis, devido à

facilidade de associar dados. Isso ocorre porque uma informação que inicialmente não é considerada sensível pode se tornar sensível ao ser combinada com outros materiais (BIONI, 2019, p. 85-86).

Segundo Doneda (2020, p. 144), acerca do tratamento dos dados sensíveis, dispõe:

> Um outro problema é que a mera proibição da coleta e tratamento de dados sensíveis – recurso utilizado em algumas das leis sobre a matéria – demonstra-se inviável, pois muitas vezes o uso de tais dados é legítimo e necessário; além do que existem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações deste gênero, como diversas entidades de pesquisa ou do setor de saúde, de caráter político, religioso ou filosófico.

Ainda, no entendimento de Doneda (2020, p. 145), a abordagem dos dados sensíveis varia conforme as leis de cada país. É essencial reconhecer que a distinção desses dados visa reduzir a possibilidade de discriminação, embora a discriminação possa ocorrer mesmo sem a utilização desses dados ou quando são usados para propósitos legítimos.

Para Pinheiro (2020, p. 210) expõe a preocupação com os cuidados que exigem para o tratamento dos dados pelos controladores:

> O tratamento de dados pessoais sensíveis, segundo a LGPD, demanda uma base legal específica e justificada, sendo o consentimento do titular a principal delas. (…) A complexidade e a relevância desses dados exigem que os controladores adotem medidas de segurança apropriadas e realizem avaliações de impacto à proteção de dados sempre que necessário.

Dessa forma, é indispensável que o controlador aja com diligência ao tratar os dados pessoais sob sua responsabilidade, seguindo os procedimentos corretos e partindo sempre pelo bom senso e pela boa-fé. Ademais, é evidente que uma regulamentação mais rigorosa dos dados pessoais, especialmente dos sensíveis, pelo Estado é fundamental para assegurar os direitos constitucionais de seus titulares, essenciais em um Estado Democrático de Direito (LIMA, 2021, p. 47-61).

Em suma, quando se discute o legítimo interesse e o tratamento de dados sensíveis, é como encontrar um equilíbrio delicado entre atender às necessidades legítimas de processar essas informações e proteger a privacidade e os direitos das pessoas. Embora o legítimo interesse possa justificar certos tipos de processamento de dados, especialmente em cenários comerciais, é crucial garantir que isso seja feito com muita responsabilidade. Isso significa adotar medidas robustas de segurança para proteger os dados e sempre respeitar os direitos das pessoas sobre suas

informações pessoais. Para isso, as organizações precisam estabelecer políticas transparentes e procedimentos claros para garantir que estejam em conformidade com as leis e regulamentações de proteção de dados.

4.3 A OBRIGAÇÃO DOS AGENTES DE TRATAMENTO EM DETRIMENTO DO RELATÓRIO DE IMPACTO

O relatório de impacto à proteção de dados, identificado como um indicador de conformidade pela LGPD, é uma das ferramentas cujo manuseio adequado e eficiente é orientado por obrigações e conceitos presentes na legislação. Através de uma análise sistemática, é possível encontrar instruções sobre como utilizá-lo corretamente (GOMES, 2019, p. 2)

Embora os relatórios de impacto à proteção de dados sejam recentes como ferramenta prevista na legislação brasileira, é importante salientar que eles já faziam parte da legislação de proteção de dados da União Europeia há pelo menos vinte anos. A UE foi uma das principais influências na elaboração da LGPD, como visto anteriormente neste trabalho (GOMES, 2019, p. 2).

O regulamento europeu (RGPD) menciona situações em que a elaboração e manutenção do relatório de impacto são obrigatórias, bem como outras em que é possível solicitar esse documento ou em que a realização do relatório é incentivada (BENNETT, 2018, p. 18).

Com base nos critérios a serem apresentados no RIPD, os legisladores europeus foram ainda mais longe ao abordar as particularidades da ferramenta, incluindo de forma sistemática na legislação quais itens devem ser obrigatoriamente adotados. Assim, os interessados em adotar o RIPD no Brasil devem considerar utilizar como base o modelo europeu, que, de acordo com o disposto no art. 35, item 7 do Capítulo 4 da GDPR, determina a inclusão de, pelo menos, as seguintes informações:

> A avaliação deve conter pelo menos:
>
> uma descrição sistemática das operações de tratamento previstas e das finalidades do tratamento, incluindo, se for caso disso, o interesse legítimo prosseguido pelo responsável pelo tratamento;
>
> uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação às finalidades;

> uma avaliação dos riscos para os direitos e liberdades das pessoas (...); e as medidas previstas para enfrentar os riscos, incluindo salvaguardas, medidas de segurança e mecanismos para garantir a proteção dos dados pessoais e para demonstrar o cumprimento do presente regulamento tendo em conta os direitos e interesses legítimos dos titulares dos dados e outras pessoas interessadas. (GDPR-INFO, 2018 - tradução livre)

Em suma, a abordagem regulatória europeia em relação ao relatório de impacto está fortemente ligada à ideia de gerenciamento de riscos, que envolve a identificação, mitigação e, principalmente, prevenção de possíveis danos aos titulares. (GOMES, 2019, p 3).

