Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP
Mestrado Profissional em Direito

Carina Magda de Souza Gimenez
Orientador: Prof.Dr. João Paulo Lordelo Guimarães Tavares

São Paulo
2025

Carina Magda de Souza Gimenez

DADOS PESSOAIS SENSÍVEIS:
Rol Exemplificativo ou Taxativo?
Uma Análise da Categoria Especial à Luz da LGPD.

Dissertação de Mestrado desenvolvida no Programa de Mestrado Profissional em Direito, sob a orientação do Professor Dr.João Paulo Lordelo Guimarães Tavares, para obtenção do Título de Mestre pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

São Paulo
2025

DADOS PESSOAIS SENSÍVEIS:
Rol Exemplificativo ou Taxativo?
Uma Análise da Categoria Especial à Luz da LGPD.

Dissertação de Mestrado desenvolvida no Programa de Mestrado Profissional em Direito, sob a orientação do Professor Dr.João Paulo Lordelo Guimarães Tavares, para obtenção do Título de Mestre pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

São Paulo, 10 de março de 2025.

Banca Examinadora

Prof.Dr.João Paulo Lordelo Guimarães Tavares
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – (IDP)
Orientador

Profª. Tainá Aguiar Junquilho
(Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – (IDP)
Examinadora

Prof. Rafael Augusto Ferreira Zanatta
Associação Data Privacy Brasil de Pesquisa – (Data Privacy Brasil
Examinador

Dedico à minha filha, Cecília, minha razão e a força das lutas que eu não desisti...

Seja forte e corajosa!

AGRADECIMENTOS

Agradeço a Deus por me guiar e proteger na escolha dos caminhos mais belos, éticos e grandiosos de conquistas e aprendizados até o momento.

À minha mãe, pela crença em mim e pelas orações sinceras que sempre senti, e sei que em muitos momentos choramos juntas, mesmo à distância.

Aos meus sogros, que incentivam cada passo meu com alegria, apoio e orgulho.

À Professora Tainá Junquilho, por me apoiar e incentivar de várias maneiras em diferentes momentos, sem perceber o quanto isso me beneficia.

Ao meu orientador, Professor João Paulo Lordelo, que exemplifica, em todos os sentidos, o significado de ser um orientador. Sua orientação, dedicação e generosidade no compartilhamento de saberes foram fundamentais para a minha caminhada acadêmica. Sou grata por sua presença em minha trajetória e levarei seus ensinamentos como fonte constante de inspiração.

Ao meu Examinador, Professor Rafael Zanatta, por sua cordialidade e, acima de tudo, por sua dedicação incansável à defesa do Direito à Privacidade, tornando-se uma referência imprescindível no Brasil. Sinto-me verdadeiramente honrada em tê-lo ao meu lado neste momento tão marcante da minha jornada.

À Eve Weck e Taty Botelho, por serem minhas parceiras incansáveis, com quem compartilhei tanto as dificuldades pessoais quanto acadêmicas. Por me segurarem firme quando minhas forças pareciam se esgotar e, juntas, me ajudaram a descobrir uma força interior que antes parecia inacessível.Hoje chamo de essa força, de amizade verdadeira, sem competições ou ressalvas.

Aos meus amigos, pelas valiosas trocas, ensinamentos e torcida sincera, e principalmente pela compreensão e apoio diante das minhas ausências ou preocupações excessivas, considerando o grande desafio que é o mestrado.

À minha gestora, Priscila, que depositou confiança em mim desde o início, fazendo-me recordar da minha importância no mundo e da bela trajetória que depende de mim, me lembrando inclusive, que sempre posso contar com seu apoio e torcida sincera e gestão.

Ao Fabinho, motorista do meu fretado, nunca esquecerei as vezes que me ligou às 4 da manhã para garantir que eu acordasse, consciente da minha intensa rotina de estudos e dedicação.

Aos meus colegas de trabalho e à minha maravilhosa equipe, que muitas vezes atuaram como minha banca examinadora. Eles me proporcionaram ensinamentos valiosos e me desafiaram, mas acima de tudo, estiveram dispostos a aprender comigo e me incentivaram a ir além todos os dias, por confiarem em mim.

“O problema da proteção de dados, mais do que uma questão individual, possui implicações sociais profundas, que vão desde questões atinentes ao gozo de direitos por coletividades até a viabilidade de modelos de negócios que podem ser intrinsicamente contraditórios com o efetivo controle dos próprios dados pessoais, e mesmo o balanço de poderes no sistema democrático.”

Danilo Doneda

RESUMO

Esta dissertação aborda a proteção de dados pessoais no Brasil, com um foco aprofundado na análise da categoria de dados sensíveis à luz da Lei Geral de Proteção de Dados Pessoais (LGPD). O principal problema de pesquisa reside na natureza do rol de dados sensíveis, questionando se deve ser tratado como taxativo, conforme previsto pela legislação, ou se, dada a constante evolução tecnológica e os riscos de discriminação, abuso e violação de direitos, esse rol deveria ser mais flexível, funcionando como um rol exemplificativo. A pesquisa utiliza a metodologia hipotético-dedutiva, com uma análise crítica e reflexiva das implicações dessa classificação para a privacidade dos indivíduos e para a proteção de seus direitos, especialmente em um contexto em que a coleta de dados pessoais se intensifica e as tecnologias evoluem rapidamente. Adicionalmente, a dissertação realiza uma comparação entre a abordagem brasileira e a do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, além de considerar a experiência de outros países com modelos de proteção mais expansivos. O objetivo é identificar semelhanças, diferenças e lições que possam ser aplicadas para o aprimoramento do sistema brasileiro de proteção de dados pessoais. Dividido em quatro capítulos, o estudo propõe uma reflexão sobre os desafios legais e éticos impostos pela revolução digital, sugerindo melhorias legislativas para garantir que a proteção de dados e a privacidade se tornem pilares indiscutíveis dos direitos humanos em um mundo cada vez mais interconectado. Essas constatações conduzem à reflexão de que o conceito de dados sensíveis, em sua forma atual, não se mostra adequado para enfrentar os desafios impostos pelas tecnologias emergentes e pelas dinâmicas sociais contemporâneas no Brasil. Esse entendimento reforça a necessidade de a LGPD tratar o rol de dados sensíveis como exemplificativo, permitindo maior flexibilidade para acomodar novas situações, garantindo a defesa ampla das pessoas naturais, conforme o princípio central da lei, que visa a proteção dos direitos fundamentais à privacidade e à autodeterminação informativa em um contexto de constante transformação digital.

Palavras-chave: privacidade, proteção de dados, dados pessoais, dados sensíveis, tecnologia, direitos humanos.

ABSTRACT

This dissertation addresses the protection of personal data in Brazil, with a focused analysis of the category of sensitive data in light of the General Data Protection Law (LGPD). The main research problem lies in the nature of the list of sensitive data, questioning whether it should be treated as exhaustive, as stipulated by the legislation, or if, given the constant technological evolution and the risks of discrimination, abuse, and rights violations, this list should be more flexible, functioning as an illustrative list. The research adopts a hypothetical-deductive methodology, with a critical and reflective analysis of the implications of this classification for individuals' privacy and the protection of their rights, especially in a context where personal data collection is intensifying and technologies are rapidly evolving. Additionally, the dissertation makes a comparison between the Brazilian approach and the European Union's General Data Protection Regulation (GDPR), while also considering the experiences of other countries with more expansive protection models. The goal is to identify similarities, differences, and lessons that could be applied to improve the Brazilian personal data protection system. Divided into four chapters, the study proposes a reflection on the legal and ethical challenges imposed by the digital revolution, suggesting legislative improvements to ensure that data protection and privacy become unquestionable pillars of human rights in an increasingly interconnected world. These findings lead to the reflection that the current concept of sensitive data is not adequate to address the challenges posed by emerging technologies and contemporary social dynamics in Brazil. This understanding reinforces the need for the LGPD to treat the list of sensitive data as illustrative, allowing for greater flexibility to accommodate new situations, ensuring the broad defense of natural persons, in accordance with the law's central principle, which aims to protect fundamental rights to privacy and informational self-determination in a context of ongoing digital transformation.

Keywords: privacy, data protection, personal data, sensitive data, technology, human rights.

LISTA DE ABREVIATURAS E SIGLAS

AI – sigla em inglês para Inteligência Artificial

ANPD - Autoridade Nacional de Proteção de Dados

CC – Código Civil

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

IDEC – Instituto de Defesa de Consumidores

GDPR - General Data Protection Regulation

LAI – Lei de Acesso à Informação

LCP – Lei de Cadastro Positivo

LGPD – Lei Geral de Proteção de Dados

MCI - Marco Civil da Internet

ML – Machine Learning

PbD - Privacy by design

RIPD - Relatório de Impacto à Proteção dos Dados Pessoais

ROPA - Record Of Processing Activities

STF – Supremo Tribunal Federal

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

ONU - Organização das Nações Unidas

SUMÁRIO

INTRODUÇÃO

A revolução digital tem transformado profundamente as dinâmicas sociais, políticas e econômicas, introduzindo novas possibilidades, mas também desafios inéditos, especialmente no que tange à proteção da privacidade e dos dados pessoais. Nas últimas décadas, a crescente interdependência tecnológica deu origem a um ecossistema vasto e complexo de informações pessoais, que são constantemente coletadas, processadas e compartilhadas a um ritmo acelerado. Esse cenário levanta a possibilidade de a pessoa natural exercer o direito de conhecer, controlar e, em determinados casos, interromper o fluxo de dados a ela relacionados, promovendo, assim, um espaço para a afirmação da *autodeterminação informativa,*[1]na sociedade da informação.[2]

O surgimento da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, promulgada em 2018, representa um marco importante no processo de regulação desse cenário. A LGPD tem como objetivo não apenas regular o tratamento de dados pessoais, mas também proteger a privacidade dos cidadãos brasileiros em um mundo cada vez mais digital. No entanto, dentro desse panorama regulatório, uma das demandas centrais ainda em debate refere-se à categoria de dados pessoais sensíveis. A lei estabelece uma lista específica de dados que são considerados sensíveis, tratando-os com maior rigor devido ao risco potencial de discriminação, abuso ou violação de direitos.

Firmadas essas premissas, o presente trabalho tem por objetivo responder ao seguinte problema de pesquisa: A categoria de dados pessoais sensíveis se trata de rol taxativo no tratamento de dados pessoais ou é possível que ao considerar a potencialidade discriminatória, ilícita ou abusiva aos titulares, este rol se torne apenas exemplificativo, permitindo ampliação e proteção aos dados pessoais "comuns", permitindo a inclusão de outros tipos de dados pessoais, desde que estes apresentem risco significativo para os direitos dos indivíduos?

O problema de pesquisa que orienta esta dissertação visa justamente investigar essa questão, questionando se a atual definição de dados sensíveis na LGPD, ao adotar um rol taxativo, está efetivamente proporcionando a proteção adequada aos indivíduos, ou se seria necessário um enfoque mais dinâmico e flexível, que permita a ampliação da proteção a outros dados pessoais não classificados como sensíveis, em virtude de seu potencial discriminatório, ilícito ou abusivo. Em um mundo onde o tratamento de dados se intensifica e se diversifica, a linha entre dados

[1] MENDES,Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Pensar, Fortaleza, v.25,n.4,p.1-18,out./dez.2020.
[22] CASTELLS, Manuel. A Sociedade em Rede.21ª ed. Paz & Terra:2013 Fim de milênio – A Era da Informação (vol.3).1ª ed. Paz e Terra:2020.

pessoais comuns e dados sensíveis nem sempre é clara, o que exige uma análise crítica da legislação e da eficácia da sua aplicação.

A metodologia adotada para abordar essa problemática será a hipotético-dedutivo, em que se partirá de uma análise teórica e legal do conceito de dados sensíveis à luz da LGPD, considerando tanto os fundamentos jurídicos da proteção de dados quanto as implicações práticas para os titulares desses dados. A pesquisa também se utilizará de uma análise comparativa entre a legislação brasileira e a legislação internacional, especialmente o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a fim de compreender as diferentes abordagens adotadas em outras jurisdições e suas implicações para o Brasil.

Para alcançar uma compreensão profunda da questão, a dissertação será dividida em quatro capítulos principais, que desenvolverão os seguintes pontos:

Capítulo 1 - Neste primeiro capítulo, o objetivo é explorar a evolução do conceito de privacidade até a proteção de dados pessoais, destacando como os avanços tecnológicos e a sociedade da informação impactaram esses direitos. O capítulo começa com a definição do que é privacidade e como ela tem sido historicamente entendida. Em seguida, será analisada a relação íntima entre a privacidade e a proteção de dados pessoais, considerando como o tratamento de dados passou a ser visto como uma extensão da privacidade no mundo digital. Também são apresentadas as primeiras iniciativas voltadas para a proteção de dados pessoais, com foco nas ações legislativas e regulatórias da União Europeia, que foi pioneira nesse campo. O capítulo fornecerá o contexto necessário para compreender a relevância da proteção de dados pessoais na sociedade contemporânea.

Capítulo 2 - Este capítulo se dedica a analisar como a proteção de dados pessoais é abordada no direito brasileiro, com um foco especial na Lei Geral de Proteção de Dados (LGPD). O capítulo começa explicando o conceito de dados pessoais sensíveis, uma categoria especial de dados que exige uma proteção ainda maior, e como essa categoria é tratada pela LGPD. Também serão discutidos os aspectos jurídicos e sociais da classificação de dados pessoais sensíveis, incluindo os desafios relacionados à coleta, processamento e armazenamento dessas informações. Além disso, o capítulo aborda um debate relevante no Brasil sobre a definição do rol de dados pessoais sensíveis: seria ele exemplificativo ou taxativo? A análise desse ponto é crucial para entender as implicações jurídicas e as possíveis limitações ou avanços na proteção dos direitos fundamentais dos indivíduos, que é o problema central desta pesquisa.

Capítulo 3 - O terceiro capítulo realiza uma análise comparativa entre as principais

abordagens legais de proteção de dados pessoais, com destaque para o GDPR da União Europeia e a LGPD do Brasil. O objetivo é comparar como essas duas legislações tratam a questão da proteção de dados sensíveis, apontando semelhanças, diferenças e a evolução normativa de cada uma. Em seguida, o capítulo explora as abordagens de outros países, incluindo os Estados Unidos, que adotam uma regulamentação setorial fragmentada. Será analisado também o impacto dessa fragmentação na proteção dos dados pessoais nos Estados Unidos. Por fim, o capítulo discute os desafios globais que envolvem a proteção de dados pessoais e as oportunidades de aprimoramento das legislações em diferentes países, sempre tendo em vista a evolução das tecnologias e a crescente troca de dados no ambiente internacional.

Capítulo 4 - Este capítulo aborda as implicações práticas da aplicação das normas de proteção de dados pessoais sensíveis, com base em situações concretas e exemplos de como a interpretação desses dados afeta os direitos dos indivíduos. Primeiramente, serão apresentados casos práticos nos quais dados comuns podem, em determinadas circunstâncias, representar riscos significativos aos direitos dos indivíduos, mostrando que a sensibilidade de um dado pode não estar apenas em sua natureza, mas no contexto em que é tratado. O capítulo também propõe uma análise da proteção de dados à luz do princípio da dignidade da pessoa humana, fornecendo uma base ética para a proteção de dados pessoais sensíveis. Além disso, são discutidos os desafios enfrentados por empresas e profissionais da área de proteção de dados, que precisam equilibrar o cumprimento das normas com as necessidades de seus negócios.

As **considerações finais**, retoma os pontos principais abordados ao longo do trabalho, refletindo sobre os desafios e avanços na proteção de dados pessoais e dados sensíveis, tanto no Brasil quanto em nível global. A conclusão sintetiza as contribuições do estudo para a compreensão da legislação vigente, seus impactos na sociedade e o papel da proteção de dados no contexto atual. Além disso, são apresentadas sugestões para futuras pesquisas e ações, tanto do ponto de vista jurídico quanto prático, para fortalecer a proteção dos direitos fundamentais à privacidade e à proteção de dados pessoais em um cenário de constante evolução tecnológica e digital.

A proteção eficaz dos dados pessoais é um dos maiores desafios enfrentados pela sociedade atual, na era digital. O avanço das tecnologias e a intensificação das práticas de coleta e processamento de informações têm colocado em “xeque” a capacidade da LGPD de garantir a segurança e a privacidade dos cidadãos, sem comprometer a segurança jurídica e a confiança nas instituições.

O problema de pesquisa proposto, portanto, se insere em um contexto mais amplo, que exige

uma reflexão cuidadosa sobre a forma mais eficaz de proteger os dados pessoais, garantindo que o sistema jurídico brasileiro esteja alinhado às necessidades da sociedade digital atual, sem comprometer a segurança jurídica e a confiança dos cidadãos. Este trabalho parte da premissa de que é necessário repensar os mecanismos de proteção atualmente previstos na LGPD, oferecendo uma análise crítica sobre seu alcance e sua eficácia. Busca-se, assim, apresentar propostas que fortaleçam o sistema jurídico brasileiro diante das demandas contemporâneas da sociedade digital, garantindo uma proteção mais robusta e adaptada à realidade tecnológica em constante transformação.

1. DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS

1.1. O QUE É PRIVACIDADE?

A palavra "privacidade" tem sua origem no latim "*privatus*", que significa algo que pertence a si próprio, que está separado do coletivo ou grupo. É um particípio passado de *"privare",* que quer dizer retirar ou separar, originando-se de *"privus"* que significa individual ou próprio.[3] A etimologia da palavra revela que, apesar das interrupções naquilo que é privado, devido à rapidez com que nossas informações são espalhadas, podemos concordar que seu significado não se perderá com o tempo, mas se encontra defasado.

Vivemos em um momento em que há um descompasso notável entre o significado semântico de certos conceitos e suas representações no mundo real. Esse fenômeno, por si só, nos leva a uma reflexão: como chegamos a esse ponto? Como a noção de privacidade, que antes se restringia a uma esfera mais pessoal e intangível, foi transformada ao longo do tempo, absorvendo novas dimensões e interações com outros aspectos da sociedade, até culminar no que hoje conhecemos como proteção de dados pessoais?

A análise dessa possível discrepância, que se desenrola entre o que entendemos por privacidade e o que ela realmente representa no contexto atual, surge como um ponto concludente para compreendermos não apenas sua evolução histórica, mas também para questionarmos as implicações dessa transformação em nossa vida cotidiana. Estamos realmente preparados para lidar com a complexidade dessa mudança, ou estamos apenas reagindo a um processo que já foge ao nosso controle?

Embora o "direito à privacidade" (*right to privacy*)[4] tenha se desenvolvido originalmente na jurisprudência e doutrina norte-americana, em seus primórdios marcados por um individualismo exacerbado e até mesmo egoísta, portava a feição do direito a ser deixado só[5] (DONEDA,2021). Mesmo na atualidade, com a privacidade reconhecida como um direito fundamental, vestígios do contexto individualista de sua origem ainda são perceptíveis. Talvez isso seja inevitável, dada a sua capacidade intrínseca de destacar as individualidades nas relações sociais.

É sensato lembrar que a privacidade já foi considerada um direito tipicamente burguês[6], na

[3]Origem da Palavra: Disponível em: https://origemdapalavra.com.br/palavras/privado/ Acesso em: 18 set. 2024.
[4] WARREN, Samuel; BRANDEIS, Louis. "The Right to Privacy". In: Harvard Law Review, v. 4, p. 193, 1890.
[5] COOLEY, Thomas McIntyre. *Treatise on the Law of Torts.* 1888. Citação do conceito *"right to be alone"*.
[6] André Vitalis sublinha alguns caracteres do direito à privacidade que denotariam sua conotação elitista, sugerindo

chamada “idade de ouro da privacidade”[7], onde se enxergava o direito à privacidade como um direito de alguns, sugerindo que a função do instituto seria a proteção da propriedade de poucos. Em 1995, o Autor André Vitallis[8], não mencionou especificamente a privacidade como sendo elitista, no entanto, ele abordou questões relacionadas à privacidade intitulado *“Informatique, pouvoir et libertés*”[9] (Informática, Poder e Liberdades), trabalho de sua autoria que contribuiu significativamente para a compreensão dos desafios relacionados à privacidade, à informatização e à regulação na era da informação.

A partir das reflexões propostas por Hesse[10], diversas legislações nacionais começaram a emergir na Europa durante a década de 1970. Destacam-se, nesse contexto, a Lei Sueca de Proteção de Dados (*Datalagen*),[11] a Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada *Informatique et Libertés*,[12] e outras normas similares adotadas em países como Espanha e Alemanha, entre outros.

Na Constituição Federal do Brasil[13] a privacidade foi reconhecida como um direito fundamental. No entanto, sua interpretação inicial estava focada na proteção da intimidade do indivíduo, abrangendo aspectos como o sigilo das correspondências, a inviolabilidade do domicílio e a proteção contra abusos de autoridade. Esse entendimento, consagrado nas primeiras versões da Constituição, refletia uma visão mais restrita da privacidade, voltada para a proteção da vida pessoal e da liberdade individual contra intervenções externas indevidas.

De acordo com Danilo Doneda, há uma proliferação de termos distintos no campo doutrinário utilizados para se referir à privacidade, como "vida privada", "intimidade", "segredo", "sigilo", "recato", "reserva", entre outros relacionados à intimidade da vida privada.[14] Tal multiplicidade terminológica pode acarretar insegurança jurídica, embora o Tribunal Europeu dos Direitos Humanos não considere viável nem necessário buscar uma definição exaustiva para o

---

que a função do instituto seria a proteção da propriedade de alguns poucos: “Cependant plus qui tout autre, le droit à l avie privée est resé de par les conditions materielles minimales qu’il implique (conditions d’habitat, séparation lieu de travail,lieu de résidence...)le privilège d’une classe minoritaire. Ceci d’auntant plus qui la Protection de I’intimité s’inspire directement des techniques visant à delimiter um droit de propriété ‘exclusif”’. André Vitalis.Informatique, pouvoie et libertés. Paris:Economia, 1988, p.148.

[7] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. 3. ed. São Paulo: Revista dos Tribunais, 2021. p. 31.

[8]VITALIS, André. Présentation d'André Vitalis sur le site du Laboratoire MICA. Disponível em: https://fr.wikipedia.org/wiki/Andr%C3%A9_Vitalis.Acesso em: 18 set. 2024.

[9] VITALIS, André; ELLUL, Jacques. Ciência Política. Publicado em 1981.

[10] A Lei de Proteção de Dados do Land alemão de Hesse foi promulgada em 30 de setembro de 1970. *The Hesse Data Protection Act.*

[11] Datalag 1973:289, de 11 de maio de 1973.

[12] Lei 78-17, de 6 de janeiro de 1978.

[13]BRASIL. Constituição da República Federativa do Brasil de 1988. Art. 5º, inciso X. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 set. 2024.

[14] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. 3. ed. São Paulo: Revista dos Tribunais, 2006. p. 101.

conceito de vida privada.[15]

Marcel Leonardi apresenta uma síntese de diversas doutrinas sobre o assunto[16], sendo pertinente destacar algumas delas: “direito de o indivíduo ser deixado em paz para viver sua própria vida com um grau mínimo de interferência”;[17] “o direito de subtrair-se à publicidade para recolher-se na própria reserva”;[18] e “espaço íntimo intransponível por intromissões ilícitas externas”[19].