A legislação brasileira e a normativa europeia possuem semelhanças em alguns aspectos, pois ambas implementaram o teste de proporcionalidade para evidenciar que os interesses legítimos do controlador ou de terceiros têm prioridade sobre as consequências para o titular (BIONI, 2019, p. 252-253).

A ANPD poderá solicitar o referido relatório em qualquer momento quando o tratamento tiver como base o legítimo interesse, conforme fundamentado no art. Art, 10, §3º da LGPD (BRASIL, 2018).

É necessário comprovar, segundo o teste, que os benefícios provenientes do tratamento dos dados, juntamente com o legítimo interesse, superam os impactos sobre o titular dos dados. A avaliação dos direitos e liberdades do titular, mencionada pela lei, interage diretamente com conceitos constitucionais amplos, ultrapassando a simples análise de riscos (BENNETT, 2018, p. 33).

No Brasil, a definição do que constitui o relatório de impacto à proteção de dados está estabelecida no artigo 5º, XVII da LGPD (2018):

> (...) documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. (BRASIL, 2018)

Nesse contexto, é essencial identificar o sujeito responsável pelo RIPD, que é o controlador, definido no inciso VI do artigo 5º da LGPD sendo “a pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões relacionadas ao tratamento de dados pessoais” (BRASIL, 2018). O teste serve como uma salvaguarda para o controlador, evitando que a base legal do legítimo interesse seja enfraquecida.

Antes de iniciar o tratamento, o responsável pelo tratamento deve conduzir a avaliação de impacto. Se houver um conjunto de operações de tratamento com

riscos elevados semelhantes, é viável realizar uma única análise, visando economia procedimental (PINHEIRO, p. 709).

Cumpre destacar que o art. 38, parágrafo único da LGPD, dispõe as regras que o RIPD deverá seguir, contendo os passos a serem seguidos, conforme extrai-se da Lei:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (BRASIL, 2018).

Embora a elaboração do relatório de impacto à proteção de dados pessoais pelos controladores não seja obrigatória para todos os tipos de tratamentos de dados, sua utilização em diversos processos trará uma mudança cultural e contribuirá para demonstrar a conformidade das organizações com a LGPD (BORELLI et al., 2020, p.182).

Ainda, de acordo com o estipulado no art. 38 da LGPD, acima indicado, para a elaboração de um RIPD para aqueles que tratam dados, o portal Gov.Br, na página dedicada à Autoridade Nacional de Proteção de Dados (ANPD), conforme sua agenda regulatória para o biênio 2023/2024, definiu por meio de seu site, na seção de perguntas e respostas sobre o RIPD, no item 6, os requisitos mínimos que devem ser incluídos no RIPD:

> Conforme o art. 38 da LGPD, o RIPD deverá conter, pelo menos:
>
> a) a descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma;
>
> b) a metodologia usada para o tratamento e para a garantia da segurança das informações; e
>
> c) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados (GOV.BR - ANPD, 2023).

Ao abordar as etapas de elaboração do relatório de impacto, Braz Junior (2019, p.1) enfatiza que o propósito não consiste em erradicar todos os riscos, mas sim em minimizá-los e determinar se os riscos remanescentes são justificados. Na

visão do autor, o documento não apenas serve como prestação de contas mencionado no art. 6, X, pelos agentes de tratamento, mas também trazendo benefícios ao negócio ao permitir a revisão de processos internos.

Segundo o autor, destaca três etapas que considera essenciais para a elaboração do RIPD: a primeira consiste no entendimento da organização e dos processos envolvidos, por meio do mapeamento de dados, uma etapa crucial para qualquer programa de conformidade com a LGPD, pois engloba a consolidação de todas as informações relacionadas ao mapeamento dos processos, subprocessos e atividades realizadas pela organização; as outras duas etapas incluem a avaliação e o gerenciamento de riscos (BRAZ JUNIOR, 2019, p. 1).

Conforme observado por Gomes (2019, p. 7-9) acerca do relatório de impacto que apesar de terem tantas etapas a serem apresentadas para mitigar os efeitos ao titular dos dados, vejamos:

> O relatório de impacto à proteção de dados não deve ser enxergado na LGPD como uma ferramenta burocrática, mas sim como uma documentação que reflete um processo de aprendizado por agentes de tratamento, que é o de realizar a governança de dados dentro de casa (GOMES, 2019, p. 9)

Acrescenta sobre a ideia do RIPD:

> (...) A ideia do relatório de impacto é refletir uma avaliação de impacto, cuja base regulatória é a identificação de riscos, que pode ser realizada para propósitos diferentes, como: avaliar o impacto de incidentes de segurança; avaliar o impacto de novas tecnologias; avaliar o impacto de novos produtos que podem gerar riscos aos direitos dos titulares de dados etc. (GOMES, 2019, p. 7).

Para se compreender a importância do RIPD na proteção dos dados pessoais, é válido destacar uma parte específica do relatório do Banco Central do Brasil (BCB, 2022, p.23), criado e disponibilizado pela própria instituição através de sua política de transparência. Esse relatório orienta as atividades relacionadas ao tratamento de dados e incentivou o estabelecimento, gerenciamento e aprimoramento de métodos para proteger tais dados, conforme evidenciado no Anexo I do documento.

> Anexo I – Gerenciamento dos Riscos à Proteção de Dados Pessoais
> (...)
>
> Metodologia de Gerenciamento dos Riscos à Proteção de Dados Pessoais
>
> (...)
>
> A metodologia desse processo de avaliação de risco, ferramenta

> fundamental para a gestão de riscos, traz como vantagens: facilitar o entendimento do negócio e suas vulnerabilidades; apontar atividades críticas com controles frágeis ou inexistentes; gerar maior qualidade nas informações de risco e trazer flexibilidade ao processo de avaliação. (BCB, 2022, p.23)

Ainda no relatório do Banco Central do Brasil, dispõe que a proteção desses dados deve seguir um padrão, que será avaliado com base nos dados da matriz de risco, no qual os gestores do processo devem avaliar a resposta adequada a cada risco identificado, buscando adequar a exposição ao risco a níveis aceitáveis, dentre as seguintes opções:

> a) mitigar o risco: planejar ações de resposta visando reduzir a ocorrência e/ou o impacto do risco, podendo ser, por exemplo, por meio da melhoria dos controles. As ações de mitigação podem envolver mais de uma unidade;
>
> b) aceitar a exposição ao risco: o risco residual está no nível aceitável ou o risco é conhecido e não haverá um tratamento devido a fatores como relação custo-benefício não favorável;
>
> c) transferir o risco a uma terceira parte: repasse total ou parcial do risco para outra unidade de negócio, órgão ou terceiro; e
>
> d) eliminar o risco: implica a decisão de eliminar a atividade geradora do risco. Esse tratamento pode ser entendido como um instrumento de gestão que permite identificar um processo ou uma atividade desnecessária, sendo fonte causadora de risco e, assim, deve ser descontinuado. (BCB, 2022, p.23).

Nesse contexto, é imprescindível a elaboração da avaliação de riscos como a RIPD, pois segundo a Fia Business School (2018, p.1) é essencial destacar que a adoção da gestão de riscos nas empresas vai além de simples obrigatoriedades legais. Não se trata apenas de melhorar o desenvolvimento das atividades, mas sim de transmitir aos consumidores a confiança de que os produtos e serviços oferecidos são de qualidade e seguros:

> A gestão de risco é o conjunto de atividades coordenadas que têm o objetivo de gerenciar e controlar uma organização em relação a potenciais ameaças, seja qual for a sua manifestação. Isso implica no planejamento e uso dos recursos humanos e materiais para minimizar os riscos ou, então, tratá-los. É uma estratégia que envolve um trabalho preventivo de se antecipar a possíveis situações e considerar a prática como parte dos processos da empresa.

Para Blum e Vainzof (2020, p. 38), destacam a importância do RIPD para organizações que lidam com os dados pessoais:

> O RIPD, conforme previsto na LGPD, é um instrumento essencial para as organizações que lidam com dados pessoais. Ele requer uma análise detalhada dos riscos que o tratamento de dados pode representar para a privacidade dos indivíduos, bem como a implementação de medidas para mitigar esses riscos. Além de ser uma obrigação legal, a elaboração do RIPD pode ser uma oportunidade para as organizações reavaliarem suas práticas de tratamento de dados e fortalecerem suas medidas de segurança e proteção da privacidade.