No contexto da proteção de dados pessoais, merecem ressaltar os seguintes entendimentos acerca da intimidade, conforme a compilação anteriormente mencionada: Milton Fernandes, ao afirmar que seria:

> O direito de excluir razoavelmente da informação alheia, fatos e dados pertinentes ao sujeito. Este poder jurídico atribuído à pessoa consiste, em síntese, em opor-se à divulgação de sua vida privada e a uma investigação nesta. A este poder corresponde o dever de todas as outras pessoas de não divulgar a intimidade alheia e de não imiscuir nela. E é neste poder que está o conteúdo do que seja intimidade.[20]

O conceito de privacidade é multifacetado e abrange uma série de necessidades fundamentais, como a busca pela igualdade, a liberdade de escolha e o desejo de não ser discriminado. Trata-se de um direito profundamente ligado à personalidade e ao desenvolvimento individual, funcionando como um eixo central em uma rede de relações complexas, cujos contornos ainda não são totalmente compreendidos, tanto pelo direito quanto pelas ciências sociais. Embora a privacidade não seja um conceito recente, sua abordagem concreta no ordenamento jurídico só ocorreu no final do século XIX, dando início a um processo de transformação que a levou às formas que conhecemos hoje.

No entanto, ao refletirmos sobre o papel da privacidade na sociedade contemporânea, surge uma questão importante: até que ponto a proteção da privacidade se traduz, de fato, em proteção dos dados pessoais? As conexões e diferenças entre esses dois conceitos – privacidade e proteção

---

[15] Tribunal Europeu de Direitos Humanos da União Europeia, Niemietz v.Alemanha, 72/1991/324/396, seção29,j.16.12.1992.
[16] LEONARDI, Marcel. *Tutela e Privacidade na internet*. São Paulo: Saraiva, 2012. p.56-61.
[17] Definição proposta pelos participantes da Conferência Nórdica sobre Privacidade, ocorrida em maio de 1967, reproduzida em justice, Privacy and the law. London: Stevens and Sons, 1970, Appendix B.
[18] CUPIS, Adriano de. *Os direitos da personalidade.*Trad. Adriano Vera Jardim e Antonio Miguel Caeiro. Lisboa: Morais, 1961.p.15.
[19] MORAES, Alexandre de. *Direitos Humanos Fundamentais:* Teoria Geral, comentários aos arts.1º e 5º da Constituição Federativa do Brasil.8. ed. São Paulo: Atlas, 2007. p. 128
[20] FERNANDES, Milton. *Proteção civil da intimidade.* São Paulo:Saraiva,1977. p.99.

de dados pessoais – não são apenas quesitos jurídicas ou teóricas, mas impactam diretamente a forma como nos relacionamos com as tecnologias e com o próprio Estado.

É nesse contexto de transição e de questionamento contínuo que se insere o desafio de compreender a relação entre privacidade e proteção de dados pessoais. Este tema, que se configura como uma interseção entre o direito, a ética e a tecnologia, será explorado no próximo tópico, onde analisaremos de forma mais aprofundada como esses conceitos têm se transformado e se conectado no cenário atual.

1.1.1. A Tecnologia e Sociedade: Impactos à Privacidade na Sociedade da Informação

> "Toda beleza e eficiência dos recursos tecnológicos e das possibilidades de interação travam uma batalha fervorosa com a privacidade, lembrando que esta já possui garantia constitucional." *(PINHEIRO, 2019).*

A tecnologia resulta da ciência e da engenharia, envolvendo um conjunto de ferramentas, métodos e técnicas criadas para resolver problemas. Ela simboliza a aplicação prática do conhecimento científico em diversas áreas de pesquisa. A etimologia da palavra tecnologia origina-se do grego "*tekhne*", que significa "técnica, arte, ofício", e do sufixo "logia", que significa estudo de algo.

As tecnologias primitivas ou tradicionais incluem a descoberta do fogo, a invenção da quando os povos primitivos começaram a transformar pedras em lâminas para cortar a madeira e caçar animais, eles já estavam conseguindo realizar avanços tecnológicos. As tecnologias medievais abrangem inovações como a prensa móvel, tecnologias militares com o desenvolvimento de armamentos e as tecnologias das grandes navegações que possibilitaram a expansão marítima. As inovações tecnológicas da Revolução Industrial, no século XVIII, causaram transformações significativas no processo de produção. No século XX, sobressaem-se as tecnologias de informação e comunicação, com a evolução das telecomunicações, o uso de computadores, o desenvolvimento da internet e, ainda, as tecnologias avançadas, que incluem o uso da Energia Nuclear, Nanotecnologia, Biotecnologia, entre outras.

Para Yuval Harari,

> Quando a revolução na biotecnologia se fundir com a revolução na tecnologia da informação, ela produzirá algoritmos de Big Data capazes de monitorar e compreender meus sentimentos muito melhor do que eu, a

> autoridade provavelmente passará dos humanos para os computadores. Minha ilusão de livre-arbítrio provavelmente vai se desintegrar à medida que eu me deparar, diariamente, com instituições, corporações e agências do governo que compreendem e manipulam o que era, até então, meu inacessível reino interior.[21]

Os avanços tecnológicos e a transformação digital têm um impacto significativo na sociedade, promovendo inovações que melhoram a qualidade de vida das pessoas em vários setores. No entanto, também trazem desafios sociais relevantes, por moldar destacadamente as relações sociais e econômicas, modificando a maneira como as informações são geradas, compartilhadas e processadas. No entanto, esse avanço tecnológico trouxe consigo uma série de desafios, principalmente no que tange à privacidade dos indivíduos.

A crescente digitalização da sociedade e a proliferação de dados pessoais têm gerado preocupações sobre o impacto dessas inovações na proteção da privacidade, que, por sua vez, é um direito fundamental previsto nas constituições de diversos países, incluindo o Brasil.

A chamada "Sociedade da Informação"[22] tem se caracterizado pela centralidade dos dados na economia global, com plataformas digitais coletando informações pessoais em uma escala nunca vista. Nesse cenário, a privacidade, enquanto direito fundamental, passa a ser constantemente ameaçada, sendo exposta a novos riscos, como o uso indevido de dados pessoais, a vigilância em massa e a manipulação digital.

A tecnologia impacta a privacidade de diversas formas, tanto no âmbito da coleta de dados quanto no uso de tecnologias de monitoramento. A proliferação de dispositivos conectados, como smartphones, câmeras de segurança e sistemas de rastreamento, ampliou a capacidade de vigilância das empresas e dos governos, criando um ambiente de vigilância constante. Esse fenômeno, denominado por Shoshana Zuboff[23] de "capitalismo de vigilância", tem gerado preocupações sobre a erosão da privacidade individual em favor da exploração comercial dos dados pessoais.

Há alguns anos, Scott MaxNally[24], executivo-chefe da *Sun Microsystems*, declarou abertamente: “Vocês não têm nenhuma privacidade, de qualquer modo. Aceitem isso”. Em 1988,

---

[21] HARARI, Noah Yuval.21 lições para o século 21. Israel: Spiegel & Grau, 2018, parte I.3.
[22] Byung-Chul Han, Sociedade da transparência, tradução de Enio Paulo Giachini (Petrópolis, RJ: Vozes, 2017), 120 p.
[23] ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.
[24] Who is Scott Mc Nealy? Disponível em: Scott McNealy - Wikipedia https://en.wikipedia.org/wiki/Scott_McNealy - Acesso em 19 de set. de 2024.

em um filme dirigido por Tony Scott, “Inimigo do Estado”[25], um dos personagens principais diz: “A única privacidade que você tem, está na sua cabeça. Talvez nem mesmo lá”.

As declarações públicas acerca da temática privacidade traduzem o cenário de incerteza da sociedade e remetem à reflexão da pergunta feita por Rodotá[26]: “O que podemos esperar do futuro? A tendência recente vai persistir, ou retornaremos ao conceito original de proteção de dados pessoais que iniciou uma nova era para a proteção das liberdades com uma abordagem realmente progressista?"

A questão proposta por Stefano Rodotá, acerca do futuro da proteção de dados pessoais e privacidade, na sociedade da informação, revisita um debate crucial sobre as direções que podem ser seguidas na regulação da privacidade e dos direitos individuais em uma sociedade digital que necessita ser encorajada à educar-se digitalmente, frente ao capitalismo de vigilância que se fortalece cada vez mais, caso contrário, poderemos testemunhar uma volta a uma abordagem menos progressista, focada mais no desenvolvimento econômico e na liberdade das empresas de utilizar os dados para fins comerciais, em detrimento das liberdades civis.[27]

Ao ganhar um novo impulso com o aumento da velocidade de seu desenvolvimento em diversas áreas, como a eletrônica, as telecomunicações, por exemplo, começaram a influenciar diretamente a sociedade, desde a filosofia de trabalho até os instrumentos de produção, bem como a distribuição do tempo e do espaço; elas também estão diretamente ligadas à essência dos instrumentos e mecanismos de controle que podem levar à erosão da privacidade ampliando fluxos de informação e, consequentemente, suas fontes e destinatários, passando os dados pessoais e a privacidade associar-se a diversos interesses, alterando significativamente seu perfil. Conforme observa Doneda, citando Rodotà: “O direito à privacidade já não se organiza mais pelo eixo 'pessoa-informação-segredo', seguindo o paradigma da *zero-relationship*, mas agora segue o eixo 'pessoa-informação-circulação-controle”[28].

As circunstâncias implicam na necessidade de compreender a nova estrutura de poder que está atrelada a essa nova arquitetura da informação. E juntamente com as mudanças no tecido social, determinou o contexto no qual a informação pessoal e a privacidade estão atualmente entrelaçadas; portanto, qualquer análise desses fenômenos deve considerar o aspecto técnico como

[25] Inimigo do Estado, dirigido por Tony Scott, 1988.
[26] RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 15.
[27] "Venda do olho: brasileiros permitem ter a íris escaneada em troca de dinheiro; valor chega até R$ 700". FDR. Disponível em: https://fdr.com.br/2025/01/18/venda-do-olho-brasileiros-permitem-ter-a-iris-escaneada-em-troca-de-dinheiro-valor-chega-ate-r-700/. Acesso em: 18 jan. 2025.
[28] DONEDA, Danilo. Direito à privacidade e proteção de dados pessoais. In: RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 15.

um dos elementos essenciais, sem perder de vista que o controle da informação sempre desempenhou um papel central na estruturação do poder em qualquer sociedade.

Embora a tecnologia possa parecer algo externo à natureza humana, é, na verdade, um produto da própria humanidade e de sua cultura, sendo projetada para interagir com ambas de maneira dinâmica e transformadora, os debates sobre direitos e privacidade têm se intensificado nos presentemente, principalmente em razão do uso crescente de tecnologias emergentes. Tais discussões surgem em um contexto onde a privacidade é constantemente desafiada pelo avanço tecnológico, que se caracteriza por sua imprevisibilidade e pelo fato de fazer parte de um universo vasto e complexo. Este universo abrange análises de impacto, projeções e testes, os quais, muitas vezes, se limitam a aproximações, uma vez que os efeitos da tecnologia são sentidos diretamente na sociedade, tornando-a vulnerável e perdendo sua autodeterminação afirmativa.

Para Ulrich[29], o risco na sociedade da informação apresenta características particulares: trata-se de um risco gerado intencionalmente pela ação humana, e a decisão de sua criação não se fundamenta diretamente em considerações éticas ou morais, mas em um mecanismo decisório fortemente influenciado pela tecnologia. Esse processo envolve um raciocínio matemático, utilizado para prever seus efeitos futuros de forma estática.

Quando devidamente analisados e processados, os dados pessoais se tornam uma fonte inesgotável e expansível, cujos resultados são fundamentais para inovações tecnológicas e de mercado, tratamento testado e comprovado, tanto que são chamados de “o novo petróleo” (*data is toe net oil)*[30]. Visão simplista e comparada com uma “mercadoria” que pode ser simplesmente extraída e comercializada sem impactos para a privacidade e os direitos dos indivíduos, razão pela qual, ao contrário do petróleo, não devem ser tratados apenas como um recurso a ser explorado sem a devida consideração dos impactos sociais, éticos, jurídicos e financeiros, afinal, se os dados são o novo petróleo, onde estão os royalties de cada titular de dados pessoais?[31].

A revolução digital que estamos testemunhando nas últimas décadas não se limita apenas à transformação de tecnologias, mas também à reconfiguração de toda a estrutura econômica global. A ascensão de uma nova economia, centrada no processamento e na circulação de dados, alterou

[29] BECK, Ulrich. La società globale del rischio. Trieste: Asterios, 2001, p. 13.
[30] THE ECONOMIST. The world’s most valuable resource is no longer oil, but data. The data economy demands a new approach to antitrust rules. 6 maio 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data . Acesso em: 29 set. 2024.
[31] Vianna, F. (2021). Se os Dados são o Novo Petróleo, Onde Estão os Royalties? O Neoliberalismo na Era do Capitalismo de Vigilância. Revista Gestão & Conexões, 10(3), 123–143. https://doi.org/10.47456/regec.2317-5087.2021.10.3.36014.128-147

profundamente a dinâmica de consumo, produção e interação entre indivíduos e organizações. Neste contexto, a coleta e o tratamento de dados pessoais tornaram-se os pilares dessa nova era, permitindo o surgimento de modelos de negócios baseados não mais apenas em produtos físicos, mas em fluxos de informações.

Manuel Castells, um dos mais proeminentes estudiosos, chancela esse fenômeno ao definir a economia digital como aquela interconectada por um "sistema nervoso eletrônico", em face da enorme quantidade de dados pessoais coletados e da capacidade computacional atual que não apenas possibilita, mas também acelera o processamento de dados, permitindo até a execução de ações automáticas e afetando vários setores econômicos[32].

A crescente centralidade dos dados na economia digital, associada à proliferação de tecnologias de monitoramento e vigilância, exige que a sociedade se reorganize para enfrentar os desafios impostos por esse novo paradigma. Não se trata apenas de uma questão técnica, mas de uma questão ética e política, que envolve a proteção da liberdade individual e a manutenção da autonomia do cidadão frente a sistemas que controlam, mas não garantem, sua privacidade. Este cenário exige uma reflexão mais profunda sobre os modelos regulatórios existentes e sobre a urgência de uma educação digital que empodere os indivíduos para compreender os riscos e os impactos do compartilhamento de suas informações pessoais.

A privacidade, como direito, deve ser constantemente defendida, e sua proteção deve ser uma prioridade tanto para os legisladores quanto para as empresas que lidam com dados pessoais. Sem um equilíbrio entre inovação tecnológica e proteção dos direitos individuais, a sociedade arrisca transformar suas próprias liberdades em mercadorias a serviço de interesses econômicos e comerciais.

A tecnologia, em sua essência, é uma ferramenta da humanidade, mas suas consequências no campo da privacidade exigem um olhar crítico e uma ação regulatória eficiente. O futuro da proteção de dados e da privacidade não pode ser encarado como uma inevitabilidade, mas como uma escolha que dependerá de nossas ações no presente. O que está em jogo não é apenas a proteção dos dados, mas a preservação da dignidade humana em um mundo cada vez mais digitalizado e interconectado.

[32] CASTELLS, Manuel. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Trad. Maria Luiza X. de A. Georges. Rio de Janeiro: Zahar, 2013. p. 11.

1.2. A Conexão Entre Privacidade e Proteção de Dados Pessoais

A relação entre privacidade e proteção de dados pessoais é clara: a privacidade visa garantir que as informações pessoais de um indivíduo sejam protegidas de abusos, sejam compartilhadas apenas com o seu consentimento ou em situações em que haja uma base legal (hipótese de tratamento de dados pessoais)[33] para o processamento, e sejam usadas de maneira ética e transparente. Nesse contexto, a proteção de dados pessoais serve como a principal ferramenta para assegurar a privacidade, pois, sem um controle rigoroso sobre a coleta, o uso e o armazenamento dessas informações, o direito à privacidade torna-se vulnerável.

Com o avanço das tecnologias, especialmente na sociedade da informação, o conceito de privacidade evoluiu para englobar o direito à proteção de dados pessoais como um direito fundamental e independente. Assim, direito à privacidade e direito à proteção de dados pessoais não são sinônimos, embora ambos tratem da segurança das informações de um indivíduo. A privacidade se refere à proteção contra intrusões externas, sendo uma liberdade negativa, ou seja, é a garantia de que o indivíduo pode se proteger de influências externas. Em contrapartida, o direito à proteção de dados pessoais é mais dinâmico, oferecendo uma liberdade positiva, permitindo ao indivíduo controlar suas próprias informações, mesmo em contextos públicos.

Para Bioni, o direito à privacidade não é idêntico ao direito à proteção de dados pessoais, pois existem várias liberdades individuais associadas ao direito à proteção de dados pessoais que não estão contempladas pelo direito à privacidade. Além disso, o "centro gravitacional[34] da proteção dos dados pessoais difere do direito à privacidade, ou seja, a percepção de que a sua tutela jurídica opera fora da dicotomia do público e do privado" (BIONI, 2019, p. 96-97).

A proteção de dados pessoais, sendo um desdobramento da privacidade, foi incorporada ao ordenamento jurídico brasileiro como um direito autônomo e também protegido pela Constituição Federal, através da Emenda Constitucional n.º 115, de 2022[35], que incluiu o artigo 5º, inciso LXXIX em um contexto de crescente digitalização e uso de tecnologias. Esse avanço se reflete não apenas nas regulamentações infraconstitucionais, mas também na própria Carta Magna, que reconhece a proteção da privacidade e dos dados pessoais como direitos constitucionais essenciais para garantir a dignidade da pessoa humana, a liberdade e a autonomia do indivíduo em um mundo cada vez mais conectado.

---

[33] ART. 7º e 11º, LGPD.
[34] A expressão original é de ZANON, João Carlos. Cit p.96.
[35] Emenda Constitucional nº 115, de 2022. Altera o artigo 5º da Constituição da República Federativa do Brasil para incluir a proteção de dados pessoais como direito fundamental. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 19 set. 2024.

Ao estabelecer regras para a coleta, o processamento e o compartilhamento de dados, a legislação de proteção de dados, como a LGPD, cria um ambiente onde o consentimento do titular é uma das bases para o tratamento de dados. Este ambiente é chamado de autodeterminação[36] informativa, o que significa que os indivíduos têm, agora, um controle mais ativo sobre suas informações pessoais, podendo controlar[37], por exemplo, se desejam ou não fornecer seus dados para uma determinada finalidade. A privacidade, portanto, não se limita ao direito de manter informações ocultas, mas se expande para o direito de ter o controle sobre como os dados são utilizados e por quem.

A proteção de dados pessoais não só preserva a privacidade dos indivíduos, mas também evita discriminação, fraudes e abusos, como o uso indevido de informações financeiras ou de saúde. Além disso, promove a segurança e a confiança nas interações digitais, permitindo que as pessoas compartilhem dados de maneira consciente e segura, sem o temor de que suas informações pessoais sejam usadas de maneira indevida.

A partir da análise do conceito de privacidade, fica claro que, diante do novo contexto social, ele foi ampliado e reinterpretado, especialmente no que tange à proteção de dados pessoais. Essa evolução vai além da simples tutela da intimidade individual, refletindo um critério essencial para a proteção dos direitos fundamentais de toda a sociedade. A proteção de dados pessoais, portanto, não se limita a uma questão legal, mas se configura como um direito constitucional, de interesse público, que visa garantir a dignidade, a liberdade e a autonomia do indivíduo na era digital.

Essa transição exige uma compreensão profunda das responsabilidades envolvidas. Para os profissionais de tecnologia, a atuação vai além da criação de sistemas seguros; ela também deve considerar a implementação de práticas que assegurem a conformidade com os direitos do indivíduo. Já os profissionais que interpretam as leis de privacidade têm o desafio de contextualizar esses direitos em um cenário dinâmico, assegurando que a legislação acompanhe os avanços tecnológicos sem perder de vista a proteção dos direitos fundamentais.

Diante das transformações rápidas e profundas que a sociedade enfrenta no cenário digital, a intersecção entre privacidade e proteção de dados pessoais emerge como um tema essencial, mas que ainda gera questionamentos complexos. Embora a proteção de dados seja reconhecida

[36] Segundo Danilo Doneda, o conceito aparece inicialmente na década de 1970 no livro Privacy and Freedom de Alan Westin.
[37] MARTINS, Leonardo (Org.). Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Montevidéu: Fundação Kontad Adenauer, 2005, páginas 233 a 235.

como um direito fundamental, distinto da privacidade, ambos compartilham o objetivo de assegurar a autonomia e a dignidade do indivíduo, especialmente em um contexto em que a coleta e o uso de informações pessoais acontecem de maneira quase imperceptível. No entanto, a dúvida persiste: estamos realmente protegendo todas as nuances da privacidade por meio da regulação da proteção de dados pessoais?

Esse paradoxo entre proteção e privacidade reflete um desafio maior: como garantir que o marco legal, embora essencial, seja flexível o suficiente para se adaptar às novas formas de coleta e utilização de dados, e, ao mesmo tempo, resguardar direitos humanos essenciais? A proteção dos dados pessoais não deve ser apenas um esforço jurídico, mas uma prática de conscientização e responsabilidade que envolve todos os cidadãos. O questionamento, portanto, não se resume a uma solução simples, mas a um contínuo processo de reflexão e adaptação, onde a privacidade e a proteção de dados devem caminhar lado a lado, com a devida sensibilidade para as complexidades dos dias atuais.

1.3. O CAMINHO DA PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS – PRIMEIRAS INICIATIVAS (EUROPA)

O presente tópico tem como objetivo a examinar as iniciativas europeias em matéria de proteção de dados pessoais, abordando suas origens, os desafios enfrentados e os avanços que, ao longo do tempo, contribuíram para a construção do atual panorama normativo e institucional da privacidade, sendo modelo global.

No cenário das últimas décadas, a Europa se destacou como a região responsável pela criação dos mais importantes e abrangentes conjuntos de leis voltadas à proteção de dados pessoais. A evolução dessa legislação remonta à década de 70, a quando a Alemanha se tornou pioneira nesse campo, impulsionada pela necessidade de proteger seus cidadãos dos abusos que ocorreram durante o regime nazista. Em 1970, o Estado de Hesse[38] adotou a Hessiches Datenschutzgesetz (HDSG)[39], uma das primeiras legislações a estabelecer normas específicas para o tratamento de dados pessoais, que, de acordo com estimativas, hoje está presente em mais de 141 países.[40]

[38] A Lei de Proteção de Dados do Land alemão de Hesse foi promulgada em 30 de setembro de 1970. *The Hesse Data Protection Act.*

[39] A Hessische Datenschutz, criou uma autoridade – o Datenschutzbeauftragter, ou comissário para a proteção de dados – que controlaria a elaboração informática de dados pessoais no confronto com a administração pública em iniciativa pioneira na Europa até então. Intersoft Consulting - Disponível em: https://dsgvo-gesetz.de/hdsig/ Acesso em 10 abr.2024.

[40] O professor Graham Greenleaf contabilizou 142 países com legislações de proteção de dados em 2020.Note-se que a sua metodologia engloba também países que não são membros da Organização das Nações Unida, bem como alguns países, como Nepal e Zimbabwe, cujas legislações aplicam-se somente ao setor público. GREENLEAF, Graham:

Esse marco histórico não apenas refletiu a crescente preocupação com a privacidade, mas também estabeleceu diretrizes fundamentais para o processamento de informações pessoais em um período de transformação tecnológica acelerada. Importante ressaltar que, naquela época, a maior ameaça à proteção de dados pessoais não provinha das grandes corporações de publicidade digital, como é o caso na atualidade, mas sim do próprio Estado. Essa realidade conferiu à legislação alemã um caráter singular e visionário, antecipando preocupações que só viriam a ser amplamente debatidas décadas depois.

O jurista Spiros Simitis (1934)[41] foi precursor nesse movimento, desempenhando um papel vital e contribuindo significativamente para o progresso do debate sobre proteção de dados, abordando temas como autodeterminação informativa e privacidade em suas aulas universitárias. É considerado por muitos o pai da proteção de dados.[42]

A legislação inicial apresentava lacunas importantes em relação a aspectos fundamentais da proteção de dados na contemporaneidade, como a exigência de uma base legal para o processamento de dados, a limitação da coleta a informações estritamente necessárias e a necessidade de um propósito específico para o tratamento dos dados.

Com o tempo, no entanto, a legislação passou por reformas significativas. Oito anos após a implementação da primeira lei nacional de proteção de dados da Alemanha e três anos após o reconhecimento, pela Suprema Corte alemã, do direito à autodeterminação informativa, a Lei de *Hesse* foi substancialmente revisada. A versão reformulada entrou em vigor em 1º de janeiro de 1987, com a criação da *Bundesdatenschutzgesetz* (BDSG), que consolidou os princípios da privacidade e da autodeterminação informativa, representando um avanço determinante na proteção de dados pessoais no país.

Dessa forma, a Europa desempenhou um papel fundamental na construção de um legado significativo no campo da proteção de dados, o qual não apenas influenciou o desenvolvimento legislativo de outras nações, mas também contribuiu de maneira substancial para a conscientização global acerca da importância da privacidade.

COTTIER, Bertil.2020 ends a decade of 62 new data Privacy laws. *Privacy laws & Business International Report*, v.163, p. 24-26, 29 jan. Disponível em: https://ssrn.com/abstract=3572611. Acesso em 18 dez.2024.

[41] GREVEN, Ludwig. "A fome por dados está crescendo". O pioneiro da proteção de dados Spiros Simitis nos vê mais perto do que nunca do cidadão transparente e considera que uma proteção mais forte de dados privados é ainda mais urgente, não apenas no censo planejado. Ein Interview. 5 set. 2009. Tradução para o português. Consultado em: 09 abr. 2024.

[42] Em reconhecimento de seu papel, admiradores às vezes o descrevem como "o homem que inventou a proteção de dados.

Em 24 de outubro de 1995, foi adotada a Diretiva 95/46/CE[43] pela União Europeia, que estabeleceu os fundamentos legais para a proteção de dados pessoais, alinhando-se aos princípios das legislações contemporâneas sobre o tema. Este marco regulatório se tornou a principal referência na Europa, abordando a proteção dos indivíduos no que se refere ao tratamento e à livre circulação de dados pessoais.

A diretiva instituiu um quadro normativo com o objetivo de equilibrar um alto nível de proteção da privacidade com a necessidade de facilitar a circulação de dados pessoais dentro da União Europeia (UE), sendo importante ressaltar o interessante fato de que em duas proposts de diretivas, a Comunidade Europeia tenha optado por atribuir aos cidadãos, um elevado grau de proteção para as suas informações pessoais[44].

Entre os principais pontos da diretiva, destacam-se:

(i) **Âmbito de aplicação da Diretiva** –

Aplica-se aos dados tratados por meios automatizados (como bases de dados informáticas de clientes) e aos dados contidos ou destinados a figurar em arquivos não automatizados (como arquivos tradicionais em papel);

Não se aplica ao tratamento de dados realizado por uma pessoa natural no exercício de atividades exclusivamente pessoais ou domésticas, nem a atividades não sujeitas à aplicação do direito comunitário, como segurança pública, defesa ou segurança do Estado.

(ii) **Princípios Essenciais:** O tratamento de dados só é lícito se:

A pessoa natural tiver dado de forma inequívoca o seu consentimento.

O tratamento for necessário para a execução de um contrato no qual a pessoa natural seja parte.

O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito.

[43] EUR-Lex Access to European Union law – disponível em: Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 2... (europa.eu). Acesso em 10/04/2024.

[44] NT: A terminologia hoje se encontra inserida na Diretiva 95/46/CE, em sua consideração 10, bem como no código italiano em matéria de proteção de dados pessoais em seu artigo 2.2.

(iii) **Organismos Nacionais de Controle:** Cada Estado-Membro deve criar um organismo nacional independente encarregado de controle de todas as atividades relacionadas com o tratamento de dados pessoais.

Para maior coerência e aplicabilidade direta a então diretiva que exigia a transposição para as legislações nacionais de cada Estado-Membro, resultando em variações na aplicação das normas de proteção de dados dentro da UE, em 25 de maio de 2018, entra em vigor, o Regulamento Geral sobre Proteção de Dados (General Data Protection Regulation – GDPR), propondo:

(iv) **Adequação ao Contexto Digital e Tecnológico Atual**: A Diretiva 95/46/CE foi criada em um contexto pré-internet, em um momento em que as tecnologias de processamento de dados estavam em sua fase inicial de desenvolvimento. O mundo digital moderno, com o crescimento das redes sociais, big data, inteligência artificial e a coleta massiva de dados, exigia um novo marco legal mais robusto e adaptado a esses novos desafios. O GDPR foi projetado para lidar com o aumento significativo do volume e da complexidade do tratamento de dados pessoais na era digital.

(v) **Fortalecimento dos Direitos dos Indivíduos**: O GDPR visa garantir uma proteção mais eficaz e explícita dos direitos dos indivíduos, fortalecendo as obrigações dos controladores de dados e das organizações. O regulamento trouxe, por exemplo, a obrigatoriedade do consentimento explícito e informado para o tratamento de dados pessoais.

(vi) **Aumento das Responsabilidades das Empresas**: O GDPR ampliou as obrigações das empresas, impondo-lhes maior responsabilidade em relação à proteção de dados pessoais. Exigiu a implementação de medidas de segurança mais rigorosas, a realização de avaliações de impacto sobre a proteção de dados e a notificação de violações de dados às autoridades competentes e aos indivíduos afetados.

(vii) **Respostas à Globalização e à Transferência Internacional de Dados**: A Diretiva 95/46/CE apresentava lacunas em relação à regulamentação da transferência de dados pessoais para fora da União Europeia, o que foi uma preocupação crescente à medida que empresas globais passaram a operar em mercados internacionais. O GDPR introduziu mecanismos mais claros e rigorosos para a transferência internacional de dados, incluindo a imposição de cláusulas contratuais padrão e a regulamentação de decisões automatizadas e transferências para países fora da UE.

(viii) **Enfrentamento de Novos Desafios no Ámbito da Segurança e Privacidade**: A Diretiva 95/46/CE não estava suficientemente preparada para enfrentar as novas ameaças à segurança dos dados, como ataques cibernéticos e violações massivas de dados. O GDPR colocou uma ênfase maior em medidas de segurança proativas e reativas, exigindo que as empresas adotassem um enfoque de "proteção desde a concepção" e "proteção por padrão" (privacy by design and by default)[45].

(ix) **Reforço das Penalidades**: As sanções previstas na Diretiva 95/46/CE eram consideradas relativamente brandas e, muitas vezes, insuficientes para garantir o cumprimento das normas. O GDPR estabeleceu multas substanciais, com limites que podem chegar a até 4% da receita anual global de uma empresa ou €20 milhões (o que for maior), o que aumentou significativamente o poder de dissuasão e incentivou as organizações a cumprir rigorosamente as normas de proteção de dados.

O Regulamento Geral de Proteção de Dados (GDPR) é amplamente reconhecido por sua robustez normativa, destacando-se principalmente pela sua capacidade de enfrentar os desafios decorrentes da rápida evolução tecnológica. Esta legislação não apenas surge como resposta à carência de um marco regulatório adaptado às novas realidades digitais, mas também se estabelece como um referencial global na proteção de dados pessoais.

Ao abordar questões emergentes relacionadas ao tratamento de informações pessoais em um contexto digital dinâmico, o GDPR representa uma tentativa de harmonizar e fortalecer a proteção da privacidade, garantindo direitos fundamentais aos indivíduos enquanto se ajusta aos avanços tecnológicos e às necessidades de um mercado globalizado.

Em síntese, à luz da crescente harmonização normativa em torno da proteção de dados pessoais no cenário global, o GDPR, aprovado pela UE e em vigor desde 2018, consolidou-se como um marco regulatório robusto e de referência internacional, ao estabelecer padrões elevados

---

[45] *Privacy by design* (é a preocupação com a privacidade dos dados desde a concepção de qualquer novo projeto ou serviço) diz respeito ao emprego de meios para se preservar a privacidade durante todo o ciclo de vida dos dados pessoais. No caso, a privacidade é base para a arquitetura dos sistemas e processos desenvolvidos, de modo a possibilitar, pelo formato disponibilizado e pelo serviço prestado, condições que permitam ao titular de dados pessoais preservar a sua privacidade e o formato em que ocorre o tratamento dos seus dados.
Privacy by default (privacidade por padrão) representa a instituição de que todas as ferramentas para preservar a privacidade estejam acionadas como padrão, isto é: a configuração padrão já confere a maior expectativa de privacidade possível ao titular de dados pessoais.
Disponível em: https://www.terracap.df.gov.br/index.php/listagem-faq/78-lgpd-lei-geral-de-protecao-de-dados-pessoais/196-53-o-que-e-privacy-by-design-e-privacy-by-default. Acesso em 02 de Fev.2025.

de proteção de dados, baseados na autodeterminação informativa, na transparência, no consentimento e na responsabilização dos agentes de tratamento. Sua influência sobre a LGPD foi determinante não apenas pelo conteúdo normativo — do qual diversos dispositivos foram diretamente inspirados —, mas também por razões de ordem econômica, jurídica e diplomática.

A adoção da LGPD reflete não apenas uma adequação ao cenário global de proteção de dados[46], mas também uma resposta às demandas locais por um sistema mais rigoroso e transparente. Em capítulo próprio, exploraremos os caminhos percorridos no desenvolvimento da legislação sobre proteção de dados, com um foco particular na gênese, implementação e desafios enfrentados pela LGPD, além de analisar sua relação com os princípios e diretrizes do GDPR.

[46] É importante distinguir dados gerais de dados pessoais, pois estes últimos possuem um vínculo objetivo com a pessoa, justamente por revelar aspectos que lhe dizem respeito (DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.p.157).

2. PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO

Embora a Lei Geral de Proteção de Dados Pessoais (LGPD) represente um marco consolidado no ordenamento jurídico brasileiro, é importante reconhecer que o arcabouço normativo relativo à proteção de dados no Brasil não se restringe a essa legislação. Trata-se, na realidade, de uma construção jurídica mais ampla e progressiva, desenvolvida ao longo das últimas décadas por meio de dispositivos legais que, embora setoriais[47], desempenharam papel fundamental na consolidação dos direitos informacionais.

Ainda nas décadas de 1970 e 1980, já se observava, por parte de determinados setores da sociedade e do legislativo, a percepção da necessidade de uma norma jurídica abrangente que disciplinasse, de forma transversal, o tratamento de dados pessoais nos mais diversos domínios, tanto que, o primeiro movimento legislativo[48] no Brasil a abordar diretamente as questões relacionadas à proteção de dados, foi em 1978, pelo José Roberto Faria Lima e foi acolhido por parlamentares que interagiam com o Movimento Democrático Brasileiro.[49]

Essa compreensão emergiu como resposta às preocupações crescentes com o uso indiscriminado de informações pessoais em cadastros e bancos de dados, bem como diante de projetos estatais com elevado potencial de centralização e controle, como o proposto Registro Nacional de Pessoas Naturais (RENAPE)[50]. Exemplo emblemático dessa sensibilidade normativa é o Projeto de Lei nº 2.796, de 1980, de autoria da Deputada Cristina Tavares[51], que visava

---

[47] Entre esses pilares, destacam-se o Código de Defesa do Consumidor (Lei nº 8.078/1990), que antecipou garantias relacionadas à transparência e ao tratamento de dados dos consumidores; o Marco Civil da Internet (Lei nº 12.965/2014), que instituiu princípios para a governança da internet e proteção à privacidade; e a Lei do Cadastro Positivo (Lei nº 12.414/2011, posteriormente alterada pela Lei Complementar nº 166/2019), que regulamenta o uso de informações financeiras com vistas à formação de histórico de crédito. Essas normas, em conjunto, pavimentaram o caminho para o desenvolvimento de uma legislação geral e transversal em matéria de proteção de dados pessoais.

[48] Como explica Rafael Zanatta no primeiro episódio da Memória LGPD: "A primeira geração é uma geração que trouxe a discussão sobre dados pessoais durante a ditadura militar. Então houve, por exemplo, um projeto do Governo Federal na época do Geisel de implementação de um sistema nacional de pessoas naturais, chamado RENAPE, o que trouxe uma reação muito grande de lideranças de juristas como Raymundo Faoro, René Ariel Dotti - inclusive, o primeiro projeto de lei sobre dados pessoais no Brasil é de 78, que é do José Roberto Faria Lima (...), uma tentativa fracassada de fazer uma legislação de proteção de dados". Disponível em: https://observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/.. Acesso em: 13 de janeiro de 2025.

[49] Para saber mais acesse: https://www.mdb.org.br/quem-somos/

[50] VIANNA, Marcelo. Um novo "1984"? O projeto RENAPE e as discussões tecnopolíticas no campo da informática brasileira durante os governos militares na década de 1970. Oficina do Historiador, Porto Alegre, Suplemento especial, ISSN 21783748, I EPHIS/PUCRS, 27 a 29 maio 2014, p. 1148-11171. Disponível em https://revistaseletronicas.pucrs.br/oficinadohistoriador/article/view/18998/12057. Acesso em: 19 de janeiro de 2025.

[51] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais, p. 46. In: BIONI, Bruno,DONEDA, Danilo, MENDES, Laura Schertel, RODRIGUES JUNIOR, Otávio Luiz, SARLET, Ingo Wolfgang (org.). Tratado de

estabelecer limites e diretrizes para a coleta e uso de dados pessoais, antevendo, já àquela altura, os desafios éticos, jurídicos e sociais que a informatização e a vigilância estatal poderiam representar para os direitos fundamentais, portanto, o PL visava garantir aos cidadãos o acesso às informações sobre eles constantes em bancos de dados, além de prever outras disposições correlatas.

Embora o PL nº 2.796, de 1980 tenha sido arquivado ao fim da legislatura, a crescente demanda por uma maior efetivação de direitos relacionados à proteção de dados pessoais, especialmente no que tange aos direitos de acesso e retificação, se intensificou ao longo da década de 1980, em sintonia com o movimento de redemocratização do país. Esse processo culminou, entre outras coisas, com a inclusão da ação de *habeas data* na Constituição de 1988.

Antes mesmo da promulgação da Constituição, algumas legislações estaduais, como as dos estados do Rio de Janeiro e de São Paulo, já previam o direito de acesso e retificação de dados pessoais. Essas normas, ao incorporar princípios como o da finalidade e o do consentimento informado, desempenharam um papel significativo na construção do debate em torno da incorporação da ação de *habeas data* na Carta Magna de 1988 em seu art. 5º., LXXII, com a seguinte forma:

> "Art.17. Todos têm direito de acesso às referências e informações a seu respeito, registradas por entidades públicas ou particulares, podendo exigir a retificação de dados, com sua atualização e supressão dos incorretos mediante procedimento judicial sigiloso.
>
> §1.º É vedado o registro informatico sobre convicções pessoais, atividades políticas ou vida privada, ressalvando o processamento de dados não identificados para fins estatísticos.
>
> §2.º A lesão decorrente do lançamento ou da utilização de registro falsos gera a responsabilidade civil, penal e administrativa."
>
> [...]
>
> "Art. 48. Dar-se-à *habeas data* aolegítimo interessado para assegurar os direitos tutelados no art 17."[52]

Sob uma análise retrospectiva, a Constituição de 1988, apesar de introduzir importantes inovações, como a previsão da ação de *habeas data* e a garantia dos direitos à vida privada, à

Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.

[52] Anteprojeto Constitucional elaborado pela comissão de Estudos Constitucionais. Diário Oficial da União, Suplemento especial, 26 de set.1986, p.5-6.

intimidade[53], e ao sigilo das telecomunicações, telegráficas e de dados[54], não foi capaz de consolidar, de imediato, a ideia de um direito à proteção de dados pessoais. Pelo contrário, o Supremo Tribunal Federal, em decisão de 2006, relatada pelo Ministro Sepúlveda Pertence – que, vale ressaltar, havia se posicionado favoravelmente em doutrina acerca da materialidade de um direito sobre dados pessoais – não reconheceu a inviolabilidade dos dados armazenados em computadores com base nas garantias constitucionais. Em sua decisão, o STF seguiu a linha de pensamento de Tércio Sampaio Ferraz Júnior, que argumentava que o ordenamento jurídico brasileiro protege o sigilo das comunicações, mas não necessariamente a proteção de dados em si[55]. Esse entendimento reflete a ausência de um reconhecimento imediato de uma tutela jurídica específica sobre os dados pessoais, mesmo diante das inovações constitucionais da época.

No Brasil, embora tenham existido diversos elementos que serviram como ponto de partida para a criação de uma legislação própria voltada à proteção de dados pessoais, esses aspectos nem sempre tiveram o mesmo impacto ou desenvolvimento. Um exemplo disso pode ser observado nas discussões que surgiram na década de 1970[56] sobre a criação de cadastros únicos para cidadãos, como o *National Data Center* também teve repercussão no Brasil. No entanto, diferentemente de muitos países europeus que, impulsionados por tais discussões, avançaram na formulação de legislações específicas sobre a matéria, o Brasil adotou uma trajetória mais gradual. Nesse processo, instrumentos como o Código de Defesa do Consumidor (Lei nº 8.078/1990) e a Lei do Cadastro Positivo (Lei nº 12.414/2011) desempenharam papel relevante ao introduzirem, ainda que de forma setorial, a temática do tratamento de dados pessoais — inclusive dados sensíveis, como informações sobre saúde, situação financeira e perfil de consumo — no ordenamento jurídico. Tais dispositivos anteciparam, de forma pontual, preocupações que viriam

[53] Art.5.º, X CF
[54] Art.5.º, XII
[55] "O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isso é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas." Note-se, para a caracterização dos blocos, que a conjunção e uma correspondência com telegrafia, segue-se uma vírgula e depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que deveria ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não está havendo quebra de sigilo. Mas, se alguém entra nessa transmissão como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados. A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação. Doutro modo, se alguém, não por razões profissionais, ficasse sabendo legitimação pessoal de forma diversa daquela binária – sigilo/abertura, público/privado– de forma que reflita a complexidade da matéria da informação [...] FERRAZ JR., Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, v.88, p.447,1993).
[56] A inserção do tema no debate público brasileiro torna-se perceptível no início da década de 1970. Veja-se o editorial do Jornal do Brasil: Quem polícia os computadores? Jornal Brasil, 27-28 fev.1972, p.6.

a ser consolidadas décadas depois com a promulgação da LGPD.

Diversos instrumentos normativos tenham contribuído como fundamentos iniciais para a construção de um arcabouço legal voltado à proteção de dados pessoais, esses elementos evoluíram de maneira desigual e fragmentada. E após algumas décadas, com a chegada da Lei Geral de Proteção de Dados (LGPD), houve não apenas a unificação de diretrizes de dados pessoais, mas também a consolidação de uma abordagem sistêmica para o tratamento de dados pessoais, obviamente absorvendo elementos dispersos no ordenamento jurídico brasileiro e criando um eixo normativo robusto que passou a orientar a disciplina no país. Dessa forma, a LGPD se tornou a base para a construção de um cenário mais seguro e transparente para a gestão dos dados pessoais dos cidadãos brasileiros e claro, trouxe classificações que definiram a diferença de dado gerais, dados pessoais e dados pessoais sensíveis.

Os dados pessoais representam um dos pilares fundamentais da legislação moderna sobre proteção de dados, tendo sido objeto de regulamentação específica em normas como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia. A definição de dados pessoais, portanto, é um ponto de partida preciso para qualquer análise aprofundada sobre a temática.

De acordo com a LGPD (Lei nº 13.709/2018), "dados pessoais" são definidos como informações relacionadas a pessoa natural identificada ou identificável[57]. Em sua essência, a definição abrange qualquer dado que, isolado ou em conjunto com outras informações, possa identificar direta ou indiretamente um indivíduo. A identificação pode ocorrer de maneira direta, como no caso de nomes, números de documentos ou dados biométricos, ou de forma indireta, quando associados a informações complementares que permitam a identificação de uma pessoa.

Essa definição de dados pessoais se alinha à concepção amplamente adotada na literatura e nas normativas internacionais, que entendem os dados pessoais como informações que envolvem, de maneira direta ou indireta, a vida privada de um indivíduo e apenas com análise da aplicabilidade, através do mapeamento e inventário de dados tais informações, estarão protegidas pela LGPD. E a utilização do verbo “proteger” também demonstra essa necessidade coerente que o legislador enxergou no titular dos dados como vulnerável em comparação aos agentes de tratamento.[58]

[57] Art.5º, inc. I, da LGPD.
[58] COTS, Márcio; Oliveira, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. São Paulo: Ed. RT, 2018. p.59.

A classificação dos dados pessoais é uma etapa essencial para a compreensão da amplitude e das especificidades do tratamento dessas informações. Essa classificação visa distinguir diferentes tipos de dados de acordo com sua sensibilidade, grau de proteção exigido e a finalidade de seu uso. Em um contexto de proteção de dados, as categorias de dados pessoais são classificadas principalmente em dados pessoais comuns e dados pessoais sensíveis, sendo estas as classificações mais amplamente reconhecidas e utilizadas por legislações e doutrinas contemporâneas.

Os dados pessoais comuns ou gerais referem-se a qualquer informação que possa identificar uma pessoa, sem que envolvam categorias de dados que exijam uma proteção especial devido à sua natureza sensível.

Exemplos típicos de dados pessoais gerais incluem, mas não se limitam à: Nome completo;Endereço de residência;Número de telefone;Endereço de e-mail;Número de identidade (RG ou CPF); e Data de nascimento. Esses dados, embora possam ser utilizados para identificar uma pessoa, seja de forma direta ou indireta, não implicam, por si só, em um risco elevado à privacidade do indivíduo, exceto quando tratados de maneira inadequada.

A principal justificativa para a distinção entre dados pessoais comuns e sensíveis está no maior risco à liberdade e à privacidade do indivíduo que a divulgação ou o uso indevido de dados sensíveis pode gerar. Em razão disso, o tratamento de dados sensíveis demanda uma abordagem mais rigorosa, com a implementação de medidas de segurança aprimoradas, além da obtenção de um consentimento expresso e claro por parte do titular, conforme estabelecido pela legislação de proteção de dados, o que será abordado de forma detalhada em tópico subsequente.

A LGPD estabelece um conjunto de normas e diretrizes destinadas a proteger os direitos fundamentais de liberdade e privacidade dos indivíduos, garantindo que os dados pessoais sejam tratados de maneira responsável, segura e transparente, razão pela qual possuí principios e norteadores para garantir que o tratamento de dados pessoais seja realizado com garantia e respeito aos direitos dos titulares de dados[59]. Dos princípios previstos, dois são de especial relevância quando do tratamento de dados sensíveis, o princípio da finalidade e o princípio da não discriminação, os quais serão estrategicamente comentados:

O Princípio da Finalidade, exige que os dados sejam tratados apenas para as finalidades previamente informadas e consentidas pelo titular. Para Doneda, “este princípio possui grande

[59] Art.5º inc. V, da LGPD.

relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)" (DONEDA, 2005, p.216).

Ainda com base no princípio da finalidade, Maria Celina Bodin de Moraes, em apresentação à obra de Stefano Rodotà, entende que o tratamento de dados e especialmente a sua coleta "não pode ser tomada como uma "rede jogada ao mar para pescar qualquer peixe". Ao contrário, as razões de coleta, principalmente quando se tratarem de "dados sensíveis", devem ser objetivas e limitadas" (MORAES, 2008, p. 9). A medida dessa objetividade e limitação será determinada justamente pela finalidade legítima do tratamento, que fica condicionada "à comunicação preventiva ao interessado sobre como serão usadas as informações coletadas; e para algumas categorias de dados especialmente sensíveis estabelece que a única finalidade admissível é o interesse da pessoa considerada" (RODOTÀ, 2008, p. 87).