Dessa forma, pode-se concluir que o relatório de impacto à proteção de dados na LGPD surge da ideia de organizar sistematicamente as operações de tratamento de dados, com o objetivo de viabilizar a visualização dos processos internos e o tratamento dos dados existentes. Isso possibilita a prevenção e a mitigação de riscos, inclusive aqueles já identificados (GOMES, 2019, p. 4). Além de garantir a conformidade com a legislação, o relatório promove a transparência e a confiança dos titulares dos dados. Ao demonstrar um compromisso com a proteção da privacidade e a segurança dos dados, as empresas podem fortalecer sua reputação e se destacar como líderes responsáveis no mercado.

5 CONCLUSÃO

A presente pesquisa buscou abordar, de maneira abrangente e detalhada, a evolução e o estado atual da privacidade e proteção de dados pessoais na sociedade da informação, analisando o contexto específico da legislação brasileira e as implicações do legítimo interesse como base legal para o tratamento de dados. Utilizando uma metodologia teórica e dedutiva, a investigação desenvolveu-se a partir de uma revisão crítica da literatura, com o objetivo de compreender as transformações e desafios enfrentados nesse campo.

Inicialmente, abordou-se a privacidade e o impacto da internet na coleta de dados no contexto da sociedade da informação. A crescente digitalização e a onipresença da internet criaram novas oportunidades e desafios para a privacidade. A coleta constante de dados, facilitada pelas tecnologias digitais, tornou-se uma prática comum, muitas vezes sem o devido consentimento dos indivíduos, colocando em risco a privacidade e os direitos fundamentais dos cidadãos. Nesse cenário, o direito à privacidade surge como um aspecto essencial dos direitos da personalidade, garantindo a proteção contra invasões indevidas e o uso abusivo de informações pessoais. Nesse sentido, a sociedade de vigilância contemporânea, caracterizada pela monitorização constante e a coleta de dados em larga escala, reforça a necessidade de uma estrutura legal e eficaz para salvaguardar a privacidade dos indivíduos. Esse cenário é acentuado pelo uso de tecnologias como a inteligência artificial e *big data*, que permitem a análise e o cruzamento de grandes volumes de dados, aumentando ainda mais os riscos à privacidade.

Em relação ao desenvolvimento da legislação brasileira de proteção de dados, a análise comparativa com legislações estrangeiras evidenciou a influência de marcos regulatórios internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, na formulação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. A LGPD representa um marco significativo na proteção de dados no país, estabelecendo diretrizes claras para o tratamento de dados pessoais e impondo obrigações rigorosas aos agentes de tratamento. Portanto, a necessidade de bases legais para o tratamento de dados pessoais é um dos pilares da LGPD, destacando-se a importância de fundamentos como o consentimento, a execução de contratos, o cumprimento de obrigações legais e o legítimo interesse.

No que tange ao contexto do legítimo interesse no tratamento de dados pessoais, a pesquisa explorou como essa base legal pode ser utilizada de forma adequada e equilibrada. O legítimo interesse do controlador ou de terceiro, embora legítimo, deve ser cuidadosamente balanceado com os direitos e liberdades dos titulares dos dados, especialmente quando se trata de dados pessoais sensíveis. A LGPD exige que os agentes de tratamento conduzam avaliações rigorosas para garantir que o tratamento de dados com base no legítimo interesse não viole os direitos fundamentais dos indivíduos. Além disso, a obrigação de elaborar relatórios de impacto sobre a proteção de dados reforça a responsabilidade dos agentes de tratamento em demonstrar a conformidade com os princípios legais e éticos na utilização de dados pessoais. Esses relatórios de impacto devem considerar não apenas os riscos potenciais à privacidade, mas também as medidas de mitigação adotadas para proteger os dados, promovendo assim uma cultura de responsabilidade e transparência.

O desenvolvimento e a implementação de uma legislação como a LGPD, não é tarefa simples. Eles exigem uma mudança significativa nas práticas de governança e na cultura organizacional das empresas e instituições que lidam com dados pessoais. A adaptação a novas regulamentações implica não apenas mudanças nos processos internos, mas também a capacitação contínua de funcionários e a implementação de tecnologias de segurança adequadas. O papel da Autoridade Nacional de Proteção de Dados (ANPD) é crucial nesse processo, pois ela tem a responsabilidade de supervisionar, orientar e fiscalizar o cumprimento da LGPD, além de promover a conscientização sobre a importância da proteção de dados.

Ao concluir esta análise, é evidente que a proteção de dados pessoais na sociedade da informação é um campo dinâmico e complexo, exigindo uma abordagem que envolva legislação robusta, regulamentação eficaz e um compromisso contínuo com a privacidade e os direitos dos indivíduos. A evolução da legislação brasileira, representada pela LGPD, é um passo indispensável na proteção dos dados pessoais, alinhando-se a padrões internacionais e respondendo às necessidades específicas do contexto brasileiro. O reconhecimento do legítimo interesse como base legal, embora valioso, deve ser implementado com rigor e transparência para assegurar que os direitos dos titulares de dados sejam devidamente protegidos.