O Princípio da Adequação, estabelece que o tratamento de dados deve ser não apenas adequado, mas também relevante para a finalidade que foi claramente informada ao titular. Nesse contexto, o Princípio da Necessidade complementa essa diretriz, ao determinar que somente os dados pessoais estritamente necessários para atingir as finalidades informadas podem ser coletados e processados, evitando-se a coleta excessiva de informações. Em consonância com esses princípios, o Princípio do Livre Acesso garante aos titulares de dados o direito de acessar suas informações, retificar dados incorretos e obter esclarecimentos transparentes sobre como seus dados estão sendo tratados, reforçando a necessidade de um controle efetivo sobre o uso das suas informações. Esse direito de acesso e correção dos dados, por sua vez, está diretamente alinhado ao Princípio da Transparência, que exige que as práticas de coleta, uso e armazenamento de dados sejam claras e acessíveis, permitindo que os titulares compreendam completamente como seus dados estão sendo manipulados.

Ademais, o Princípio da Segurança exige que sejam implementadas medidas técnicas e administrativas adequadas para proteger os dados contra acessos não autorizados, perdas, vazamentos ou qualquer outro tipo de incidente de segurança, assegurando que as informações pessoais sejam devidamente protegidas e que riscos sejam minimizados. Dessa forma, todos esses princípios interagem e se complementam, formando um conjunto de diretrizes que visam garantir a proteção e o respeito à privacidade dos titulares de dados, ao mesmo tempo em que asseguram a transparência, a minimização de riscos e a adequação no uso das informações pessoais.

O Princípio da Não Discriminação, visa prevenir o uso discriminatório de dados pessoais.

A coleta e o tratamento de dados pessoais sejam conduzidos de maneira a evitar discriminação ou exclusão injustificada. No que tange ao princípio da não discriminação, é proibido o uso dos dados pessoais para fins discriminatórios ilegais ou excessivos. O legislador, ao associar o uso discriminatório às características de ilegalidade e excessividade, parece admitir a possibilidade de tratamento diferenciado, desde que este seja legítimo e não excessivo. Ou seja, aparentemente, seria válido para o operador de dados realizar tratamentos que impliquem diferenciação, desde que esses não resultem em consequências excludentes que possam ser interpretadas como ilegais.

Por fim, o Princípio da Responsabilização e Prestação de Contas: implica que o controlador[60] de dados pessoais deve ser capaz de demonstrar a conformidade com a LGPD, assumindo a responsabilidade por quaisquer danos causados pelo uso inadequado dos dados.

Além dos princípios, a LGPD também se baseia em uma série de fundamentos[61] que orientam sua aplicação que em sua essência, visam assegurar a proteção dos direitos dos titulares e a boa prática no tratamento de dados pessoais, sendo eles: O respeito à privacidade; A autodeterminação informativa; A liberdade de expressão, de informação, de comunicação e de opinião; A inviolabilidade da intimidade, da honra e da imagem; O desenvolvimento econômico e tecnológico e a inovação;A livre iniciativa, a livre concorrência e a defesa do consumidor; e Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Os fundamentos e principios da LGPD evidenciam seu objetivo de estabelecer normas claras e rigorosas sobre o tratamento de dados pessoais, assegurando aos indivíduos o controle sobre suas informações e garantindo que o uso dessas dados seja feito de forma transparente e responsável, desta forma, surge o questionamento sobre a classificação entre dados pessoais sensíveis e não sensíveis. Afinal, não seria mais coerente tratar todos os dados pessoais com o mesmo nível de cuidado e conformidade com a lei, independentemente de sua natureza? Todos os dados pessoais, ao final, têm o potencial de afetar a privacidade, a liberdade e a dignidade do indivíduo, caso sejam utilizados de maneira indevida. Será, então, que a diferenciação entre dados comuns e sensíveis é, de fato, a melhor abordagem para a proteção da privacidade no cenário atual?

2.1.DADOS PESSOAIS SENSÍVEIS: ANÁLISE DA CATEGORIA ESPECIAL À LUZ DA

[60] Para fins da LGPD, é considerado controlador "qualquer pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º., VI).
[61] Art. 2º, da LGPD.

Na contemporaneidade, marcada pela predominância da informação, o corpo transcende a mera representação física e visível, englobando também um conjunto de dados pessoais que caracterizam os indivíduos. Esse conceito foi abordado por Stefano Rodotá[62] que o denomina de "corpo eletrônico". Ao introduzir essa noção, o jurista italiano enfatiza a relevância da proteção dos dados pessoais não apenas como um direito fundamental para o exercício pleno da cidadania, mas também como uma estratégia de resistência ao aumento da vigilância estatal e ao uso indiscriminado dessas informações por diversas entidades institucionais.

Outro risco significativo envolve o tratamento de dados pessoais sensíveis ou dados de crianças e adolescentes, especialmente quando não são observados os preceitos legais aplicáveis, e o tratamento é realizado de forma automatizada e em grande escala. Por isso, é fundamental que todas as situações de tratamento de dados pessoais sejam avaliadas com cautela, mesmo que, a princípio, não envolvam dados sensíveis ou dados pertencentes a crianças e adolescentes[63]/[64].

Pode se dizer, a propósito, tendo-se em vista o mencionado tratamento legal, que, para fins de direito, os dados pessoais de criança e adolescentes serão sempre considerados sensíveis, uma vez que, por estarem em uma situação peculiar de desenvolvimento progressivo de suas capacidades, são mais vulneráveis e suscetíveis, inclusive às atividades de tratamento,coleta, processamento, manipulação e hiperexposição de dados pessoais.[65]

O direito à titularidade dos dados pessoais é um prerrogativa garantida a toda pessoa natural[66], partindo do princípio de que qualquer dado pessoal[67] que a identifique ou possibilite sua

---

[62] C.f. RODOTÁ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[63] Notório caso, onde o cruzamento de dados pessoais de padrões de consumo gera o dado pessoal sensível a respeito da gravidez de uma adolescente antes mesmo do seu pai tomar conhecimento do fato (How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did). Disponível em: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ Acesso em 18 de set de 2024.

[64] "(...) quando o consentimento for utilizado para o tratamento de dados pessoais sensíveis, de crianças e adolescentes ou para transferência internacional, além de livre, informado e inequívoco, para uma finalidade determinada, ele deverá também ser realizado de forma específica e em destaque" (VAINZOF, Rony in NOBREGA MALDONADO, Viviane; OPICE BLUM, Renato (coord.). LGPD – Lei Geral de Proteção de Dados comentada. São Paulo: revista dos Tribunais, 2019. P. 209).

[65] HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. Tratado de Proteção de Dados Pessoais. Coordenação de Danilo Doneda. 2. ed. Rio de Janeiro: Forense, 2023. p. 218.

[66] C.f. MAIA,Roberta Mauro Medina.A natureza jurídica da titularidade dos dados pessoais.In MULHOLLAND, Caitlin. A LGPD e o novo marco normativo no Brasil. Arquipelogo, 2020, p. 124.

[67]Danilo Doneda afirma que, "em relação a utilização dos termos "dado" e "informação" é necessário notar preliminarmente que o conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. (DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados.2. ed. São Paulo:Thomson Reuters Brasil, 2019, p.136.

identificação possui relevância. Esta proteção, que reflete uma consideração especial pelas informações do indivíduo, encontra respaldo no conceito abrangente de dado pessoal estabelecido pela legislação. A Lei Geral de Proteção de Dados (LGPD) adota, assim, uma abordagem expansiva, semelhante ao modelo europeu, ao definir dado pessoal como "informação relacionada a pessoa natural identificada ou identificável". Esse entendimento amplo visa não apenas a salvaguarda da privacidade, mas também a afirmação da autonomia individual em um contexto de crescente digitalização e interconexão global.

Em seu artigo 5º, inciso II, a LGPD define os dados pessoais sensíveis[68] como "dados pessoais sobre origem racial ou étnica, convicções religiosas, opiniões políticas, 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"[69]. Essa definição reflete a percepção de que, dada a natureza íntima dessas informações, seu uso inadequado pode resultar em discriminação, estigmatização ou outros danos sérios ao indivíduo.

O valor protegido por essa categoria é a igualdade material, sem prejudicar o conceito tradicional de privacidade, e, acima disso, a liberdade, que permitiria ao titular dos dados exercer seus direitos de forma autônoma, sem imposições abusivas ou indevidas, conforme observa Caitlin Mulholland: os conteúdos dos dados sensíveis trazidos no art. 5º, II, da LGPD, são opções realizadas pelo legislador motivadas pelo efeito potencialmente lesivo do seu tratamento".[70]

Essa categorização tem como fundamento a compreensão de que tais dados, pela sua natureza, apresentam maior potencial de causar danos à privacidade e à dignidade do titular, caso sejam utilizados indevidamente. Nesse sentido, a legislação impõe condições mais rigorosas para o tratamento desses dados, com a exigência de consentimento explícito[71] do titular, a não ser em situações excepcionais, como nos casos de cumprimento de obrigação legal ou regulatória, proteção da vida ou da saúde, entre outras hipóteses previstas no artigo 11 da referida Lei.

Para Teffé:

> Entende-se que a defesa da privacidade e dos dados pessoais deve integrar as proteções individuais e coletivas dos direitos fundamentais, tendo em vista a importância de ambas para a tutela integral da pessoa humana e de sua comunidade. Quando se controla o tratamento de informações pessoais, não se resguarda apenas o indivíduo, cujos dados estão

[68] A Lei nº12.414/2011, de Cadastro positivo Art. 3º, II, trouxe a expressão "informação sensível", proibindo anotações em banco de dados usados para análise de crédito.
[69] Art. 11, da LGPD
[70] MULHOLLAND, Caitlin. A tutela dos dados pessoais sensíveis, op.cit., p.123.
[71] Dado de forma clara e sem ambiguidades, por meio de uma ação afirmativa do titular, exigido especialmente para dados sensíveis. Na LGPD, é um requisito para o tratamento desses dados, conforme detalhado no artigo 11.

> relacionados, mas também o seu grupo social, interesses coletivos e as futuras gerações.[72]

A citação em questão reflete uma compreensão ampla da privacidade e da proteção dos dados pessoais, reconhecendo que esses direitos não devem ser encarados de maneira isolada, mas sim como parte de um sistema de proteções que abrange tanto os direitos individuais quanto coletivos. A defesa da privacidade, nesse contexto, assume um papel importante na proteção integral da pessoa humana, ao considerar não apenas o indivíduo, mas também o seu pertencimento a uma comunidade mais ampla.

Esse entendimento ressalta que a gestão e o controle sobre o tratamento de dados pessoais não visam apenas resguardar a identidade e a autonomia de cada indivíduo, mas também preservar o equilíbrio e os direitos do grupo social ao qual pertence, refletindo uma preocupação com as implicações dessas práticas para as gerações futuras, sublinhando a necessidade de uma abordagem holística e intergeracional na proteção da privacidade, enfatizando a importância da sustentabilidade dos direitos fundamentais em um cenário de constantes transformações tecnológicas e sociais.

A criação da categoria especial de dados sensíveis não ocorreu de forma arbitrária. Ao contrário, ela reflete uma preocupação legítima com o impacto que o uso indevido dessas informações pode ter sobre o indivíduo. Os dados sensíveis, por sua natureza, podem ser usados para discriminar, estigmatizar ou prejudicar uma pessoa em diversos contextos, como no mercado de trabalho, em processos judiciais ou em serviços públicos. Por exemplo, informações sobre a religião de uma pessoa, quando utilizadas sem consentimento ou de forma inadequada, podem levar a preconceitos, exclusões ou abusos. Assim, a LGPD reconhece a necessidade de um tratamento especial, que limite o uso desses dados e forneça uma proteção mais robusta.

Outro ponto fulcral na análise dos dados sensíveis é a exigência de consentimento explícito para o seu tratamento, um princípio que está profundamente alinhado com a ideia de autodeterminação informativa. A LGPD exige que o titular dos dados forneça consentimento claro e informado, o que significa que ele deve ser plenamente consciente de como suas informações serão usadas. No caso dos dados sensíveis, a necessidade de um consentimento mais robusto é ainda mais evidente, visto o risco acrescido de danos que seu uso inadequado pode causar.

No entanto, a prática do consentimento pode ser um tema controverso, especialmente em

[72] TEFFÉ, Chiara Spadaccini de. *Dados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas*. 1. ed. São Paulo: Foco, 2022. p. 13.

um cenário em que os indivíduos frequentemente fornecem seus dados sem uma compreensão plena de suas implicações. A complexidade dos processos envolvidos na coleta, no armazenamento e no compartilhamento de dados pessoais, muitas vezes, dificulta a conscientização dos titulares sobre o que estão realmente autorizando. A LGPD tenta mitigar esse problema ao exigir informações claras e acessíveis sobre o tratamento dos dados, mas resta saber se isso será eficaz para garantir que os titulares realmente compreendam e controlem o uso de suas informações sensíveis.

Desde a promulgação da Lei de Cadastro Positivo – Lei 12.414/11 - que em seu artigo 3º, § 3º, II, proíbe anotações em bancos de dados[73] usados para análise de crédito de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas". Significa dizer que para fins de análise de concessão de crédito - princípio da finalidade - estão vedadas inclusões nas bases de dados de quaisquer informações de natureza personalíssima e que não se relacione à finalidade almejada com a análise de crédito, com o objetivo de evitar o tratamento discriminatório - princípio da não discriminação.

Além disso, a classificação dos dados sensíveis alinha-se a um padrão internacional de proteção de dados, como o regulamento europeu de proteção de dados pessoais (GDPR), que também adota uma abordagem diferenciada para essa categoria. Esse alinhamento com a legislação de outros países reflete a importância de se estabelecer normas globais para o tratamento de dados que possam transitar além das fronteiras nacionais, assegurando a proteção dos direitos fundamentais dos indivíduos.

2.2.A Categoria de Dados Pessoais Sensíveis: Aspectos Jurídicos e Sociais

Ao afirmar a importância do livre desenvolvimento da personalidade, reconhece-se que todo indivíduo possui o direito de determinar seu próprio modo de viver. Esse princípio implica que cada pessoa deve ter a liberdade de construir e expressar, de maneira plena, seu projeto de vida, orientando suas ações de acordo com suas escolhas e convicções pessoais,[74] havendo, tanto um direito à individualidade, quanto um direito à diferença.

---

[73] Tribunal de Justiça 1 Súmula (550), 2 acórdãos de repetitivos e 10 acórdãos que tratam da temática relacionada ao sistema de "credit scoring". As decisões, de uma maneira geral, reconhecem o direito do consumidor de ter o acesso aos dados que foram utilizados pelas financeiras ou bancos para a negativa do direito ao crédito. Ver por todos, nesse sentido, o julgamento do Recurso Especial 1.304.736/RS, Rel. Ministro Luis Felipe Salomão, Segunda Seção, julgado em 24/02/2016.

[74] "A personalidade tem relevância positiva nem tanto no momento processual-isto é, nos remédios aos quais recorrer para a cessação da atividade lesiva, para a reintegração de forma específica, para a averiguação, para o ressarcimento, quanto na avaliação substancial do interesse merecedor de concretização, destinado a modificar, a partir do interior,

Enquanto direito fundamental, o livre desenvolvimento da personalidade, deve ser assegurado tanto pelo Estado quanto por terceiros, por meio da implementação de atos, iniciativas e políticas que possibilitem aos indivíduos a plena realização de sua identidade. Esse direito exigiu a criação de um quadro normativo que favoreça o reconhecimento das capacidades, a atribuição de poderes e a delimitação de responsabilidades.

O ordenamento jurídico tem como função assegurar à pessoa humana um amplo espaço para o exercício de suas escolhas, reconhecendo que a liberdade está intrinsecamente relacionada à responsabilidade. O limite desse direito é determinado pela proteção da dignidade de terceiros. Dessa forma, ao proteger os dados pessoais, está-se garantindo diretamente a liberdade, a igualdade e a integridade tanto do indivíduo quanto das coletividades. Por essa razão, é evidente a preocupação de estudiosos da área quanto ao uso indevido de dados pessoais, que pode fomentar práticas discriminatórias em diversas esferas da sociedade e não apenas na área da saúde, por exemplo.

Nessa linha, Thiago Junqueira argumenta que a proteção de dados pessoais e a prevenção da discriminação estão interligadas. Ao restringir o uso de determinados dados, impede-se que esses dados sejam utilizados de forma prejudicial ao titular. Além disso, a LGPD traz instrumentos como o princípio da não discriminação ilícita, a exigência de relatórios de impacto e auditorias pela ANPD, que contribuem para um controle mais eficaz da discriminação nas relações privadas no Brasil. Em resumo, a LGPD tem o potencial de elevar o nível de controle sobre a discriminação no país:

> A ligação entre proteção de dados e prevenção da discriminação é intuitiva. Ao restringir ou condicionar o uso de determinados dados pessoais pelos agentes de tratamento, tem-se, como corolário, o impedimento de sua consideração em prejuízo ao titular deles. Em uma sociedade cada vez mais digital, os instrumentos fornecidos aos indivíduos pelas leis de proteção de dados, como o direito de acesso aos dados tratados pelo controlador e os direitos à explicação e revisão das decisões automatizadas, afiguram-se essenciais para a exposição e minimização de tratamentos discriminatórios. Some-se a eles, ainda, a explicitação de um princípio da não discriminação ilícita ou abusiva, a possível exigência de um relatório de impacto à proteção de dados pessoais (RIPD) e uma auditoria pela ANPD para verificação de aspectos discriminatórios nos tratamentos automatizados, e logo se conclui: o controle da discriminação nas relações entre privados no Brasil tende a mudar de patamar com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD).[75]

a maior parte dos institutos jurídicos, mudando a sua função. A exigência do respeito da personalidade, de sei livre desenvolvimento, incide sobre a sua função[...]" (PERLINGIERI, Pietro. O direito civil na legalidade constitucional. Rio de Janeiro:Revovar,2008, p. 768-769).

[75] JUNQUEIRA, Thiago. Tratamento de Dados Pessoais e Discriminação Algorítmica nos Seguros Revista dos

Destaca-se por Scott Skinner que as proteções legais escassas para a privacidade causam diretamente danos concretos a comunidades marginalizadas, incluindo discriminações de toda ordem, assédio e violência. Estruturas de violência opressiva e sistemática têm sido historicamente destinadas às minorias[76], como negros, homossexuais e transexuais, definindo suas condições de vida e bloqueando sua capacidade de influenciar e moldar a governança democrática, defendendo a necessidade de serem ampliados os instrumentos que efetivamente garantam o direito à privacidade, diante da capacidade do referido direito de promover objetivos relacionados à igualdade, servindo como uma forma de resistência expressiva às vigilâncias governamental e corporativa, bem como de libertação da opressão.

Nesse contexto, a proteção dos dados sensíveis é essencial para assegurar os direitos e liberdades fundamentais de seu titular, requerendo uma proteção mais rigorosa e detalhada por parte das diferentes estruturas sociais, tecnológicas e jurídicas. Isso se justifica pela natureza e pela importância das informações envolvidas, já que seu tratamento inadequado ou eventual vazamento pode acarretar riscos consideráveis à pessoa, servindo como base para preconceitos e discriminações ilegítimas ou prejudiciais contra o titular.[77]

2.3. Debate Brasileiro: Rol Exemplificativo ou Taxativo? Qual o Impacto da Definição do Rol na Proteção dos Direitos Fundamentais: Implicações e Desafios ou Segurança Jurídica e Limitações.

A definição de quais dados são considerados sensíveis reflete a percepção de que a circulação de certas informações pessoais pode representar um risco significativo para seus titulares, dependendo do contexto social e político em que estão inseridos. Contudo, em uma sociedade marcada por diversas formas de discriminação e desigualdade, como a brasileira, será que essa seleção de dados sensíveis é realmente suficiente para proteger os indivíduos de maneira eficaz?

A compreensão dos mecanismos necessários para a proteção dos dados sensíveis deve, portanto, passar por um entendimento mais profundo das dinâmicas discriminatórias presentes na sociedade, questionando se as normas atuais são capazes de abarcar a complexidade desses desafios.

A Constituição Federal de 1988 estabeleceu como um dos seus objetivos fundamentais a

Tribunais,2020, p.240.
[76] SKINNER-THOMPSON, Scott.*Privacy at margins*. Cambridge: Cambridge University Press,2021.
[77] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2.ed. São Paulo: Thomson Reuters, Brasil, 2019.

promoção do bem de todos, assegurando a igualdade e a não discriminação com base em origem, raça, sexo, cor, idade ou qualquer outra forma de diferenciação. Essa diretriz constitucional reflete um compromisso com a eliminação de práticas discriminatórias no Brasil. Já em 1990, a Organização das Nações Unidas (ONU), ao emitir as Diretrizes para a Regulamentação de Arquivos de Dados Pessoais Computadorizados, demonstrou uma evolução no entendimento sobre a proteção de dados pessoais, associando a proteção das informações à necessidade de garantir o princípio da não discriminação. Esse documento reforçou a importância de prevenir o uso de dados pessoais de forma a perpetuar práticas discriminatórias, ampliando o debate sobre a interseção entre a proteção da privacidade e a luta contra as discriminações em nível global.

Dessa forma, as duas datas marcam momentos distintos, mas complementares, na construção de um arcabouço jurídico e normativo que visa a proteção das pessoas contra abusos e discriminação, tanto no âmbito interno quanto internacional, sendo ressaltado pela ONU: "(...) Dados que possam dar origem a discriminação ilegal ou arbitrária, incluindo informações sobre origem racial ou étnica, cor, vida sexual, opiniões políticas, crenças religiosas, filosóficas e outras, bem como a filiação a uma associação ou sindicato, não devem ser compilados."[78] (traduzido para o português).

É fundamental destacar que, apesar dos avanços na garantia dos direitos fundamentais, os grupos mais vulneráveis e as minorias continuam a ser os mais perseguidos e vítimas de violência na sociedade brasileira. Isso torna a proteção ampliada dos dados sensíveis não apenas essencial, mas urgente, sendo igualmente necessário um questionamento profundo das estruturas de poder e vigilância discriminatórias e opressivas.

A LGPD, em seu §2º do Art. 12, define que dados pessoais também podem incluir aqueles utilizados para a formação do perfil comportamental de uma pessoa natural, caso ela seja identificada[79]. Diante disso, surge a reflexão: será que os dados relacionados ao comportamento, por si só, não deveriam ser classificados como dados sensíveis, conforme o rol previsto na LGPD?

De acordo com Laura Schertel, o conceito de "perfil" pode ser entendido como um registro detalhado e abrangente de uma pessoa, que visa oferecer uma visão completa de sua

[78] *"(...) data likely to give rise to unlawful or arbitrary discrimination,including information on racial or ethnic origin, colour, sex life, political nopinions, religious philosophical and other beliefs as well as membership of an association or trade union, should not be compiled*." Disponível em: https://digitallibrary.un.org/record/99493 Acesso em 03 jan. 2025.

[79] MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozati; FALEIROS JÚNIOR, José Luiz. A pandemia da covid-19, o *profiling* e a Lei Geral de Proteção de Dados. Migalhas, 28 de abr,2020. Disponível em https://www.migalhas.com.br/depeso/325618/a-pandemia-da-covid-19--o--profiling--e-a-lei-geral-de-protecao-de-dados . Acesso em 20 de jan. De 2025.

personalidade. Esse perfil é construído a partir da coleta e análise de uma série de dados, que podem abranger diversos aspectos da vida do indivíduo, como suas preferências, comportamentos, interações e características pessoais. A partir dessa reunião de informações, busca-se construir uma representação fiel e, muitas vezes, minuciosa do sujeito, com o intuito de compreender e, em muitos casos, antecipar suas ações, decisões ou reações em diferentes contextos: "uma imagem detalhada e confiável, visando, geralmente, à previsibilidade de padrões de comportamento, de gostos, hábitos de consumo e preferências do consumidor".[80]

Danilo Doneda, argumenta que a técnica de perfilamento utiliza dados pessoais juntamente com métodos estatísticos, técnicas de inteligência artificial e outras ferramentas, com a finalidade de gerar uma "metainformação". Essa metainformação é uma síntese dos hábitos, preferências pessoais e registros de vida de um indivíduo, permitindo, assim, a construção de um perfil que pode prever tendências em suas decisões, comportamentos e até mesmo futuros destinos, tanto para uma pessoa quanto para um grupo.[81]

Nesse contexto, Mulholland e Kremer,[82] defendem a importância de se adotar uma abordagem que leve em conta a diversidade ao implementar a proteção dos dados pessoais sensíveis. O direito deve ser acionado para promover os princípios da igualdade material e da não discriminação, rompendo com a desigualdade formal e combatendo a utilização de características étnico-raciais, sexuais e de gênero como instrumentos de exclusão e segregação.[83]

É válido ressaltarmos a existência dos dados estruturados,84esses dados, quando manipulados de maneira inadequada, têm o potencial de ser utilizados de forma lesiva e discriminatória contra seus titulares. A exploração indevida dessas informações pode não apenas violar a privacidade, mas também possibilitar a revelação de aspectos altamente pessoais e íntimos da vida de um indivíduo, exacerbando vulnerabilidades e criando um ambiente propício à marginalização ou exclusão social, como por exemplo os referidos dados que não estão categorizado como sensíveis na LGPD, por exemplo: (i) faturas de cartão de crédito, (ii) histórico de compras em supermercados ou compras online, (iii) origem social (iv) dados de localização e geolocalização (v) dados financeiros (vi) dados sobre antecedentes85 e (vii) gênero, sempre que

---

[80] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. São Paulo:Saraiva,2014, p.53-54.

[81] DONEDA, Danilo. Da Privacidade à proteção de Dados Pessoais.Rio de Janeiro: Renovar,2006,p.173.

[82]

[83] MULHOLLAND,Caitlin;KREMER,Bianca.Responsabilidade civil por danos causados pela violação do princípio da igualdade no tratamento de dados pessoais. In Rodrigo da Guia Silva: Gustavo Tepedino.Org. O Direito Civil na era da inteligência Artificial. São Paulo: Revista dos Tribunais,2020, p.580.

[84] Usualmente existentes em banco de dados relacionais, que podem ser recuperados e processados de forma eficiente, pois organizados, como os contidos em planilhas.

[85] Acerca dos dados relativos a antecedentes criminais vale ressaltar o tratamento realizado a partir da análise de

vinculados a uma pessoa natural.

Além das preocupações mencionadas nos itens anteriores, outras interrogações, já abordadas em pesquisas realizadas ao longo de mais de uma década, também merecem destaque. Um exemplo notável é o estudo desenvolvido por pesquisadores da Universidade de Cambridge, evidenciou86 que registros digitais de comportamento facilmente acessíveis, como as curtidas no Facebook, podem ser utilizados para prever, de forma automática e precisa, atributos pessoais sensíveis, como orientação sexual, etnia, pontos de vista religiosos e políticos, traços de personalidade, inteligência, felicidade, uso de substâncias viciantes, separação dos pais, idade e sexo. A partir dos perfis analisados, o modelo foi capaz de identificar com elevada acurácia características como a orientação sexual (homossexuais e heterossexuais), a etnia (usuários brancos e negros) e a vinculação partidária (republicana ou democrata).

Se os quesitos abordados acima demonstram a capacidade de identificar informações altamente íntimas com elevada acurácia por meio de uma simples curtida em uma rede social, surge uma reflexão ainda mais inquietante: e se tais dados forem utilizados para treinar inteligências artificiais de diversas categorias?

Nesse contexto, qualquer informação compartilhada nas plataformas, como mensagens, curtidas e histórico de navegação, poderia ser igualmente empregada. Essa perspectiva levanta sérias preocupações sobre a privacidade e a potencial exploração de dados pessoais e inclusive os potencialmente sensíveis, ampliando significativamente os riscos associados ao uso de dados digitais. Como observa Rafael Zanata, o caso representa uma violação aos direitos da personalidade das pessoas: “Os nossos dados são nós mesmos, são o nosso corpo eletrônico. Eles merecem proteção por estarem relacionados à nossa dignidade enquanto pessoa humana.”[87]

Quando estruturados, os dados pessoais podem ser empregados de diversas maneiras, o que

---

certidões e documentos que trazem antecedentes civis e criminais,além de informações acadêmicas e profissionais de uma pessoa, no chamado *background check:*processo realizado pelas orgnizações que iniciam processos seletivos para novos colaboradores,sobretudo para cargos estratégicos , para avaliar a sua idoneidade. Isso costuma ser levantado, por exemplo, nos perfis nas redes sociais, junto a tribunais de justiça ou em orgão como SPC e Serasa. No Brasil, tanto a legislação trabalhista quanto a justiça do trabalho são rigorosos em relação à realização de *background check* e possíveis procedimentos discriminatórios *em relação aos trabalhadores(...).*TST.(PINHEIRO,Iuri;BOMFIM,Vólia.A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. Disponível em: http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho Acesso em 20 de dez.de 2024.

[86] KOSINSKI, Michal; STILLWELL,David;GRAEPEL,Thore.Private traits and atributes are predictable from digital records of human behavior.PNAS, vol.110,n.15,abril/2013, p.5802-5805. Disponível em: https://www.pnas.org/doi/full/10.1073/pnas.1218772110. Acesso em 21 de dez. de 2024.

[87] X vai usar dados de usuários para treinar IAs; é possível se proteger? Disponível em: https://www.estadao.com.br/link/cultura-digital/x-amplia-vai-usar-dados-de-usuarios-para-treinar-ias-e-possivel-se-proteger-nprei/ Acesso em 30 de out. De 2024.

levanta dúvidas sobre a eficácia da proteção legal, cuja finalidade é mitigar os riscos e evitar a discriminação dos indivíduos. Contudo, surge a indagação: até que ponto os titulares de dados compreendem plenamente os impactos negativos que seus dados pessoais podem causar, especialmente antes de serem confrontados com as consequências de sua utilização? A proteção legal seria, portanto, suficiente para garantir a conscientização e a proteção efetiva dos direitos dos indivíduos, ou ela se mostra limitada diante da complexidade e da dinâmica da coleta e uso dos dados pessoais?

Neste cenário, imaginemos que a política de privacidade detalhe expressamente como os dados serão utilizados e com quais terceiros serão compartilhados, imaginemos que o titular tenha consentido, simplesmente por precisar dos serviços ofertados naquele momento. Para embasar os argumentos, observemos os casos de perfilamento[88] que gerou tratamento discriminatório, apresentando por Mulholland. Os casos ocorreram nos EUA e se referiram à contratação de serviços médicos e de seguridade:

Caso1: algumas seguradoras utilizavam dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez, pois o risco contratado seria muito alto.

Caso2: em outro caso relacionado a dados de saúde, “quando uma pessoa tem um derrame, alguns bancos, ao descobrir tal fato, começam a cobrar o pagamento dos empréstimos realizados.”[89]

A distinção entre dados "comuns" e "sensíveis" no tratamento de dados pessoais levanta indagações cruciais sobre a eficácia dessa diferenciação na proteção integral dos direitos dos titulares. Embora dados "comuns" possam ser tratados com menos restrições, muitos desses dados, quando combinados com outras informações, podem revelar aspectos tão íntimos e pessoais quanto aqueles classificados como sensíveis.

O legislador reconhece que as regras relativas ao tratamento de dados sensíveis também se aplicam aos dados pessoais que, embora não sejam considerados sensíveis, possam eventualmente revelar informações sensíveis.[90] Nesse contexto, é pertinente questionar a adequação da categorização tradicional dos dados, especialmente à luz das tecnologias contemporâneas de

[88] *Proffiling* – perfil.
[89] MULHOLLAND, Caitlin. Os contratos de seguro e a proteção dos dados pessoais sensíveis. In.GOLDBERG,Ilan; JUNQUEIRA, Thiago (coords.). Temas Atuais de Direito Dos Seguros, Tomo I. São Paulo: Ed.Thomson Reuters.2020.
[90] Art. 11, §1º da LGPD

processamento e análise, que frequentemente permitem o cruzamento de diferentes fontes de dados para a construção de perfis detalhados dos indivíduos, independentemente da classificação original dos dados.

No que tange à exigência de dano prevista nesse dispositivo legal, é fundamental evitar uma interpretação literal que restrinja a aplicação do artigo 11 da LGPD. A leitura mais apropriada é a de que, sempre que ocorrer o tratamento de dados pessoais sensíveis fora das hipóteses previstas nos incisos I e II do artigo 11 da Lei, haverá um dano presumido, decorrente da violação dos direitos fundamentais, como a dignidade humana, a privacidade e a identidade pessoal, sem prejuízo da autonomia na proteção de dados. Trata-se de um dano in re ipsa, que decorre diretamente do tratamento irregular ou inadequado, não sendo necessário provar a existência de consequências jurídicas adicionais, como o prejuízo patrimonial, conferindo-se, assim, um tratamento diferenciado às situações existenciais envolvidas.[91]

Na comparação entre os artigos 7º (dados gerais) e 11º (dados sensíveis), verifica-se a coincidência de diversas regras comuns, sendo em qualquer caso o consentimento a base primordial para o tratamento de dados, mas especificando-se a existência de outras bases legais. Entretanto, há diferenças marcantes entre os artigos, destacando-se a permissão prevista no art. 11, II, "b", para que haja tratamento de dados sensíveis sem a necessidade de fornecimento de consentimento do titular de dados, quando for indispensável para o tratamento compartilhado de dados necessários à execução pela administração pública, de políticas públicas previstas em leis ou regulamentos[92]. Neste sentido, conforme observa Caitlin:

> O consentimento do titular dos dados sensíveis, seja ele genérico ou específico, poderia ser dispensado em razão de uma ponderação de interesses realizada pela lei, de forma apriorística, que considera como mais relevantes e preponderantes os interesses de natureza pública em relação aos interesses do titular, mesmo que estes últimos sejam qualificados como direitos fundamentais. A autora critica tal preceito, "especialmente se considerarmos que a proteção do conteúdo dos dos dados pessoais sensíveis é fundamental para o pleno exercício de direitos fundamentais, tais como o da igualdade, liberdade e privacidade."[93]

A interpretação de dados sensíveis como um rol taxativo — ou seja, uma lista fechada e imutável de categorias — impõe limitações significativas ao avanço da proteção dos dados pessoais. Se, por um lado, a listagem exaustiva oferece uma visão clara e objetiva sobre o que

[91] MULHOLLAND, Caitlin. A tutela dos dados pessoais sensíveis, op.cit., p.132.
[92] LUCCA, Newton de; MARTINS, Guilherme Magalhães. Direitos fundamentais e sociedade tecnológica.,São Paulo, Foco 2022 p. 7-10.
[93] MULHOLLAND, Caitlin. A tutela dos dados pessoais sensíveis, op.cit., p.128.

deve ser tratado com maior cautela, por outro, pode se tornar obsoleta frente à constante evolução das tecnologias e das formas de processamento de dados.

Uma abordagem positiva, em que o rol de dados sensíveis seja considerado exemplificativo, permitiria uma maior flexibilidade para acomodar novas categorias de dados que podem, em determinado contexto, revelar informações igualmente sensíveis. Isso não só ampliaria a proteção dos titulares, mas também tornaria o sistema mais adaptável às mudanças rápidas no campo da tecnologia e da análise de dados.

Considerando as diversas possibilidades de uso e cruzamento de dados, bem como o constante aprimoramento das ferramentas tecnológicas, torna-se cada vez mais difícil conceber um dado pessoal que não tenha, em algum grau, o potencial de ser sensível[94]. Assertada afirmação, vez que a presente realidade, impõe desafios significativos às categorizações tradicionais, demandando uma reflexão mais profunda sobre como equilibrar a proteção de dados pessoais e a inovação no contexto contemporâneo, onde qualquer menção, opinião e escolha poderá gerar "sensibilidade".

No sistema jurídico brasileiro, o debate acerca da interpretação do conceito de dado sensível não se limita à aplicação da legislação, mas se estende a implicações mais amplas, como a conscientização da população sobre o uso de seus dados.

Questões de segurança jurídica também surgem, especialmente quando consideramos que a rigidez de um rol taxativo pode gerar insegurança na aplicação da lei, diante de novas realidades tecnológicas e sociais. Uma reflexão crítica é a de que, na atual estrutura normativa, a decisão sobre o que é ou não um dado sensível recai, em primeira análise, sobre o Controlador de dados, o que levanta perquirições sobre a imparcialidade e adequação dessa decisão. Até que ponto a autonomia do Controlador garante, de fato, uma proteção robusta para os titulares, ou se, ao contrário, coloca em risco o cumprimento dos direitos fundamentais de privacidade e dignidade? Será que, ao delegarmos tal responsabilidade ao Controlador, corremos o risco de flexibilizar a proteção de dados em favor de interesses corporativos, em detrimento da segurança e da confiança do cidadão?

Estes são questionamentos que exigem uma análise crítica e contínua, considerando o cenário dinâmico e as rápidas mudanças tecnológicas que impactam a privacidade e a segurança

[94] TEFFÉ, Chiara Spadaccini de. Dados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas. 1. ed. São Paulo: Foco, 2022. p. 47.

das pessoas, cujos dados pessoais pertencem.

3. ESTUDO COMPARATIVO: ABORDAGENS LEGAIS

3.1. Proteção de Dados Sensíveis: GDPR da União Europeia X LGPD do Brasil

Acerca do tratamento de categorias especiais de dados no GDPR, é amplamente reconhecido que a lista de dados sensíveis contida no Art. 9º, nº 1, é exaustiva[95], ou seja, apenas os dados especificamente mencionados nesse artigo são considerados sensíveis e, portanto, sujeitos a um regime de proteção mais rigoroso. Contudo, para garantir uma proteção mais robusta aos titulares desses dados sensíveis, o GDPR impõe requisitos mais rigorosos ao consentimento relacionado a esses dados.

Além de ser expresso, o consentimento deve ser livre, explícito, inequívoco, informado e específico, conforme detalhado no considerando (51), o que reforça a necessidade de clareza e transparência na coleta e no tratamento desses dados pessoais, mesmo dentro dos limites da lista exaustiva definida pela norma, conforme segue:

> Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. **Deverão incluir-se** neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por

[95] GEORGIEVA, Ludmila; KUNER, Cristopher. Article 9 Processing of special categories of personal data In: KUNER, Cristopher; Bygrave, Lee; DOCKSEY, Cristopher. The EU General Data Protection Regulation (GDPR): A Commentary.1. Oxford University Press:2020. p.373.

> exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.[96] *(*Grifo meu*).*

O considerando (51) do GDPR estabelece que "merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais". Este trecho sugere que a proteção de dados sensíveis deve ser abordada com uma maior cautela, considerando o impacto potencial que seu tratamento inadequado pode ter sobre os direitos e liberdades dos indivíduos. Além disso, a referência a "riscos significativos" implica que, à medida que novos contextos ou tecnologias emergem, o tratamento de certos dados pode passar a gerar riscos antes não previstos, o que poderia justificar uma ampliação do rol de dados sensíveis.

Dessa forma, seria possível argumentar que, dados pessoais que inicialmente não são considerados sensíveis, podem, com o tempo, passar a ser reconhecidos como tal, caso o tratamento dessas informações venha a demonstrar um potencial significativo para causar danos aos direitos e liberdades do titular?

Essa reflexão levanta a questão de que a classificação de dados sensíveis não é estática, mas pode evoluir conforme a identificação de novos riscos ou consequências prejudiciais aos indivíduos. Tal perspectiva sugere que o conceito de "dados sensíveis" no contexto da proteção de dados pode ser flexível e adaptável, à medida que o desenvolvimento tecnológico e as mudanças sociais criam ameaças aos direitos dos titulares. Essa dinâmica levanta a necessidade de revisar periodicamente os critérios utilizados para determinar quais dados exigem proteção específica, à medida que os riscos associados ao seu tratamento se tornam mais evidentes.

Adicionalmente, o comentário (71)[97] do GDPR ressalta a responsabilidade do controlador

---

[96] Considerando 51 do REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016.

[97] Considerando 71 do REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016: O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada

de dados em adotar medidas para proteger as informações pessoais, considerando os potenciais riscos para os interesses e direitos dos titulares. O regulamento também enfatiza a importância de prevenir efeitos discriminatórios, como aqueles relacionados à origem racial ou étnica, opiniões políticas, religião ou convicções, filiação sindical, estado genético ou de saúde e orientação sexual.

Essas disposições evidenciam a necessidade de uma vigilância constante sobre as implicações do tratamento de dados sensíveis, sugerindo que, embora o regulamento forneça uma lista específica de categorias sensíveis, o escopo do que pode ser considerado sensível poderia ser ampliado, dado que novas questões e contextos podem emergir à medida que as tecnologias de processamento de dados evoluem.

O considerando (85) do GDPR, em seus ditames, nos leva a refletir que existem uma ampliação de proteção, além da categoria especial de dados que, embora não classificados como tais, também poderiam gerar riscos consideráveis para os indivíduos. Isso porque os danos associados ao tratamento inadequado de dados não se limitam exclusivamente àqueles classificados como sensíveis, mas podem ocorrer também com dados pessoais "comuns ou gerais", a depender do contexto e da forma como são utilizados, portanto, aparenta existir extensão destes dados como sensíveis, a partir da possibilidade de danos causados ao titular.

O GDPR tratou de forma adequada o risco de danos resultantes do tratamento inadequado de dados pessoais. Nesse cenário, é fundamental ressaltar o aumento do uso de algoritmos baseados em grandes volumes de dados, os quais, dependendo de sua programação, podem ocasionar efeitos adversos aos titulares. Esses danos não se limitam a dados sensíveis, mas podem ocorrer em situações igualmente delicadas, como análises de crédito e processos seletivos de emprego. Nessas situações, a aplicação de algoritmos pode gerar decisões enviesadas,

---

pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança.A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas.

comprometendo a equidade e a justiça nos processos.

A possibilidade de viés nos sistemas automatizados reforça a necessidade de uma regulamentação rigorosa e de uma interpretação de dados sensíveis em tempo real, analisando o resultado do dano aos titulares de dados, a fim de mitigar os impactos negativos do tratamento de dados pessoais e garantir a proteção dos direitos e interesses dos indivíduos.

Considerando que a Inteligência Artificial (IA) se configura como uma das tecnologias mais relevantes da contemporaneidade (RUSSELL, 2019), torna-se imperativo tratar seu design ético como um direito fundamental. Isso se justifica pela magnitude dos riscos associados ao seu uso, que abrangem, entre outras questões, ameaças à democracia, à privacidade e a potencial criação ou reforço de preconceitos.[98]

Milena Donato e Jennifer Silva observaram de forma precisa ao descreverem que a discriminação algorítmica pode ser direta ou indireta:

> A discriminação pode ser ilícita por se basear diretamente em elementos vedados para certos fins, como a cor ou o gênero (discriminação direta), ou quando, embora com amparo em critérios aparentemente inofensivos, como endereço residencial, acaba por atingir negativamente pessoas de determinada raça, por exemplo (discriminação indireta). Decisões automatizadas, efetuadas com base em algoritimos, podem apresentar conteúdo discriminatório (direto ou indireto). Mostra-se emblemático o famoso caso da Amazon, em que um algoritimo de recrutamento utilizado pelo setor de recursos humanos favorecia a contratação de funcionários do sexo masculino. O algoritimo foi alimentado com dados que refletem a predominância masculina no mercado de trabalho, daí concluindo que candidatos homens seriam preferíveis às candidaturas de mulheres. Como se percebe, a qualidade dos dados utilizados influi na qualidade dos resultados alcançados: se os dados trazem vieses, os resultados também serão enviesados, pois os algoritimos aprendem com os dados que os alimentam".[99]

Considerando o contexto europeu, existe uma análise teórica realizada por Sandra Wachter e Brent Mittelstadt[100] sobre as inferências feitas a partir de dados pessoais, e se, dependendo do conteúdo oferecido, essas inferências podem ser classificadas como dados sensíveis, considerando que:

---

[98] JUNQUILHO, Tainá Aguiar. Inteligência Artificial no Direito: Limites Éticos. São Paulo: Editora JusPodivm, 2022. p. 16.

[99] OLIVA, Milena; Silva,Jeniffer. Discriminação algorítimica nas relações de consumo. Migalhas, publicado em 23 de fevereiro de 2021. Disponível em https://www.migalhas.com.br/depeso/340680/discriminacao-algoritimica-nas-relacoes-de-consumo . Acesso em 28 de dez.2024.

[100] WACTHER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data Protection law in the age of big data and AI.Columbia Business Law review, vol.2019, issue 1, p.01-130.

> É importante observar que gênero, idade, informações sobre a situação financeira de uma pessoa, geolocalização e perfis pessoais não são considerados dados sensíveis nos termos do art. 9º [do GDPR], apesar de muitas vezes servirem como motivo de discriminação. Foi estabelecida uma proibição geral de tratamento de dados sensíveis com várias exceções, incluindo consentimento explícito, fins científicos ou estatísticos ou quando "o tratamento se referir a dados pessoais que sejam manifestamente tornados públicos pelo titular dos dados". Preocupações com inferências estão implícitas na definição de "categoria especial de dados pessoais". A frase "revelação de dados pessoais" sugere que a definição se destina a cobrir dados que divulgam dados indiretamente ou diretamente atributos protegidos (...) em um conjunto posterior de diretrizes sobre a criação de perfis, ou grupo de trabalho do artigo 29, observou que as atividades de criação de perfis podem criar dados sensíveis "por inferência de dados que não são dados de categoria especial por direito próprio, mas se tornam assim quando combinados com outros dados". Embora esses dados proxy, como um código postal, não sejam sensíveis por natureza, o grupo de trabalho do artigo 29º acredita claramente que devem ser tratados como tal, se "revelarem indiretamente" ou puderem ser usados para inferirem atributos sensíveis.[101] [102] (tradução livre).

Os autores destacam[103] que dados considerados não sensíveis podem adquirir caráter sensível quando utilizados para inferir atributos de natureza sensível, embora o conteúdo desses dados permaneça inalterado. Isso implica que a distinção entre dados pessoais gerais e dados pessoais sensíveis apresenta falhas fundamentais, especialmente quando empregada como critério para regular a coleta de dados pessoais. Na era da análise de *Big Data*, essa diferença se torna cada vez mais difusa, uma vez que qualquer dado pode, potencialmente, ser classificado como sensível, desde que seja possível encontrar uma forma de inferir informações sobre atributos protegidos a partir dele.

Embora a LGPD tenha se alinhado, em grande parte, aos princípios estabelecidos pela legislação europeia, ao comparar as duas normas, observa-se que a LGPD não define de forma expressa (como nos considerando do GDPR) o conceito de dados sensíveis. O artigo 5º, inciso II,

---

[101]Texto Original: It is important to note that gender, age, financial situation information, geolocation, and personal profiles are not considered sensitive data under Article 9 [of the GDPR], even though they often serve as grounds for discrimination. A general prohibition on the processing of sensitive data has been established with several exceptions, including explicit consent, scientific or statistical purposes, or when "the processing concerns personal data which are manifestly made public by the data subject." Concerns about inferences are implicit in the definition of "special category of personal data." The phrase "disclosure of personal data" suggests that the definition is intended to cover data that indirectly or directly discloses protected attributes... In a subsequent set of guidelines on profiling, or the Article 29 Working Party, it was noted that profiling activities can create sensitive data "by inference from data that is not special category data in itself, but becomes so when combined with other data." Although such proxy data, like a postal code, is not sensitive by nature, the Article 29 Working Party clearly believes that they should be treated as such if they "indirectly reveal" or can be used to infer sensitive attributes.