Por fim, a pesquisa destaca a necessidade de uma vigilância contínua e adaptativa das políticas de proteção de dados. As tecnologias e práticas de coleta e

uso de dados estão em constante evolução, exigindo que a legislação e as práticas de governança de dados sejam igualmente dinâmicas e flexíveis. A colaboração internacional, a troca de melhores práticas e a harmonização das normas de proteção de dados são essenciais para criar um ambiente digital global mais seguro e respeitoso dos direitos dos indivíduos. A proteção da privacidade e dos dados pessoais não é apenas uma questão de conformidade legal, mas uma questão de respeito aos direitos humanos e de promoção de uma sociedade mais justa e ética.

REFERÊNCIAS

ALBERS, M. A complexidade da proteção de dados. **Revista Brasileira de Direitos Fundamentais & Justiça**. Belo Horizonte. v. 10, n. 35, p. 19–45, 2016, p. 43. DOI: 10.30899/dfj.v10i35.93. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/93. Acesso em: 5 maio. 2024.

ARENDT, Hannah. **A condição humana**. Trad. Roberto Raposo. Rio de Janeiro: Forense Universitária, 2010, p. 77-85.

ARANHA, Estela, FERREIRA, Lucia Maria Teixeira. Artigo: **O direito fundamental à proteção de dados e a importância da proposta de alteração constitucional nº 17/2019.** Revista Estadão: Rio de Janeiro, 2020, p. 1.

BANCO CENTRAL DO BRASIL. **Relatório de Impacto à Proteção de Dados Pessoais**. BCB, 2022, p. 23. Disponível em: https://www.bcb.gov.br/content/acessoinformacao/lgpd_docs/relatorio_de_impacto_a_protecao_de_dados_pessoais.pdf. Acesso em: 5 maio 2024.

BENNETT, Colin; e RAAB, Charles D. Revisiting '**The Governance of Privacy':** Comtemporary Policy Instruments in Global Perspective. Versão revisada será publicada em "Regulation and Governance". 2018, p. 1-3,18, 5-6, 33, 31-32 e 33.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 3 rev., atual., ampl. Rio de Janeiro: Forense, 2021, p. 34, 91 e 107.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 Reimpr. Rio de Janeiro: Forense, 2019, p. 84, 85-86, 248 – 249, 252-253.

BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD:** quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021, p. 6.

BITTAR, Carlos Alberto. **Os direitos da personalidade.** 7a ed. Rio de Janeiro: Forense Universitária, 2008, p. 49, p. 7-8.

Blum, Renato Opice e Vainzof, Rony. **LGPD - Lei Geral de Proteção de Dados Pessoais: Manual de Implementação.** São Paulo: Editora Thomson Reuters, 2020, p. 38.

BORELLI, Alessandra et al. **Comentários ao GDPR:** regulamento geral de proteção de dados da união europeia. 2. ed. São Paulo: Thomson Reuters, 2020, p. 182.

BRASIL. Superior Tribunal de Justiça **- STJ. Resp nº 22.337/RS**. Rel. Ministro Ruy Rosado de Aguiar, DJ, Brasília, 20 mar. 1995, p.6119.

BRASIL. **Lei nº 9.296, de24 de julho de 1996.** Lei da Escuta Telefonica. Brasília, DF: Senado, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em 5 maio. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Senado, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 5 maio. 2024.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à informação. Brasília, DF: Senado, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 5 maio. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Senado, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 5 maio. 2024.

BRAZ JUNIOR, Marcilio. Das etapas de elaboração de um DPIA: propósito de um data protection impact assessment não é eliminar todos os riscos, mas minimizar a existência destes. **Revista Jota.** 2019. p. 1. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/das-etapas-de-elaboracao-de-um-dpia-27042019. Acesso em: 5 maio. 2024.

BUCHAIN, Luiz Carlos. **A Lei Geral de Proteção de Dados: noções gerais.** Revista dos Tribunais, vol. 1010, ano 108. São Paulo: Revista dos Tribunais, dezembro 2019, p. 209-229.

CASTELLS, Manuel. **A sociedade em rede**. Tradução Roneide Venâncio Majer. 8.ed.rev.ampl. São Paulo: Paz e Terra, 2005, p. 24-25.

CASTELLS, Manuel. **Redes de indignação e esperança: movimentos sociais na era da internet.** Tradução Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2017, p. 153.