[102] WACTHER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data Protection law in the age of big data and AI.Columbia Business Law review, vol.2019, issue 1, p.70-72.

[103] WACTHER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data Protection law in the age of big data and AI.Columbia Business Law review, vol.2019, issue 1, p.73.

da LGPD apenas apresenta, para os fins da Lei, a definição de dados sensíveis como aqueles relacionados à origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados relativos à saúde ou à vida sexual, além de dados genéticos e biométricos, quando vinculados a uma pessoa natural. Embora a Lei forneça uma lista de categorias de dados sensíveis, ela não se aprofunda nas implicações, nos critérios ou nos contextos em que essas informações devem ser tratadas de maneira diferenciada, o que pode gerar lacunas na aplicação prática da norma.

Na seção destinada ao tratamento de dados pessoais sensíveis, o Art. 11º da LGPD estabelece hipóteses e proibições para que esse tratamento seja realizado, sendo que alguns de seus parágrafos e incisos dependem de regulamentação adicional pela Autoridade Nacional de Proteção de Dados (ANPD). De forma sucinta, o §1º do referido artigo dispõe que as disposições contidas no Art. 11º aplicam-se a qualquer tratamento de dados pessoais que revele dados sensíveis e que possa acarretar danos ao titular, ressalvadas as exceções previstas em legislação específica.

A concepção de dados pessoais sensíveis começou a ganhar maior atenção e relevância a partir de 1980, com a publicação das *Diretrizes sobre a Proteção da Privacidade e o Fluxo Transfronteiriço de Dados Pessoais*[104] pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE). As diretrizes da OCDE, embora não vinculativas, sugeriram que os países membros incorporassem o conceito de dados sensíveis em suas legislações nacionais de proteção de dados. No entanto, elas não forneceram uma definição detalhada nem especificaram claramente quais dados deveriam ser classificados como sensíveis. A compreensão predominante foi a de que não seria viável estabelecer um conjunto de dados que pudesse ser considerado sensível de forma universal.[105]

Recordemos que, quando da promulgação da LGPD, já existiam precedentes na legislação brasileira sobre a proteção de dados sensíveis, especialmente em normas setoriais como as da saúde e das relações de trabalho. No entanto, é imprescindível salientar que **nem todo dado é, por natureza, sensível — mas pode se tornar sensível em razão do contexto ou da forma como é tratado**. O princípio da finalidade e da contextualização do tratamento de dados é fundamental nesse entendimento.

---

[104] MCCULLAGH, K. Data Sensitivity:Proposals for Resolving the Conundrum, Journal of International Commercial Law and Tecnology 2, 2007, p.190-201.

[105] Disponívelem:http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandransborderflowsofpersonaldata.htm . Acesso em 29 de dez. de 2024.

Utilizando da colocação de Junquilho (2022) ao Citar: “Meu País. Meu lugar de fala”[106], traz uma afirmação, carregada de identidade e pertencimento e convida à reflexão sobre as múltiplas vozes silenciadas ao longo da história brasileira — entre elas, a das mulheres. No Brasil, as desigualdades sociais se entrelaçam de forma complexa com marcadores de gênero, raça e classe. Quando se analisa a inserção das mulheres no mercado de trabalho[107], especialmente em cargos de liderança[108], torna-se evidente o desequilíbrio estrutural que ainda rege os espaços de poder. A desigualdade de gênero no recrutamento é alimentada por estereótipos culturais profundamente arraigados, que associam qualidades como autoridade, racionalidade e firmeza ao universo masculino. Ao proteger, ocultando o gênero do(a) candidato(a), teríamos resultados igualitários?[109]

Reconhecer a desigualdade de gênero como um problema estrutural é o primeiro passo para enfrentá-lo. Como nos lembra a citação inicial, ocupar o lugar de fala é reivindicar também o direito de transformar a realidade. No entanto, essa transformação exige não apenas ações afirmativas, mas também uma revisão crítica das estruturas legais e institucionais que moldam o tratamento de dados e a formulação de políticas públicas. Embora existam diversas campanhas isoladas promovendo igualdade de gênero[110], diversidade e inclusão — muitas delas conduzidas por empresas, organizações da sociedade civil e até mesmo por órgãos públicos — essas iniciativas, embora importantes, muitas vezes não são sustentadas por uma base normativa sólida que garanta sua continuidade, fiscalização e efetividade.

Um exemplo emblemático dessa lacuna é a ausência da categoria “gênero” como dado pessoal sensível na Lei Geral de Proteção de Dados Pessoais (LGPD), a inexistência de gênero dessa lista suscita questionamentos importantes: como proteger, com o devido rigor, dados que podem ser essenciais para diagnosticar e combater desigualdades estruturais no ambiente de trabalho e na sociedade como um todo? A ausência da categoria “gênero” como dado pessoal

[106]JUNQUILHO, A.TAINÁ “O que se cala” – Canção de Elza Soares, 2018. Para ouvir: https://www.letras.mus.br/elza-soares/o-que-se-cala/

[107] Desafios da mulher no mercado de trabalho: desigualdade de gênero e racismo persistem. Disponível em: https://www.gov.br/trabalho-e-emprego/pt-br/noticias-e-conteudo/2025/marco/desafios-da-mulher-no-mercado-de-trabalho-desigualdade-de-genero-e-racismo-persistem. Acesso em 14 de março de 2025.

[108] Relatório Global sobre a Desigualdade de Gênero 2024 Disponível em: https://www.weforum.org/publications/global-gender-gap-report-2024/. Acesso em 14 de março de 2025.

[109] Recrutamento às cegas aumenta diversidade nas empresas. Disponível em: https://forbes.com.br/carreira/2018/11/recrutamento-as-cegas-aumenta-diversidade-nas-empresas/. Acesso em 14 de março de 2025.

[110] Crescem iniciativas que promovem igualdade de gênero no ambiente de trabalho, aponta estudo.Disponível em: https://portal.fgv.br/noticias/crescem-iniciativas-promovem-igualdade-genero-ambiente-trabalho-aponta-estudo. Acesso em 14 de março de 2025.

sensível na Lei Geral de Proteção de Dados (LGPD) revela uma fragilidade nesse cenário. A legislação atual reconhece como sensíveis dados que, por sua natureza, expõem o indivíduo a maiores riscos de discriminação. A não inclusão expressa do gênero nessa lista levanta uma questão fundamental: como proteger dados que são essenciais para identificar desigualdades estruturais, como a exclusão de mulheres e pessoas trans em espaços de poder, sem o devido reconhecimento legal de sua sensibilidade? Caberá ao Controlador de dados pessoais individualmente ter essa sensibilidade e considerar Gênero como dado pessoal sensível?

Nesse sentido, questiona-se: assim como o GDPR, que, em seu considerando, estabelece diretrizes claras sobre a abrangência e possível abertura do rol de dados pessoais sensíveis, a LGPD poderia ter criado elementos decisórios mais precisos sobre essa categoria, evitando que ficasse a cargo de interpretações subjetivas? A LGPD deveria ter, de maneira transparente, abordado os danos e seus efeitos sociais, como exige dos controladores a transparência com os titulares dos dados? Se a resposta for sim, seria esclarecido o que constitui efetivamente dados sensíveis, mas também os possíveis danos decorrentes de seu tratamento. Além disso, seria essencial incluir a possibilidade de ampliação dessa categoria, conforme avaliação constante em um relatório de impacto à proteção de dados pessoais, garantindo uma adaptação contínua às mudanças sociais e aos riscos emergentes.

A análise comparativa entre o GDPR da União Europeia e a LGPD do Brasil revela uma série de questões fundamentais sobre a proteção de dados pessoais sensíveis, tanto no que diz respeito à definição desses dados quanto aos mecanismos legais para sua salvaguarda. Ambos os regulamentos reconhecem a necessidade de uma proteção mais rigorosa para dados sensíveis devido aos riscos que seu tratamento inadequado pode acarretar aos direitos e liberdades fundamentais dos indivíduos. No entanto, ao comparar as abordagens, notam-se lacunas e diferenças significativas, especialmente no que tange à clareza da definição e à abrangência dos dados sensíveis, bem como à flexibilidade de adaptação às novas tecnologias e contextos sociais.

3.2. A Sensibilidade de Dados Pessoais: Perspectivas Comparativas entre os Sistemas Jurídicos de outros países

A proteção de dados pessoais, particularmente aqueles considerados sensíveis, tornou-se um dos temas centrais no cenário jurídico e tecnológico global. A digitalização crescente e a interdependência das economias mundiais ampliaram a complexidade dos desafios relacionados ao tratamento de dados pessoais, exigindo a adoção de regulamentações específicas para garantir os direitos dos indivíduos e mitigar os riscos associados à coleta e uso de informações pessoais.

A análise comparativa visa identificar as semelhanças e diferenças nas definições, categorias e tratamentos dos dados sensíveis, além de discutir o impacto das normas dentro de seus respectivos contextos socioculturais e econômicos.

Em resposta a essa necessidade, diversas jurisdições ao redor do mundo desenvolveram legislações próprias, mas com abordagens que variam consideravelmente, refletindo as diferenças culturais, sociais e jurídicas entre os países, considerando os dados pessoais como sensíveis: Argentina[111] e uruguaia[112] encontra-se a expressão *datos sensibles;* e nas leis: filipina[113], islandesa[114], aparecem como *sensitive personal data/information.*

Embora o conceito de "dados sensíveis" seja amplamente reconhecido nas legislações globais, sua definição e os critérios de tratamento variam conforme a estrutura jurídica de cada país. A União Europeia, através do **GDPR**, apresenta uma definição de categoria especial[115],

---

[111] Ley 25.326(Ley Proteccion de los Datos Personales). Disponível em: https://observatoriolegislativocele.com/datos-personales/ Acesso em 12 de fev.2025. "Art2º (...) "Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual."

[112] Ley nº 18331/2008 (Ley de Proteccion de Datos Personales). Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008 Acesso em 12 de fev. 2025. "Art. 4º "E" Dato sensible: datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual."

[113] REPUBLIC ACT 10173 DATA PRIVACY ACT OF 2012, Disponível em: https://privacy.gov.ph/data-privacy-act/#w13. Acesso em 02 de fev. 2025. " SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;(b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing; (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority."

[114] Act on the Protection of Privacy as regards the Processing of Personal Data, No. 77/2000 of May 10, 2000 as amended by Act No. 90/2001, Act No. 30/2002, Act No. 81/2002 and Act no. 46/2003. Disponível em: https://www.humanrights.is/en/moya/page/act-on-the-protection-of-privacy-as-regards-the-processing-of-personal-data-no-77-2000-of-may-10-2000-as-amended-by-act-no-90-2001-act-no-30-2002-act-no-81-2002-and-act-no-46-2003 . Acesso em 12 de fev. 2025. " Article 7 – Sensitive Personal Data Sensitive personal data shall mean personal data revealing: racial or ethnic origin;political opinions;religious or philosophical beliefs; trade-union membership; data concerning health or sex life; data concerning criminal convictions or the commission of criminal offenses.
The processing of sensitive personal data is prohibited, unless: the data subject has explicitly consented to the processing of such data; processing is necessary for compliance with a legal obligation or for the establishment, exercise, or defense of legal claims; processing is necessary to protect the vital interests of the data subject or another person;processing is carried out in the course of employment or in the context of social security or health care, based on relevant legal provisions;processing is necessary for reasons of substantial public interest, based on legal grounds.The provisions of this article do not apply to processing carried out by public authorities in the course of their duties, when there are other legal grounds for such processing.

definindo-os como os dados sensíveis como informações relacionadas à origem racial ou étnica, opinião política, convicções religiosas ou filosóficas, dados genéticos, dados biométricos, dados de saúde e vida sexual, entre outros. A proteção desses dados é justificada pelo risco de discriminação ou danos irreparáveis aos direitos fundamentais dos indivíduos caso sejam tratados de forma inadequada.

No Brasil, a LGPD adota uma abordagem semelhante, incluindo categorias como dados relacionados à origem racial, saúde, e dados genéticos, mas com uma adição importante: a lei brasileira também classifica como sensíveis dados biométricos. Este aspecto reflete uma preocupação crescente com a segurança e a privacidade de dados altamente pessoais, como impressões digitais e reconhecimento facial, que são amplamente utilizados em processos de autenticação e segurança.

Já a Lei de Proteção de Informações Pessoais de 2013 da África do Sul (PoPIA)[116] define como informação pessoal especial as crenças religiosas e filosóficas, origem étnica e racial, filiação sindical, concepção política, dados de saúde, vida sexual e informação biométrica e antecedentes criminais referentes à suposta prática de infração ou sua apuração.[117]

As diferenças regionais, jurídicas e sociais desempenham um papel crucial na definição do que pode ser abrangido dentro dessa categoria. A legislação da África do Sul, similar a outras legislações, reconhece a necessidade de proteção adicional para dados relacionados a antecedentes criminais. De forma ainda mais abrangente, a California Consumer Privacy Act de 2018 (CCPA)[118] estabelece uma lista expandida de dados pessoais que merecem proteção, os quais são relevantes citar nesta pesquisa: (i) Número de identificação da segurança social, carteira de motorista, carteira de identidade estadual ou passaporte do consumidor;(ii) O login da conta do consumidor, conta financeira, cartão de débito ou número de cartão de crédito em combinação com qualquer segurança necessária ou código de acesso, senha ou credenciais que permitam acesso a uma conta do consumidor;(iii) A geolocalização precisa do consumidor;(iv) A origem racial ou étnica, as crenças religiosas ou filosóficas ou a filiação sindical do consumidor;(v) O conteúdo da correspondência, e-mail e mensagens de texto do consumidor, a menos que a empresa seja o destinatário pretendido da comunicação;(vi) Dados genéticos de um consumidor; (2) (i) O

[116]Protection of Personal Information Act. Disponível em: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf . Acesso em 12 de fev.2025.
[117]Sobre a taxatividade do rol de dados pessoais sensíveis publicado em 13 de jan.2024. Disponível em: https://www.conjur.com.br/2024-jan-13/sobre-a-taxatividade-do-rol-de-dados-pessoais-sensiveis/ Acesso em 12 de fev.2025.
[118] Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em 12 de fev. 2025.

processamento de informações biométricas com a finalidade de identificar exclusivamente um consumidor;(ii) Informações pessoais coletadas e analisadas relativas à saúde do consumidor;(iii) Informações pessoais coletadas e analisadas sobre a vida sexual ou orientação sexual de um consumidor.(traduzido para o português).

A proteção de dados de consumidores sob a CCPA coloca uma **ênfase forte na autonomia** e no controle dos indivíduos sobre suas próprias informações pessoais, algo crucial em um mundo cada vez mais digitalizado. Ao permitir que os consumidores acessem, excluam ou controlem como suas informações são utilizadas, a lei busca **empoderar** os indivíduos e proporcionar maior transparência às empresas que lidam com dados pessoais.

A análise comparativa das legislações de proteção de dados pessoais, em especial os dados sensíveis revelam um panorama global em que, embora exista um reconhecimento universal da importância da privacidade e da proteção contra o uso indevido de dados, as abordagens jurídicas variam significativamente. A definição e o tratamento dos dados sensíveis são moldados pelas especificidades culturais, sociais e econômicas de cada país, refletindo suas prioridades e preocupações.

No contexto da União Europeia, o GDPR estabelece uma categoria rigorosa de proteção para dados sensíveis, com a justificativa de que esses dados podem causar danos irreparáveis ao indivíduo caso sejam mal utilizados. A LGPD no Brasil, por sua vez, adota uma abordagem semelhante, incluindo categorias como dados biométricos, destacando sua relevância no contexto da crescente utilização de tecnologias de autenticação e segurança. Já a PoPIA da África do Sul e a CCPA da Califórnia demonstram uma compreensão ainda mais abrangente da privacidade, incorporando uma ampla gama de dados, desde identificações governamentais até informações financeiras e geolocalização.

Na China, a proteção de dados pessoais é mais voltada para a segurança e o controle social, com a prioridade sendo a regulação do uso de dados para fins estatais e econômicos. Embora a China tenha promulgado a Lei de Proteção de Informações Pessoais (PIPL), a abordagem em relação aos dados sensíveis em seu Art. 28[119] reflete proteção dos direitos individuais, sendo

[119] PIPL 中华人民共和国个人信息保护法 (Zhōnghuá Rénmín Gònghéguó Gèrén Xìnxī Bǎohù Fǎ) (Personal Information Protection Law of the People's Republic of China) Disponível em: https://personalinformationprotectionlaw.com/chapter-ii-rules-for-handling-personal-information/Acesso em: 12 de fev. 2025. “Art.28 Informações pessoais sensíveis referem-se às informações pessoais que podem facilmente levar à violação da dignidade pessoal de pessoas físicas ou ao dano à segurança pessoal ou patrimonial, uma vez vazadas ou usadas ilegalmente, incluindo informações como biometria, crença religiosa, identidades específicas, saúde médica, contas financeiras e paradeiro, e informações pessoais de menores de 14 anos. Os processadores de informações pessoais podem processar informações pessoais confidenciais somente quando tiverem uma finalidade específica e

considerados como dados confidenciais (informações pessoais confidenciais) “(sensíveis)”.

Essas diferenças nas legislações não apenas ilustram a adaptação das normas à realidade de cada país, mas também destacam a evolução da percepção sobre a privacidade. Enquanto na União Europeia e no Brasil há uma forte ênfase na proteção contra discriminação e danos aos direitos fundamentais, legislações como a CCPA colocam um foco significativo no controle do indivíduo sobre seus dados, oferecendo-lhe a capacidade de acessar, excluir e gerenciar suas informações.

Esse movimento sinaliza uma tendência crescente de empoderamento dos indivíduos, detentores dos dados pessoais. À medida que as legislações avançam na regulação do tratamento dessas informações, torna-se imperativo que a sociedade compreenda de maneira mais profunda os direitos relacionados à sua privacidade e ao uso de seus dados e se tornem mais aptos a exercerem controle sobre suas próprias informações e a participar ativamente da construção de um ambiente digital mais seguro e transparente.

3.2.1. Estados Unidos: Abordagens Fragmentadas e Regulamentação Setorial para Dados Pessoais

Nos Estados Unidos, a proteção de dados pessoais sensíveis não é centralizada em uma única legislação, como ocorre no GDPR ou na LGPD. Em vez disso, as leis variam amplamente entre os estados, com alguns adotando leis estaduais de privacidade de dados do consumidor e outros dependendo de regulamentações federais em áreas específicas. Por exemplo, a HIPAA oferece proteção rigorosa para dados de saúde, enquanto a GLBA regulamenta os dados financeiros.

Por outro lado, os **Estados Unidos** adotam uma abordagem fragmentada e menos rigorosa em relação aos dados sensíveis. Embora existam leis federais como a **HIPAA** (Health Insurance Portability and Accountability Act) que regula os dados de saúde, e a **GLBA** (Gramm-Leach-Bliley Act) que trata da privacidade financeira, os Estados Unidos não possuem uma legislação federal única que trate de forma ampla e uniforme da proteção de dados pessoais sensíveis. A abordagem é, em grande parte, baseada na autorregulação e em leis estaduais, com algumas exceções para categorias específicas de dados.

Além disso, a falta de uma legislação nacional única para a proteção de dados pessoais nos Estados Unidos resulta em um ambiente regulatório fragmentado. Vários estados têm adotado suas próprias leis de privacidade, com destaque para legislações como as de California, Colorado

---

necessidade suficiente, e tomarem medidas de proteção rigorosas.”

e Virginia, que oferecem um nível de proteção mais robusto. No entanto, essa abordagem descentralizada gera desafios tanto para as empresas, que precisam se adaptar a diferentes regras conforme sua atuação nos estados, quanto para os consumidores, que podem ter níveis distintos de proteção dependendo de sua localização.

A ausência de uma legislação geral de proteção de dados nos Estados Unidos tem se mostrado um desafio significativo para o mercado digital, dificultando a adaptação das empresas e a definição de diretrizes claras para o tratamento de dados pessoais. David Cohen, CEO do Interactive Advertising Bureau (IAB) dos Estados Unidos, destaca essa dificuldade ao observar:

> "Hoje, temos 19 estados com leis de privacidade de dados em vigor, e todas são diferentes. Há algumas semelhanças entre elas, mas a complexidade delas invariavelmente vai prejudicar o crescimento do mercado. É complicado e caro conseguir cumprir todas as 19 leis estaduais".

Cohen, continua afirmando na mesma oportunidade, que a falta de uma legislação geral sobre o assunto desafia o mercado, que se adapta a diferentes diretrizes: "Estamos há cerca de 10 anos atrasados em relação a isso. Além disso, temos novidades como a IA. É muito difícil criar uma lei para IA quando não temos uma lei básica de privacidade de dados. Então, isso vai se acumular. Estamos tentando aprovar uma lei de privacidade infantil também. É definitivamente um desafio para a indústria acompanhar. Até termos uma lei nacional, acho que as pessoas continuarão a agir da maneira que acreditam ser responsável no mercado".[120]

À medida que as questões relacionadas à privacidade e proteção de dados sensíveis se tornam cada vez mais prementes, observa-se uma tendência crescente de harmonização das legislações em nível global. A União Europeia, com o GDPR, tem se consolidado como um modelo de referência para outras jurisdições, incluindo o Brasil. Nos Estados Unidos, a pressão por uma regulamentação mais uniforme também tem aumentado, com diversos estados implementando suas próprias leis de privacidade e o debate sobre uma possível lei federal ganhando força.

A harmonização entre as legislações internacionais pode representar uma oportunidade para criar um ambiente jurídico mais coeso, simplificando o cumprimento das normas e

[120] Disponível em: https://www.meioemensagem.com.br/midia/lei-privacidade-dados-publicidade-eua - 27 de agosto de 2024. Acesso em 12 de fev. de 2025.

proporcionando maior proteção aos direitos dos indivíduos. Contudo, a adaptação das regulamentações deve respeitar as diferenças culturais e sociais de cada país, assegurando que as leis de privacidade atendam às necessidades e expectativas locais.

A proteção de dados pessoais sensíveis é uma questão complexa que envolve não apenas a definição legal. Enquanto a União Europeia e o Brasil têm adotado uma abordagem mais centralizada e rigorosa para proteger esses dados, os Estados Unidos operam em um cenário de regulação fragmentada, o que levanta questões sobre a eficácia e a equidade na proteção dos indivíduos.

A comparação dessas abordagens destaca a diversidade nas estratégias de privacidade e sugere que, apesar das diferenças, a tendência global é a de fortalecer as proteções para dados pessoais e sensíveis, criando um ambiente regulatório que reflita as novas realidades digitais e as necessidades de privacidade dos indivíduos globalmente.

3.3. Desafios e Oportunidades para a Proteção de Dados Pessoais e Dados Pessoais Sensíveis em uma Perspectiva Global

As diferentes abordagens adotadas por países ao redor do mundo, como o GDPR da União Europeia, a LGPD no Brasil e as legislações em constante evolução nos Estados Unidos, revelam não apenas divergências normativas, mas também contrastes culturais, sociais e políticos que influenciam profundamente o tratamento e a proteção de dados pessoais e sensíveis. Assim, surge a questão central: até que ponto as normas e regulamentos atuais são suficientes para lidar com as especificidades e os desafios impostos por um ambiente digital globalizado? E como equilibrar os benefícios do uso de dados com os direitos dos indivíduos à privacidade e à segurança de forma uniforme e global?

É comum que os indivíduos realizem cadastros online para acessar conteúdos digitais, incluindo plataformas de serviços governamentais, que frequentemente exigem o preenchimento de formulários completos para liberar o acesso a informações específicas.