COÊLHO, Amanda Carmen Bezerra. **A Lei Geral de Proteção de Dados Pessoais Brasileira Como Meio de Efetivação dos Direitos da Personalidade.** Orientador: Alfredo Rangel Ribeiro. 2019. 52 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) -Universidade Federal da Paraíba, João Pessoa, 2019, p. 34-35. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/14305/1/ACBC05052019.pdf. Acesso em: 29 abril. 2024.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. **Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais.** Revista Brasileira de Direito Civil em Perspectiva, Belém, v. 5, n. 2, p. 22-41, 2019. Disponível em: <https://bit.ly/3dSrV0T>. Acesso em: 28 mar. 2024.

COE- COUNCIL OF EUROPE. (CONSELHO EUROPEU). **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Full list. Treaty Office. Disponível em: https://www.echr.coe.int/Documents/Handbook_data_protection_Por.pdf Acesso em: 02 abril 2024.

DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos Monaco. Apresentação. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos. **LGPD na Saúde**. São Paulo: Revista dos Tribunais, 2020, p. 5.

DANTAS, Juliana de Oliveira Jota; COSTA, Eduardo Henrique. **A natureza jurídica do consentimento previsto na Lei Geral de Proteção de Dados**: ensaio à luz da teoria do fato jurídico. In: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo (Coord.). Direito Civil e tecnologia. Belo Horizonte: Fórum, 2020. p.69-89.

CANEDO, Fabiolla Labelle Ornelas. **Privacidade e ética na sociedade de dados:** uma reflexão filosófica sobre a Lei Geral de Proteção de Dados brasileira. 2021. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito da Pontifícia Universidade Católica de São Paulo, São Paulo, 2021. Disponível em https://repositorio.pucsp.br/jspui/handle/handle/24533. Acesso em: 02 abr. 2024.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: Teoria Geral do Direito Civil. 33a ed. São Paulo: Saraiva, 2016, p. 133-134.

DONEDA, Danilo. **Da privacidade à proteção de dados.** Rio de Janeiro, Editora Renovar, 2005, p. 160-161.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006, p. 56, 126-127.

DONEDA, Danilo; ALMEIDA; Virgílio. **O que é Governança de Algoritmos?** 1.ed. São Paulo: Boitempo, 2018, p. 141-148.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. Rio de Janeiro: Revista dos Tribunais, 2020, p. 140, 161, 144-145, 192, 194, 272.

EUROPA. **Directiva 95/46/CE do parlamento europeu e do conselho.** Luxemburgo: 1995, p. 2. Disponível em: https://www.conjur.com.br/dl/di/diretiva-europeia.pdf. Acesso em 09 abril 2024.

FERRETTI, Federico. **Data Protection and the Legitimate Interest of Data Controllers:** Much Ado About Nothing or the Winter of Rights? Common Market Law Review 51. United Kingdom. 2014. p. 844-850, 859-863.

FIA. BUSINESS SCHOOL. **O que é gestão de risco?** Fia, 2018, p. 1. Disponível em: https://fia.com.br/blog/o-que-e-gestao-de-risco/amp/. Acesso em: 5 maio 2024.

FOUCAULT, Michel. **A verdade e as formas jurídicas.** Rio de Janeiro. Ed. Nau. 1999, p. 88.

FOUCAULT, Michael. **A verdade e as Formas Jurídicas**. Rio de Janeiro. Ed. Nau. 2005, p.8-10.

FORNASIER, Mateus de Oliveira; LIMA, Luciano. A internet e as novas tecnologias de informação e comunicação versus privacidade: o olhar jurisprudencial. **Revista Paradigma**, Ribeirão Preto, n. 24, p. 2-16, 2015. Disponível em: http://www9.unaerp.br/revistas/index.php/paradigma/article/view/495/519. Acesso em 28 mar. 2024.

FRAZÃO, Ana. Decisões algorítmicas e direito à explicação. **Revista Jota**. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/decisoes-algoritmicas-e-direito-a-explicacao-24112021. Acesso em 28 mar. 2024.

FREIRE, J. R. B., DISSENHA, L. A. (2021). LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E AS COOPERATIVAS: IMPRESSÕES INICIAIS**. Revista Eletrônica Do Curso De Direito Da UFSM**, 16(1). Disponível em: https://doi.org/10.5902/1981369441636, Acesso em: 22 abr. 2024.

GDPR-INFO. **Art. 35 GDPR Data Protection Impact Assessment**. Gdpr-info, 2023. Disponível em: https://gdpr-info.eu/art-35-gdpr/. Acesso em: 5 maio. 2024.

GOMES, Maria C. O. **Relatório de impactos à proteção de dados:** uma breve análise da sua definição e papel na LGPD. Academia, 2019, p. 2, 7-9. Disponível em: https://www.academia.edu/41160034/Relat%C3%B3rio_de_Impacto_a_Prote%C3%A7%C3%A3o_de_Dados_Pessoais_uma_breve_an%C3%A1lise_da_sua_defini%C3%A7%C3%A3o_e_papel_na_LGPD. Acesso em: 5 maio 2024.

GUARDIA, Andrés Felipe T. S. **De surveillance a dataveillance:** enfoque a partir da noção jurídica de tratamento de dados. Revista dos tribunais online, São Paulo,v. 109, n. 1012, fev. 2020, p. 494.

HAN, Byung-Chul. **No enxame: perspectivas do digital.** Petrópolis: Vozes, 2018, p. 43, 60, 65-66.

HAN, Byung-Chul. **Sociedade da transparência.** Petrópolis: Vozes, 2017, p. 60.

LÉVY, Pierre. **Cibercultura**. 3ª ed. São Paulo: Editora 34, 1999, p. 29.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Editora Saraiva, 2011, p. 67-68, p. 59.

LEONARDI, Marcel. **Principais bases legais de tratamento de dados pessoais no setor privado.** In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). Caderno Especial: Lei Geral de Proteção de Dados (LGPD). São Paulo: Revista dos Tribunais, 2019, p. 71-85.

LIMBERGER, Têmis. **Informação em Rede:** uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, São Paulo: Editora Foco, 2019, p. 563.

LIMA, Caio César Carvalho. Capítulo II - Do Tratamento de Dados Pessoais. In: MALDONADO. Viviane Nóbrega; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados comentada. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 179-188.

LUGATI, L. N.; ALMEIDA, J. E. de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, [S. l.], v. 12, n. 02, p. 01–33, 2020, p. 2. DOI: 10.32361/2020120210597. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 22 abr. 2024.
MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos; PARANHOS, Mario Cosac Oliveira. **LGPD e GDPR:** uma Análise Comparativa entre as Legislações. São Paulo, 2018. Disponível em: http://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise- comparativa-entre-as-legislacoes. Acesso em: 29 abr. 2024.

MAJCHER, Klaudia. **E-Commerce in the EU:** Searching for Coherence of Data Protection and Competition Law in the Context of Geo-Blocking. 24 Colum. J. Eur. L. 2018. p. 587;

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet:** uma análise comparada do Regulamento Geral de Proteção de Dados europeu e do Projeto de Lei 5.276/2016. 2017. 86 f. Trabalho de Conclusão de Curso (Bacharelado em Direito). Universidade de Brasília, Brasília, 2017. Data da publicação: 8 jan. 2018. Disponível em: bdm.unb.br/handle/10483/18883. Acesso em 22 abril 2024.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 55-56.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados.** Revista de Direito do Consumidor, vol. 120. São Paulo: Ed. RT., 2018, p. 469-483.

MENDES, Laura Schertel. **A Lei Geral de Proteção de Dados Pessoais:** um modelo de aplicação em três níveis. Caderno Especial LGPD. São Paulo: Ed. RT, 2019, p. 39, 43-44.

MENDES, L. S., & FONSECA, G. C. S. da. **Proteção de Proteção de dados para além do consentimento:** tendências contemporâneas de materialização. REI – Revista Estudos Institucionais, 6(2), 2020, p. 507–533. Disponível em: https://doi.org/10.21783/rei.v6i2.521. Acesso em 22 abril 2024.

OECD- **Diretrizes da OCDE sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais**, OECD Publishing, Paris, 2002, p. 2, disponível em: https://doi.org/10.1787/9789264196391-en. Acesso em 09 abril 2024.

OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPD: Lei Geral de Proteção de Dados Pessoais.** 1.ed. São Paulo: Thomson Reuters Brasil, 2020, p. 50.

OLIVEIRA, Brenno Henrique De; GUERRA, Carolinne Cardoso. **O Impacto do Regulamento Geral de Proteção de Dados Pessoais da União Europeia no Brasil.** In: Governança e Direitos Fundamentais: revisitando o debate entre o público e o privado. 1ª ed. Porto: Universidade de Santiago de Compostela, 2020, p. 75-83.

PASQUALINI, Alexandre. **Hermenêutica e sistema jurídico**. Porto Alegre: Livraria do Advogado, 1999, p. 80-81.

PEIXOTO, Erick Lucena Campos; EHRHARDT JUNIOR, Marcos. **O direito à privacidade na sociedade de informação.** In: ENCONTRO DE PESQUISAS JURÍDICAS - ENPEJUD, 1, 2016, Maceió, Alagoas. 2016, p. 358.