No mesmo sentido, Iramina (2020, p. 92), ressalta que:

> Em uma sociedade cada vez mais informatizada, na qual o uso de dados se tornou um componente crucial para o comércio, as comunicações e as interações sociais, a proteção de dados pessoais passou a ser uma preocupação para grande parte dos países. Nesse contexto, muitos países

> têm adotado novas regras de proteção de dados ou modernizado as que já tinham, como Coreia do Sul, Chile, Tailândia, Índia, Indonésia e Brasil. Atualmente, já são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo.

Em um mundo cada vez mais globalizado, onde dados circulam entre países e continentes, as diferenças nas legislações podem gerar conflitos de interpretação e aplicação das normas, dificultando a criação de uma regulamentação eficaz e harmonizada. A harmonização, portanto, se torna um objetivo difícil de alcançar, pois envolve não apenas questões legais, mas também o respeito às particularidades culturais e políticas de cada nação.

No entanto, a troca de experiências e a cooperação internacional podem abrir oportunidades para a criação de normas mais flexíveis e adaptáveis, que considerem tanto os direitos fundamentais dos indivíduos quanto as necessidades de desenvolvimento econômico e inovação tecnológica. O que se observa, então, é uma crescente pressão para que as nações adaptem suas legislações de proteção de dados, com uma crescente convergência em torno de normas como as do GDPR e da LGPD, que servem como modelo para países fora da União Europeia e da América Latina.

A sensibilidade de dados é um conceito que transcende as fronteiras legais, exigindo uma análise crítica das diferentes abordagens adotadas ao redor do mundo. As estruturas jurídicas de cada país influenciam diretamente a forma como os dados sensíveis são tratados, sendo o contexto cultural, social e político um determinante crucial para a definição e a aplicação das normas.

Em uma perspectiva global, a convergência de normas de proteção de dados é essencial para garantir que os direitos dos indivíduos sejam adequadamente protegidos, sem prejudicar o potencial de inovação tecnológica e crescimento econômico. A harmonização das abordagens legais, embora desafiadora, é um caminho necessário para construir um ambiente digital seguro, ético e justo, em que a sensibilidade dos dados seja tratada com o cuidado e a responsabilidade que merece.

4. IMPLICAÇÕES PRÁTICAS NA INTERPRETAÇÃO DE DADOS PESSOAIS SENSÍVEIS

4.1. Casos Relevantes e Interpretação da Categoria de dados em situações potencialmente sensíveis

As novas e sofisticadas formas de tratamento de dados têm ampliado as possibilidades de

classificação dos dados pessoais, tornando cada vez mais urgente a reflexão sobre a criação de novas categorias, relações e formas de proteção. Com os avanços tecnológicos e científicos, dados pessoais que antes não eram considerados sensíveis podem, agora, apresentar riscos substanciais aos indivíduos, desafiando as definições tradicionais de dados protegidos. Diante disso, seria o caso de surgirem novas categorias, como os chamados "dados pessoais críticos", que exigiriam um nível elevado de proteção devido ao seu potencial de causar danos significativos à privacidade e aos direitos dos titulares?

O nome, sem dúvida, é um dos meios mais comuns de identificação pessoal. Em uma coletividade, pode haver várias pessoas com o mesmo nome, sendo, muitas vezes, necessário recorrer ao sobrenome para estabelecer uma diferenciação mais precisa. De acordo com a LGPD, o nome não é classificado como dado pessoal sensível, sendo tipicamente considerado um dado geral ou comum em um mapeamento de dados pessoais (ROPA)[121].

É pertinente refletir sobre situações nas quais o nome, embora não classificado como dado sensível, possa ser utilizado como um fator de discriminação ou causar danos ao indivíduo, particularmente quando associado a contextos sociais e históricos que carregam estigmas ou preconceitos. Para ilustrar esse ponto, apresenta-se um exemplo prático que pode facilitar a reflexão sobre como um dado não considerado sensível, ao ser contextualizado, ainda assim pode impactar negativamente o titular dos dados, revelando-se sensível:

“Uma pesquisa revelou que motoristas com o nome Mohammed pagam, em média, £1.000 a mais em seguros de carro do que motoristas com nomes tradicionais ingleses, como John. Grandes empresas de seguros, como Admiral, Marks & Spencer, Bell, Elephant e Diamond, foram envolvidas em uma controvérsia após fornecerem cotações significativamente mais baixas para motoristas com nomes ingleses. A investigação, conduzida pelo jornal The Sun, expôs a prática de diferenciação nos preços de seguros com base no nome dos motoristas, levantando enigmas sobre discriminação implícita em processos de precificação no setor.” “Quando era "John Smith" querendo um seguro totalmente abrangente para um Ford Focus 2007 em Leicester, a cotação era de £ 1.333, as para "Mohammed Ali" foi de £ 2.252 - um enorme £ 919 a mais”[122]

Surge uma questão desconcertante: qual o real motivo por trás da afirmação? O estereótipo de que "Mohammeds" são piores motoristas diz respeito à habilidade no volante ou esconde algo

[121] *Record Of Processing Activities* - que significa Registros das Atividades de Tratamento. Ou seja, são provas de como é feita a coleta de dados, o que é feito com essas informações e como é feita a exclusão, se ocorre.
[122] MO COMPARE Motorists fork out £1,000 more to insure their cars if their name is Mohammed. Disponível em: https://www.thesun.co.uk/motors/5393978/insurance-race-row-john-mohammed/. Acesso em 20 de jan. de 2025.

mais profundo? Seria o ódio a Maomé alimentando esse preconceito, ou estamos tratando de uma visão sutil, que vê o "Mohammed" como inferior por ser estrangeiro? E, por fim, será que a ideia de motoristas ingleses superiores não é apenas mais uma forma de exaltar uma nacionalidade, como se isso garantisse melhor desempenho no trânsito?

Em 2015, uma situação envolvendo determinado pró-reitor da Universidade federal de Santa Maria, que requisitou informações aos programas de pós-graduação da instituição, incluindo uma questão específica sobre a presença de alunos e/ou professores de nacionalidade israelense[123]. A solicitação gerou questionamentos sobre os possíveis impactos dessa coleta de dados na promoção de discriminação. O pedido procurou atender a uma solicitação de acesso à informação (LAI) dirigida à Universidade, por algumas entidades. Doneda e Monteiro analisaram caso que ensejou questionamentos a respeito da razão de seu requerimento e de possíveis tratamentos discriminatórios que poderia promover. Na análise, os autores destacaram:

> [...] "O fato de a informação referente à nacionalidade ter elevado potencial discriminatório – ainda que a nacionalidade não seja comumente considerada em si como uma informação sensível – depreende-se do tratamento sensível que pode ser dado a tal informação, capaz de estigmatizar, classificar, pré-julgar e mesmo comprometer a segurança dos cidadãos afetados. Note-se que a discriminação em razão da procedência nacional é, inclusive, tipificada como crime no Art. 1º da Lei 7.716/1989. Para tal ponderação contribui, igualmente, a motivação discriminatória passível de ser inferida pela série de considerando ao pedido de acesso à informação, ao julgar de forma contundente atos que eventualmente teriam sido praticados pelo Estado de Israel."[124]

Como sabemos, nacionalidade não está inserida na categoria descrita pela LGPD como dado pessoal sensível, todavia, a depender do contexto do uso de dados não sensíveis, igualmente causarão danos ao titular de dados.

E a sua data de nascimento? Um dia extremamente feliz e comemorativo, no documento, é identificador, tão logo de natureza individual, é um dado pessoal de fácil acesso e necessário em

---

[123] PF e MPF apuram suposto racismo contra israelenses na UFSM: Em ofício, UFSM pediu dados sobre a presença de israelenses no campus. Reitor diz que atendeu a pedido feito por entidades em cumprimento de lei. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2015/06/pf-e-mpf-apuram-suposto-racismo-contra-israelenses-na-ufsm.html. Acesso em 20 de jan. de 2025.

[124] DONEDA, Danilo; MONTEIRO, Marília. Acesso à informação e privacidade no caso da Universidade Federal de Santa Maria. Jota, 2 jul.2015. Disponível em: https://www.jota.info/artigos/acesso-a-informacao-e-privacidade-no-caso-da-universidade-federal-de-santa-maria . Acesso em 20 de jan. de 2025.

diversas ocasiões e embora, em princípio, não seja considerada um dado sensível, ela pode ser classificada como tal, uma vez que revela a faixa etária de um indivíduo e, consequentemente, pode ser empregada para justificar práticas discriminatórias.

O etarismo, também conhecido como *ageísmo*[125], refere-se à discriminação e preconceito fundamentados na idade de um indivíduo, seja ele mais jovem ou mais velho. Esse tipo de discriminação afeta profissionais de diferentes gerações, conforme revela uma pesquisa do *Infojobs*,[126] que aponta que 57% dos trabalhadores já vivenciaram algum tipo de preconceito relacionado à sua faixa etária. Profissionais das gerações Y e Z, por exemplo, frequentemente relatam ser subestimados por sua juventude, enquanto membros da Geração X enfrentam desconfiança por parte de colegas mais jovens, que questionam seu profissionalismo.

Esses dados evidenciam como o etarismo se manifesta de maneira distinta entre as faixas etárias, criando um ambiente de trabalho marcado por estigmas que prejudicam tanto a inclusão quanto o desenvolvimento profissional de indivíduos de diferentes idades.

Em entrevista à Agência Brasil, Mórris Litvak, disse: “a relação entre etarismo e mercado de trabalho provoca uma dor muito grande nas pessoas. Isso porque, para muitos, a idade tem um peso grande para que se recoloquem profissionalmente.”[127] (Grifo meu).

O uso indevido dessa informação tem o potencial de gerar danos substanciais ao titular, como a exclusão do mercado de trabalho e a limitação de oportunidades em várias esferas da vida social. Tais práticas não apenas violam os princípios da igualdade e da dignidade, mas também perpetuam um ambiente no qual o indivíduo é marginalizado ou prejudicado unicamente a partir da sua data de nascimento.

Nesse cenário, abre uma questão importante: até que ponto o nome, data de nascimento, nacionalidade etc., em suas funções identificadoras complementares, pode ser um vetor de vulnerabilidade, e não simplesmente uma informação comum? Tal reflexão desafia a visão tradicional da LGPD, que poderia, em determinados contextos, precisar revisar a classificação de dados pessoais para incluir uma camada de proteção mais adaptada às realidades sociais complexas.

---

[125] Etarismo e mercado de trabalho: preconceito etário prejudica a inserção dos 50+. Instituto de Longevidade MAG.2024 Disponível em: https://institutodelongevidade.org/longevidade-e-trabalho/carreira/etarismo-e-mercado-de-trabalho. Acesso em 23 de jan. de 2025.

[126] Disponível em: Etarismo: 57% dos profissionais já sofreram preconceito por causa da idade | Exame Acesso em 23 de jan. de 2025.

[127] Etarismo e mercado de trabalho: preconceito etário prejudica a inserção dos 50+. Instituto de Longevidade MAG.2024 Disponível em: https://institutodelongevidade.org/longevidade-e-trabalho/carreira/etarismo-e-mercado-de-trabalho . Acesso em 23 de jan. de 2025.

Se **interpretado de forma taxativa**, o rol de dados sensíveis se tornaria restrito, significando que somente as categorias listadas pela LGPD seriam consideradas sensíveis, sem a possibilidade de incluir novos tipos de dados sob essa classificação. Esse enfoque tem alguns aspectos positivos: primeiro, oferece clareza e segurança jurídica no tratamento de dados, pois fica evidente quais dados exigem um tratamento mais rigoroso e quais não se enquadram nessa categoria. As empresas poderiam se concentrar em adaptar suas práticas de proteção de dados a essas categorias específicas, simplificando o processo de conformidade. No entanto, a abordagem taxativa também apresenta limitações. A evolução constante das tecnologias e das formas de tratamento de dados poderia tornar esse rol obsoleto, já que novos tipos de dados poderiam surgir com o tempo, sem que estivessem devidamente protegidos pela legislação. Além disso, a interpretação restritiva poderia criar lacunas na proteção de dados que, apesar de não estarem explicitamente listados na lei, ainda assim possuem características sensíveis e merecem um tratamento mais cuidadoso.

Por outro lado, **se o rol for exemplificativo**, a legislação poderia ser interpretada de maneira mais flexível, permitindo a inclusão de novos tipos de dados sensíveis conforme a sociedade, a tecnologia e a jurisprudência evoluíssem. Essa abordagem tem vantagens consideráveis, pois proporciona maior adaptabilidade à lei. Novos dados que apresentem riscos elevados à privacidade poderiam ser automaticamente reconhecidos como sensíveis, sem a necessidade de alterações legislativas. Além disso, essa flexibilidade permite uma proteção mais abrangente e dinâmica, cobrindo não apenas os dados listados de forma explícita, mas também outros que, com o tempo, poderiam se revelar igualmente “perigosos” para os direitos dos titulares.

Entretanto, a interpretação exemplificativa traz desafios práticos. Ela pode gerar insegurança jurídica para as empresas, que ficariam na incerteza sobre quais dados deveriam ser considerados sensíveis em determinadas situações. Além disso, essa flexibilidade poderia levar a interpretações divergentes, tanto por parte das autoridades regulatórias quanto dos tribunais, tornando o cumprimento da legislação mais complexo e sujeito a diferentes entendimentos. Isso pode aumentar a carga de compliance das empresas, que precisariam realizar uma análise

constante sobre a natureza dos dados coletados e tratados. Prática recomendada para a garantia dos direitos fundamentais.

Essas duas abordagens apresentam benefícios e limitações, e a escolha entre elas exige um equilíbrio entre a proteção eficaz da privacidade dos indivíduos e a necessidade de garantir clareza e previsibilidade para as empresas. A reflexão sobre a classificação de dados como sensíveis, especialmente à luz de casos como os discutidos neste tópico, revela a complexidade e a dinâmica

que a proteção de dados exige em um mundo cada vez mais digital e interconectado.

Dessa forma, a LGPD deve ser vista como um ponto de partida para a construção de um marco legal que não apenas proteja os dados sensíveis de forma rigorosa, mas também se adapte às necessidades de um contexto social em constante transformação. O futuro da proteção de dados, especialmente no que diz respeito aos dados sensíveis, dependerá da capacidade do sistema jurídico de evoluir e se ajustar às novas realidades, sempre com o objetivo de resguardar a privacidade e os direitos fundamentais dos cidadãos.

4.2. Classificação e Gestão de Dados Sensíveis: O Desafio da Ambiguidade e da Evolução do Conceito

A classificação e gestão de dados sensíveis representam um dos maiores desafios contemporâneos no campo da proteção de dados pessoais. Embora o conceito de dados sensíveis tenha sido consagrado em legislações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a ambiguidade na definição e a evolução das tecnologias e práticas de coleta e tratamento de dados dificultam a compreensão e implementação efetiva das normas. Este tópico busca analisar a complexidade dessa classificação, refletindo sobre as ambiguidades do conceito de dados sensíveis e como ele evolui frente às novas demandas sociais, tecnológicas e jurídicas.

O conceito de dados sensíveis, conforme expresso em normas como o artigo 9º do GDPR e o artigo 11º da LGPD, abrange categorias de dados que, por sua natureza, merecem proteção reforçada devido ao potencial impacto que seu tratamento inadequado pode ter sobre os direitos e liberdades fundamentais dos indivíduos. Tais dados envolvem informações sobre a origem racial ou étnica, convicções religiosas, opiniões políticas, dados genéticos, biométricos, entre outros.

No entanto, a identificação de quais dados devem ser considerados sensíveis ainda gera ambiguidades. A definição legal é, em muitos casos, limitada a uma lista taxativa de categorias, mas a realidade dinâmica das interações digitais e do comportamento humano nos ambientes virtuais desafia essa rigidez.

Os dados que, em um contexto, não são considerados sensíveis podem adquirir tal natureza em outro, dependendo da forma como são tratados, combinados ou utilizados. Um exemplo disso pode ser visto nas informações relacionadas à saúde de um indivíduo: em um contexto médico, tais dados são claramente sensíveis, enquanto em uma campanha de marketing direcionado,

poderiam ser utilizados sem essa classificação. Isso nos leva a uma questão crucial: como assegurar que a classificação de dados sensíveis seja ao mesmo tempo precisa e eficaz, evitando que se torne excessivamente restritiva ou, por outro lado, permissiva demais? No entanto, ao refletirmos mais profundamente sobre o tema, surge a reflexão fundamental: realmente precisamos dessas classificações, quando estamos diante de uma transição paradigmática em que qualquer dado pessoal, dependendo do seu tratamento, pode acabar gerando contextos discriminatórios? Assim, a verdadeira questão não é apenas estabelecer categorias rígidas, mas compreender que a sensibilidade dos dados pode emergir a partir do contexto e do uso a que são submetidos.

A evolução das tecnologias de coleta e análise de dados, especialmente com o avanço da inteligência artificial (IA) e o uso de algoritmos de perfilamento, criou desafios para a definição e a gestão dos dados sensíveis. As inovações tecnológicas permitem a obtenção de dados antes considerados irrelevantes ou neutros, que, quando combinados com outras informações, podem revelar aspectos sensíveis da vida de uma pessoa, como suas preferências políticas, comportamentos de consumo, ou até sua saúde mental e emocional.

Além disso, a criação de perfis comportamentais detalhados, que identificam tendências, hábitos e comportamentos, amplia as fronteiras do conceito de dados sensíveis. Por exemplo, com a coleta massiva de dados sobre preferências de compra e navegação na internet, as empresas podem criar perfis tão precisos que conseguem prever, com grande precisão, o comportamento futuro dos indivíduos. Isso levanta uma questão jurídica e ética: esses dados, que por sua própria natureza não seriam sensíveis, tornam-se classificados como tal quando usados para traçar perfis altamente detalhados que invadem a esfera privada dos indivíduos?

Essa evolução do conceito também exige um olhar mais atento sobre as definições legais. A proteção de dados sensíveis não pode ser tratada de forma estática, mas sim adaptativa, considerando o impacto da inovação tecnológica sobre a privacidade e os direitos dos indivíduos. Os reguladores devem estar preparados para revisar e atualizar continuamente as definições de dados sensíveis, para que possam refletir as novas realidades tecnológicas e sociais, sem comprometer a proteção dos direitos fundamentais dos indivíduos.

O caminho para uma gestão eficiente de dados sensíveis depende de uma constante revisão das práticas e conceitos, com base em uma análise crítica das implicações éticas, jurídicas e sociais. Só assim poderemos garantir uma proteção robusta, que não apenas se adapte às mudanças tecnológicas, mas também promova o respeito pela dignidade humana em um mundo cada vez mais conectado e digital.

4.2.1. Contribuições para uma análise baseada no princípio da dignidade da Pessoa Humana

Uma análise fundamentada no princípio da dignidade da pessoa humana oferece um ponto de partida crucial para a compreensão e aplicação dos direitos e garantias relacionados à proteção de dados pessoais. Este princípio, que ocupa uma posição central nas constituições democráticas modernas, incluindo a Constituição Brasileira, pressupõe o respeito à autonomia e à privacidade do indivíduo, elementos essenciais para a preservação da sua dignidade.

A dignidade humana, enquanto valor supremo[128], exige que os indivíduos sejam tratados com respeito e tenham sua privacidade protegida em todas as esferas da vida social, seja na interação com empresas, governo ou outros indivíduos. A coleta, o uso e o armazenamento de dados pessoais, quando realizados de forma transparente, consentida e informada, são compatíveis com esse princípio. No entanto, a utilização excessiva ou indiscriminada desses dados, sem a devida proteção, pode resultar em um cenário onde a dignidade da pessoa seja comprometida, seja pela discriminação, seja pela invasão de sua privacidade.

O princípio da dignidade da pessoa humana e o direito fundamental à proteção de dados pessoais são dois pilares essenciais na construção de sistemas jurídicos contemporâneos, especialmente no que se refere à proteção de direitos individuais em um contexto de crescente digitalização e interconexão. A interligação entre esses dois conceitos é fundamental, pois ambos visam preservar e promover a autonomia, a liberdade e a privacidade do indivíduo, elementos essenciais para a integridade e o bem-estar humano. No entanto, a forma como esses direitos são compreendidos e aplicados pode variar significativamente de acordo com a ordem jurídica e o contexto cultural e social de cada país.

A LGPD também reconhece a efetivação e a promoção dos direitos humanos fundamentais

[128] MORAES, Maria Celina Bodin de. Danos à pessoa humana: uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003, p.121.

como justificativa para a tutela dos dados pessoais[129] (Art. 2º, VIII).[130]

O princípio da não discriminação deve se manifestar sempre que o uso de dados, sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam inequitativos. Esse princípio deve servir de sustentação para a tutela dos dados sensíveis, especialmente em se tratando do exercício de direitos sociais, como o trabalho, a saúde, a moradia e a educação.[131]

Roger Raupp, formula um conceito constitucional de discriminação, reportado a "qualquer distinção, exclusão, restrição ou preferência que tenha o proposito ou o efeito de anular ou prejudicar o reconhecimento, gozo ou o exercício em pé de igualdade de direitos humanos e liberdades fundamentais nos campos econômico, social, cultural ou em qualquer campo da vida pública.[132]

O ordenamento jurídico civil-constitucional deve agir como um contrapeso às dinâmicas do mercado, que, segundo Stefano Rodotà, fragmentam a unidade da pessoa. Em vez de uma pessoa íntegra, surgem as "pessoas eletrônicas", cujas múltiplas existências são moldadas pelos interesses econômicos que incentivam a coleta de dados. Como destaca Rodotà, "estamos nos tornando 'abstrações no cyberspace', e, mais uma vez, nos vemos diante de um indivíduo 'multiplicado'. Contudo, essa multiplicação não ocorre por escolha do indivíduo, nem pela vontade de assumir várias identidades, mas sim como uma forma de reduzi-lo à lógica das relações mercadológicas."[133]

Para além do marco regulatório, a sociedade brasileira precisa investir em educação digital e na conscientização dos cidadãos sobre seus direitos em relação à proteção de dados. Somente com um ambiente mais informado e crítico será possível garantir que todos, especialmente os mais vulneráveis, possam usufruir da tecnologia de maneira equitativa e com plena proteção de sua privacidade. A dignidade da pessoa humana só será plenamente respeitada quando todos os

---

[129] LUCCA, Newton de; MARTINS, Guilherme Magalhães. Direitos fundamentais e sociedade tecnológica.,São Paulo, Foco 2022 p. 4.

[130] Em importante precedente coletivo, relacionado à biometria na linha 4 do metrô de São Paulo, o tribunal de justiça de são Paulo considerou a responsabilidade objetiva do agente de tratamento (TJSCP, ACP 1090663-42.2018.8.26.0100, 37ª Vara Cível – Foro Central Cível, j. 07.05.2021). Com a seguinte ementa: Proibição da coleta e tratamento de imagens e dados biométricos tomados, sem prévio consentimento, de usuários das linhas de metrô 4. A Ré confessa que há detecção da imagem dos usuários, usada para fins estatísticos, mediante o uso de algoritmos computacionais. CDC, publicidade enganosa e abusiva – métodos comerciais coercitivos ou desleais – art. 6, III e IV. Art. 31, CDC, informações corretas, claras e precisas, ostensivas. Danos morais coletivos arbitrados em R$ 1000.0000,00.

[131] MULHOLLAND, Caitlin. A tutela dos dados pessoais sensíveis. In MULHOLLAND, Caitlin (org) A LGPD e o novo marco normativo no Brasil. Arquipelogo, 2020, p. 124.

[132] RIOS, Roger Raupp. Direito da antidiscriminação; discriminação direta, indireta e ações afirmativas, Porto Alegre; Livraria do Advogado 2008, p.20-21.

[133] RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Org, seleção e apresentação Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro. Renovar, 2008, p. 125.

indivíduos, independentemente de sua classe social, raça, gênero ou origem, puderem viver sem o temor de que seus dados pessoais sejam usados para perpetuar ciclos de desigualdade.