PEREIRA, Caio Mário da Silva. **Instituições de direito civil:** volume I. Rio de Janeiro: Editora Forense, 2010, p. 206.

PIMENTEL, Alexandre Pinto; CARDOSO, Mateus Queiroz. **A regulamentação do direito ao esquecimento na Lei do Marco Civil da internet e a problemática da responsabilidade civil dos Provedores**. Revista da AJURIS, v. 42., 2015, p. 48.

PINHEIRO, Alexandre Sousa et al. **Comentário ao Regulamento Geral de Proteção de Dados.** Coimbra: Almedina, 2018, p. 709.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 2. ed. São Paulo: Saraiva, 2020, p. 40.

PINHEIRO, Patrícia Peck. **Direito Digital Aplicado 4.0.** 2ª ed., São Paulo: Saraiva, 2020, p. 210.

RECUERO, Raquel. **Redes sociais na internet.** Porto Alegre: Sulina, 2009, p. 116.

REIS, N. C. M. **Decisões automatizadas, revisão humana e direito à proteção de dados:** uma análise à luz da Lei Geral de Proteção de Dados Pessoais. Dissertação (Mestrado em Direito Constitucional) Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2021, p. 157.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Organização e seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 24-37, 41-47, 46-47, 23-24, 96 e 97-98.

RODOTÀ, Stefano. **Il diritto di avere.** Roma: Laterza, 2012, p. 320.

SALOMÃO, Mariana Silva. **Marco Civil da Internet:** Perspectivas de Aplicação e seus Desafios. 2016, p. 19. Artigo Científico. (Curso de Pós-Graduação). Escola da Magistratura do Estado do Rio de Janeiro.

Disponível em: https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2016/pdf/MarianaSilvaSalomao.pdf. Acesso em: 22 abr. 2024.

SARLET, Ingo Wolfgang. **As dimensões da dignidade da pessoa humana:** construindo uma compreensão jurídico-constitucional necessária e possível. In: SARLET, Ingo Wolfgang (Org.). Dimensões da Dignidade: Ensaios de Filosofia do Direito e Direito Constitucional. Porto Alegre, RS: Editora Livraria do Advogado, 2013, p. 20.

SARLET, Gabrielle Bezerra Sales. COSTA, Ana Paula Motta. **A perspectiva da proteção de Dados pessoais em face dos Direitos das crianças e Adolescentes no sistema Normativo brasileiro**. In: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio. Proteção de dados: temas controvertidos. São Paulo: Editora Foco, 2021, p. 305.

SILVA, Priscila; MANGETH, Ana Laura; CARNEIRO, Giovana. **Conceito e limites do interesse legítimo:** um estudo comparado. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). Caderno Especial: Lei Geral de Proteção de Dados (LGPD). São Paulo: Revista dos Tribunais, 2019, p. 87.

SCHREIBER, Anderson. **Direitos da Personalidade.** 2ª ed. São Paulo: Atlas. 2013, p. 135-136.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. 2ª ed. São Paulo: RT. 2005, p. 118-119.

TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica**. Rio de Janeiro, p. 1-38. 10 dez. 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em: 04 abr. 2024.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. **Tratamento de Dados Pessoais na LGPD:** estudo sobre as bases legais dos artigos 7º e 11. In: BIONI, Bruno Ricardo; DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; SARLET, Ingo Wolfgang (Org.). Tratado de Proteção de Dados. São Paulo: Forense, 2021. p. 146.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei Geral de proteção de Dados Pessoais.** Comentado artigo por artigo. 4 ed. São Paulo: Saraiva Jur, 2022. p. 25, 27, 31-32.

TEPEDINO, Gustavo. **Temas em Direito Civil.** 3ª ed. Rio de Janeiro: Renovar, 2004, p. 29.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. **Consentimento e proteção de dados pessoais na LGPD**. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019, p. 287-322.

UNIÃO EUROPEIA. **Grupo de Trabalho do art. 29 para proteção de dados.** Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE. 2014, p. 2, 36, 40, 5-9, 10, 33, 36, 37 e 40. Disponível em: https://www.uc.pt/protecao-de-dados/suporte/20140409_wp_217_partecer_2_2014_conceito_interesses_legitimos_resp_trat_diretiva_95. Acesso em 2 maio 2024.

ZUBOFF, Shoshana. **Big Other:** capitalismo de vigilância e perspectivas para uma civilização de informação. Tradução Heloísa Cardoso Mourão. 1.ed. São Paulo: Boitempo, 2018, p. 31 e 40.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na fronteira do poder. Rio de Janeiro: Intrínseca, 2020, p. 19, 22, 24, e 270.