Em última análise, é urgente que a sociedade, o Estado e as empresas adotem uma postura ética e responsável na gestão dos dados pessoais. A proteção de dados não é apenas uma questão de segurança da informação, mas uma **questão de justiça social**, onde a dignidade do ser humano é a prioridade máxima. Somente assim poderemos criar um futuro mais justo, inclusivo e igualitário, onde o uso da tecnologia seja uma ferramenta para a promoção da liberdade, da igualdade e dos direitos fundamentais de todos os cidadãos.

Portanto, o verdadeiro avanço na proteção da dignidade da pessoa humana passa pela valorização da privacidade e pela defesa intransigente dos direitos relacionados aos dados pessoais, promovendo um futuro em que cada cidadão tenha o controle de sua identidade e das informações que definem sua existência, sem que sua intimidade seja exposta ou usada para perpetuar ciclos de desigualdade ou exclusão social. Este é, sem dúvida, um caminho para uma sociedade mais justa, equitativa e, sobretudo, digna.

4.3. Desafios práticos para Profissionais de Proteção de Dados Pessoais e Empresas

A proteção de dados pessoais, em especial os dados sensíveis, representa um dos maiores desafios para as empresas e profissionais de privacidade no cenário atual. Com a promulgação da LGPD, as organizações se viram diante de um marco regulatório que impõe a necessidade de adequação de suas práticas de tratamento de dados pessoais, o que, embora categórico para garantir os direitos dos indivíduos, também apresenta obstáculos significativos na implementação de conformidade com as exigências da legislação. Este tópico aborda os principais desafios práticos enfrentados por empresas e profissionais especializados em proteção de dados pessoais, considerando tanto os aspectos normativos quanto os operacionais, e como a categoria de dados sensíveis, especialmente, impõe questões ainda mais complexas.

Como dito por Bruno Bioni: “Regulação de Dados é uma janela de oportunidade”[134].O autor segue mencionando que ainda é comum se referir a LGPD enquanto um espantalho. Seria mais uma regulação, dentre tantas outras já existentes, que travaria a economia e a inovação no país. O pessimismo é destilado por meio do medo. Quem não estiver em conformidade com a nova legislação amargará prejuízos de até R$ 50 milhões, uma das suas penalidades previstas [...].[135]

[134] BIONI, Bruno R. Regulação de dados é uma janela de oportunidade. Jornal Valor Econômico, 29 de mar. 2019. Acesso em 30 de jan. de 2025.
[135] BIONI, Bruno R. Proteção de dados:contexto, narrativas e elementos fundantes/1º ed. – Curitiba: Appris, 2022.p.57.

A LGPD parte da premissa de que toda organização deve não só conhecer os dados que possui, mas sobretudo, convertê-los em uma informação útil. Todo o sistema gira em torno da lógica de se criar uma trilha auditável do dado, pela qual o cidadão e os demais agentes de econômicos enxerguem todo o seu ciclo de vida e principalmente a sua repercussão nas atividades económicas e relações sociais de que fazem parte. A "nova lei, não veio para travar o fluxo informacional, mas, muito pelo contrário, estimulá-lo dentro de uma lógica de sustentabilidade entre quem produz essa matéria prima e quem a explora." [136]

Com a crescente pressão para a transparência, as empresas precisam equilibrar a necessidade de coletar e divulgar dados com a obrigação de proteger as informações pessoais de seus clientes e funcionários. Além disso, a ascensão das mídias sociais e tecnologias inovadoras intensifica o risco de vazamento de dados pessoais, exigindo estratégias robustas de segurança cibernética e a implementação de práticas claras de consentimento e controle sobre os dados compartilhados. Isso torna ainda mais difícil garantir que as informações sejam utilizadas de forma ética e legal, sem comprometer a privacidade dos indivíduos.

A primeira grande dificuldade está na necessidade de reestruturação dos processos internos das empresas para garantir que todas as operações de tratamento de dados, especialmente os sensíveis, estejam em conformidade com os princípios da LGPD, como a transparência, a finalidade, e a minimização de dados.

O segundo grande desafio está no princípio da segurança da informação, que é um dos pilares da LGPD, e as empresas têm a obrigação de adotar medidas técnicas e administrativas para proteger os dados pessoais e sensíveis contra acessos não autorizados, vazamentos, e outras formas de violação. No entanto, garantir a segurança desses dados sem comprometer sua acessibilidade e usabilidade é um desafio constante. A implementação de sistemas de segurança robustos, como criptografia[137], autenticação multifator[138] e monitoramento contínuo, exige recursos financeiros e humanos substanciais. A grande dificuldade para as empresas é encontrar um equilíbrio entre a proteção dos dados e a operação eficiente dos processos de negócios.

Além disso, o aumento das ameaças cibernéticas e a constante evolução das técnicas de

[136] BIONI, Bruno R. Proteção de dados:contexto, narrativas e elementos fundantes/1º ed. – Curitiba: Appris, 2022.p.57.
[137] A criptografia é usada para proteger os dados contra roubo, alteração ou comprometimento e funciona transformando os dados em um código secreto que só pode ser desbloqueado com uma chave digital exclusiva.
[138] A autenticação multifator (MFA) é um processo de login de conta com várias etapas que obriga o usuário a inserir informações que vão além de uma simples senha.

ataque, como *ransomware*[139], *phishing*[140] e ataques de engenharia social[141], coloca as empresas sob uma pressão contínua para atualizar suas medidas de segurança. Para os profissionais da área, o monitoramento das ameaças e a manutenção de uma infraestrutura de proteção adequada são tarefas desafiadoras que exigem constante vigilância, atualização e investimento.

O terceiro desafio é a exigência trazida pela LGPD, que o consentimento seja não apenas explícito, mas também facilmente revogável a qualquer momento. A revogação do consentimento precisa ser simples e acessível ao titular, o que exige que as empresas criem sistemas eficazes para rastrear e gerenciar as escolhas de consentimento ao longo do tempo. Quando um titular decide revogar seu consentimento, a empresa deve ser capaz de garantir que os dados sejam apagados ou anonimizados, o que demanda processos claros e transparentes, salvo recusa justificada e legal.

Em vista disso, surge uma reflexão primordial: ao mesmo tempo em que a LGPD busca garantir que o tratamento de dados pessoais sensíveis seja realizado com respeito à privacidade, a realidade é que a prática do consentimento no cotidiano pode ser mais complicada do que imaginamos. Como as empresas conseguem equilibrar a necessidade de tratar dados pessoais com a responsabilidade de obter e gerenciar consentimentos claros e transparentes, enquanto os titulares nem sempre têm plena consciência do que isso envolve? Esse desafio operacional reflete uma tensão constante entre o direito dos indivíduos à privacidade e a necessidade das empresas de utilizar dados pessoais para atividades essenciais e cotidianas.

É preciso conscientização e treinamento contínuo, mas um quarto desafio para os profissionais de privacidade e fazer com que a governança de dados, especialmente em organizações de grande porte, onde diferentes áreas lidam com dados sensíveis de formas variadas, estejam com processos mapeados, com as devidas bases legais e em conformidade jurídica. Muitas vezes, a falta de consciência sobre a importância de práticas adequadas de proteção de dados leva à não conformidade com a LGPD, expondo a empresa a riscos legais e

---

[139] *Ransomware* é um tipo de software malicioso (malware) projetado para bloquear ou criptografar arquivos no sistema de uma vítima, impedindo o acesso a esses arquivos. O atacante exige um resgate (geralmente em criptomoeda) para liberar a chave de descriptografia ou devolver o acesso aos dados. Este tipo de ataque pode afetar empresas e indivíduos, causando perda de dados importantes e impactos financeiros significativos. O ransomware pode ser espalhado por e-mails de phishing, downloads maliciosos ou vulnerabilidades no sistema.

[140] *Phishing* é uma técnica de ataque cibernético em que o criminoso tenta enganar a vítima para que ela forneça informações confidenciais, como senhas, números de cartão de crédito ou dados bancários, por meio de mensagens fraudulentas. Essas mensagens frequentemente parecem ser de fontes confiáveis, como bancos ou empresas legítimas, e geralmente incluem links ou anexos que, quando clicados, redirecionam o usuário a sites falsificados ou infectam o sistema com malware. O phishing pode ocorrer via e-mail, mensagens de texto ou redes sociais.

[141] Ataques de engenharia social são táticas que exploram a manipulação psicológica das pessoas para obter informações confidenciais ou para induzi-las a tomar ações prejudiciais, como clicar em links maliciosos ou fornecer senhas. Diferente de ataques técnicos, os ataques de engenharia social dependem da interação humana e geralmente exploram características como confiança, curiosidade ou medo. Exemplos incluem phishing, pretexting (onde o atacante finge ser alguém de confiança para obter dados) e baiting (onde o atacante oferece algo tentador em troca de informações).

danos à reputação. O grande obstáculo é como engajar e garantir que todos na organização compreendam, de forma clara e constante, a importância de uma governança eficaz, sem deixar que o tempo e a falta de interesse dificultem essa mudança cultural dentro das empresas.

Na sociedade contemporânea, a transparência tem sido elevada à condição de virtude moral[142], sendo constantemente promovida como um valor essencial tanto nas esferas pessoais quanto profissionais. Os indivíduos são incitados a manter uma postura de total abertura, ocultando apenas aquilo que possa ser considerado constrangedor ou vergonhoso. Esse fenômeno é, em grande medida, impulsionado pela ascensão das mídias sociais, que possibilitaram, de maneira inédita, o compartilhamento de informações pessoais com um público vasto e acessível.

Em meio ao crescente desafio de garantir a privacidade dos dados pessoais na sociedade contemporânea, surge uma reflexão primordial sobre como falar de privacidade em um cenário onde a cultura de proteção de dados ainda não está plenamente enraizada nas pessoas e na sociedade? A LGPD estabelece requisitos rigorosos, mas a verdade é que a conscientização e a implementação desses princípios ainda encontram barreiras significativas, especialmente em um contexto cultural onde a transparência muitas vezes se sobrepõe à privacidade, e a gestão de dados pessoais ainda é vista por muitos como uma tarefa secundária.

Como é possível, então, ser ouvido nas organizações quando a cultura de proteção de dados pessoais não está ainda incorporada ao cotidiano individual? A verdade é que a urgência da implementação de boas práticas de governança de dados, entra em conflito com a falta de tempo e de interesse de muitos em tratar a privacidade como uma prioridade real. Isso se reflete na resistência à mudança pessoal e na dificuldade em adotar uma abordagem contínua de capacitação e conscientização.

Neste cenário, o desafio é duplo: por um lado, há a necessidade de garantir que as empresas se ajustem a um marco regulatório exigente e, por outro, é preciso encontrar maneiras eficazes de envolver as pessoas – tanto dentro das organizações quanto na sociedade – na causa da privacidade. Não basta que as leis sejam estabelecidas, é necessário que as pessoas realmente compreendam suas implicações e se sintam responsáveis pela proteção dos seus dados pessoais. Isso só será possível quando a governança de dados for integrada à cultura social e organizacional de forma clara e constante, o que, por sua vez, exige um esforço conjunto entre os profissionais da área de privacidade e todos os membros de uma organização.

[142] Byung-Chul Han, Sociedade da transparência, tradução de Enio Paulo Giachini, Petrópolis, RJ: Vozes, 2017.

Portanto, a reflexão que fica é: como podemos, de fato, fazer da privacidade uma prioridade em um contexto em que a transparência é amplamente celebrada, mas a incompreensão dificulta a implementação eficaz de práticas de proteção de dados? É uma mudança de mentalidade, que deve ser externa: Pessoas conscientes, levam consciência por onde andarem. É preciso educação!

5. CONSIDERAÇÕES FINAIS

A análise da privacidade e da proteção de dados pessoais, especialmente no contexto da transformação digital, revela a importância crítica dessas questões para a sociedade contemporânea. A privacidade, um direito humano fundamental, tem se expandido nas últimas décadas para englobar a proteção de dados pessoais, reflexo direto da digitalização crescente das interações sociais e econômicas.

Nesse processo, a interconexão entre esses dois conceitos — privacidade e proteção de dados — torna-se cada vez mais evidente e necessária, não apenas no contexto de normativas locais, mas também na construção de um ambiente jurídico global que consiga equilibrar a proteção dos direitos fundamentais com o avanço da tecnologia. Este estudo abordou de maneira detalhada as implicações e desafios presentes nesse cenário, com destaque para as lições aprendidas na Europa com o Regulamento Geral de Proteção de Dados (GDPR) e sua aplicação no Brasil com a Lei Geral de Proteção de Dados (LGPD).

A construção do GDPR na União Europeia representa um marco regulatório fundamental que influenciou diretamente legislações em todo o mundo, incluindo a LGPD. No entanto, a comparação entre essas legislações revela tanto avanços quanto desafios comuns. A transição da proteção de dados pessoais para o foco nos dados sensíveis ilustra bem esses desafios, uma vez que a definição de dados sensíveis continua sendo um tema complexo, com implicações profundas tanto do ponto de vista jurídico quanto social.

O debate no Brasil sobre se o rol de dados sensíveis deve ser exemplificativo ou taxativo ilustra o dilema constante entre garantir segurança jurídica e, ao mesmo tempo, assegurar uma proteção robusta aos direitos dos indivíduos. Esse dilema reflete a dificuldade de conciliar a necessidade de clareza nas normas com a realidade dinâmica e mutável dos riscos tecnológicos, que, por sua natureza, são frequentemente imprevisíveis.

Uma das questões centrais no debate sobre a proteção de dados pessoais é a classificação dos dados sensíveis. Estes dados, conforme abordados sob diversas perspectivas jurídicas, sociais e tecnológicas, trazem à tona um conjunto de desafios práticos e éticos. A necessidade de adaptação das empresas e profissionais a essas novas realidades normativas demanda um esforço contínuo para harmonizar a inovação com a proteção dos direitos fundamentais. A gestão e classificação de dados sensíveis, em contextos em que as fronteiras entre o que constitui um dado pessoal e um dado sensível nem sempre são claras, exigem não só o rigor na aplicação das normativas, mas também uma reflexão sobre o papel da privacidade e da dignidade da pessoa humana. Este princípio, que deve ser um norte para as políticas de proteção de dados, assegura

que as práticas de tratamento de dados não comprometam os direitos individuais em nome de interesses econômicos ou tecnológicos.

Ao refletir sobre a definição de dados pessoais, observa-se que qualquer dado que identifique uma pessoa natural pode ser considerado um dado pessoal. No entanto, a classificação de um dado como sensível ou não depende, em grande parte, do contexto em que ele é utilizado. Essa constatação, a partir de um entendimento expansionista, à luz da dignidade da pessoa humana, reforça a importância de ampliar a definição de dados sensíveis, considerando o impacto que o uso indevido ou a exposição desses dados pode ter sobre a dignidade dos indivíduos. A ampliação do rol de dados sensíveis, além de ser uma medida de segurança jurídica, também se configura como uma estratégia de proteção dos direitos fundamentais.

A proteção de dados pessoais, portanto, transcende a aplicação técnica ou jurídica das normas. Ela representa uma responsabilidade social e ética das instituições, que devem operar de maneira transparente e responsável. Em um cenário onde a confiança da sociedade depende da forma como as informações pessoais são tratadas, a conformidade com as normas de proteção de dados torna-se um fator determinante para a legitimidade e a sustentabilidade das organizações. Isso é particularmente relevante em um contexto em que os avanços tecnológicos não param de desafiar as fronteiras do que é possível fazer com os dados pessoais.

A proteção de dados pessoais vai além da simples aplicação técnica ou jurídica das normas, representando uma responsabilidade social e ética por parte das instituições. Essas entidades devem operar de maneira transparente e responsável, especialmente em um cenário onde a confiança da sociedade depende diretamente da forma como as informações pessoais são tratadas. A conformidade com as normas de proteção de dados, nesse contexto, se torna um fator essencial para a legitimidade e sustentabilidade das organizações, pois garante que os direitos dos indivíduos sejam respeitados e preservados. Isso é ainda mais crucial diante dos constantes avanços tecnológicos que ampliam as possibilidades de uso e manipulação dos dados pessoais, desafiando os limites do que é considerado aceitável.

Com isso, é imprescindível que as regulamentações acompanhem a evolução tecnológica para garantir que os direitos dos titulares de dados não sejam prejudicados. Nesse sentido, a redação do artigo da Lei Geral de Proteção de Dados Pessoais (LGPD) referente aos dados pessoais sensíveis deve ser revista para deixar claro que o rol apresentado é exemplificativo e não taxativo. A ANPD poderia, fundamentadamente, emitir posicionamentos para esclarecer e pacificar o entendimento sobre a classificação de dados sensíveis, fornecendo diretrizes mais claras para os agentes de tratamento e possibilitando uma fiscalização mais eficaz e uniforme. Essa abordagem permitiria uma maior flexibilidade para enfrentar os desafios trazidos pela

constante inovação tecnológica, sem comprometer a proteção dos direitos fundamentais dos indivíduos.

Neste sentido, a proteção de dados pessoais não deve ser encarada apenas como uma exigência regulatória, mas como um pilar essencial da convivência social no século XXI. Ao ampliar a proteção dos dados sensíveis, estamos não apenas protegendo a privacidade, mas também defendendo os direitos fundamentais de cada indivíduo, assegurando que a sociedade digital, em sua expansão, não se torne um risco à dignidade humana. Ao adotar um olhar mais holístico sobre a privacidade, a proteção de dados e o respeito aos direitos individuais, podemos avançar na construção de uma sociedade mais equilibrada, que promova o desenvolvimento tecnológico sem renunciar aos valores que sustentam os direitos humanos.

Esses pontos levantam questões importantes: seria o conceito de "dados sensíveis" em sua forma atual adequado para enfrentar os desafios impostos pela tecnologia e as dinâmicas sociais contemporâneas brasileiras? Entendo que temos muitos mecanismos de ampliações a depender do contexto de tratamento dos dados pessoais, tornando o rol exemplificativo, para a defesa das pessoas naturais de forma abragente, tal como objetivo, criou-se a LGPD.

REFERÊNCIAS

.BIONI, Bruno R. **Proteção de Dados Pessoais: a função e os limites do Consentimento**. 2 ed. – Rio de Janeiro : Forense,2020.

BECK, Ulrich. **La società globale del rischio**. Trieste: Asterios, 2001.

BIONI, Bruno R. **Proteção de dados [livro eletrônico]:contexto, narrativas e elementos fundantes/** – São Paulo : B. R. Bioni Sociedade Individual de Advocacia, 2021. PDF

BORTALI, H. P. **Limites da atividade do provedor: o gerenciamento de dados e a responsabilidade sobre conteúdo de terceiros**. 2020. 134 f. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2020.

Byung-Chul Han, **Sociedade da transparência,** tradução de Enio Paulo Giachini - Petrópolis, RJ: Vozes, 2017.

CASTELLS, M. **A sociedade em rede. A era da informação: economia, sociedade e cultura**. São Paulo: Paz e Terra, 2011.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Trad. Maria Luiza X. de A. Georges. Rio de Janeiro: Zahar, 2013.

COTS, Márcio; Oliveira, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: Ed. RT, 2018.

CUPIS, Adriano de. **Os direitos da personalidade**.Trad. Adriano Vera Jardim e Antonio Miguel Caeiro. Lisboa: Morais, 1961.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 3ª. ed. São Paulo: Revista dos Tribunais, 2021.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 3º. ed. São Paulo: Revista dos Tribunais, 2006.

DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados**. 2º. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. **Direito à privacidade e proteção de dados pessoais**. In: RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

FERNANDES, Milton. **Proteção civil da intimidade**. São Paulo:Saraiva,1977.

GEORGIEVA, Ludmila; KUNER, Cristopher. Article 9 Processing of special categories of personal data In: KUNER, Cristopher; Bygrave, Lee; DOCKSEY, Cristopher. The EU General Data Protection Regulation (GDPR): A Commentary.1. Oxford University Press:2020.

HARARI, Noah Yuval.**21 lições para o século 21**. Israel: Spiegel & Grau, 2018.

HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. **Tratado de Proteção de Dados Pessoais.** Coordenação de Danilo Doneda. 2. ed. Rio de Janeiro: Forense, 2023.

IRAMINA, A. **RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União** Europeia. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, n. 2, p. 91-117, outubro de 2020.

JUNQUEIRA, Thiago. **Tratamento de Dados Pessoais e Discriminação Algorítmica nos Seguros** Revista dos Tribunais,2020.

JUNQUILHO, Tainá Aguiar. **Inteligência Artificial no Direito: Limites Éticos**. São Paulo: Editora JusPodivm, 2022.

LEONARDI, Marcel. *Tutela e Privacidade na internet*. São Paulo: Saraiva, 2012.
LGPD – Lei Geral de Proteção de Dados comentada. São Paulo: revista dos Tribunais, 2019.

LGPD – Lei Geral de Proteção de Dados comentada. São Paulo: revista dos Tribunais, 2019.

LUCCA, Newton de; MARTINS, Guilherme Magalhães. **Direitos fundamentais e sociedade tecnológica**.,São Paulo, Foco 2022.

MAIA,Roberta Mauro Medina. **A natureza jurídica da titularidade dos dados pessoais**.In MULHOLLAND, Caitlin. A LGPD e o novo marco normativo no Brasil. Arquipelogo, 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014.

MENDES,Laura Schertel Ferreira. **Autodeterminação informativa: a história de um conceito**. Pensar, Fortaleza, v.25,n.4, 2020.

MORAES, Alexandre de. **Direitos Humanos Fundamentais: Teoria Geral**, comentários aos arts.1º e 5º da Constituição Federativa do Brasil.8. ed. São Paulo: Atlas, 2007.
MORAES, Maria Celina Bodin de. **Danos à pessoa humana: uma leitura civil-constitucional dos danos morais**. Rio de Janeiro: Renovar, 2003.
MULHOLLAND, Caitlin. **Os contratos de seguro e a proteção dos dados pessoais sensíveis**. In.GOLDBERG,Ilan; JUNQUEIRA, Thiago (coords.). Temas Atuais de Direito Dos Seguros, Tomo I. São Paulo: Ed.Thomson Reuters.2020.

MULHOLLAND, Caitlin; KREMER, Bianca. **Responsabilidade civil por danos causados pela violação do princípio da igualdade no tratamento de dados pessoais.** In Rodrigo da Guia Silva: Gustavo Tepedino.Org. *O Direito Civil na era da inteligência Artificial*. São Paulo: Revista dos Tribunais,2020.

PERLINGIERI, Pietro. **O direito civil na legalidade constitucional**. Rio de Janeiro:Revovar,2008.

PINHEIRO, P. P. **Proteção de Dados Pessoais**. 3. ed. São Paulo: Saraiva Educação, 2021.

PINHEIRO, P. P. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** São Paulo: Saraiva Jur, 2018.

RIOS, Roger Raupp. **Direito da antidiscriminação; discriminação direta, indireta e ações afirmativas**, Porto Alegre; Livraria do Advogado 2008.
RODOTÁ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SKINNER-THOMPSON, Scott.*Privacy at margins*. Cambridge: Cambridge University Press,2021.

TEFFÉ, Chiara Spadaccini de. **Dados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas.** 1. ed. São Paulo: Foco, 2022.

VAINZOF, Rony in NOBREGA MALDONADO, Viviane; OPICE BLUM, Renato (coord.).

VITALIS, André; ELLUL, Jacques. **Ciência Política**, 1981.

WACTHER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data Protection law in the age of big data and AI.Columbia Business Law review, vol.2019.

ZANATTA, Rafael A. F. **A proteção coletiva dos dados pessoais no Brasil: vetores de interpretação**. Belo Horizonte: Letramento, 2023.

ZUBOFF, Shoshana. The Age of Surveillance Capitalism: **The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019.