

UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES
PRÓ-REITORIA DE ENSINO, PESQUISA E PÓS-GRADUAÇÃO
CAMPUS DE ERECHIM
DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

GABRIELA MARIA

**UMA ANÁLISE DA AUTODETERMINAÇÃO INFORMATIVA
COMO MARCO LEGAL DA LEI GERAL DE PROTEÇÃO DE DADOS**

ERECHIM

2024

GABRIELA MARIA

**UMA ANÁLISE DA AUTODETERMINAÇÃO INFORMATIVA
COMO MARCO LEGAL DA LEI GERAL DE PROTEÇÃO DE DADOS**

Trabalho de conclusão de curso apresentado como requisito parcial à obtenção do grau de Bacharel em Direito do Curso de Direito do Departamento de Ciências Jurídicas e Sociais da Universidade Regional Integrada do Alto Uruguai e das Missões — Campus Erechim/RS.

Orientador(a): Prof.^a M.e Simone Gasperin de Albuquerque

ERECHIM

2024

GABRIELA MARIA

**UMA ANÁLISE DA AUTODETERMINAÇÃO INFORMATIVA
COMO MARCO LEGAL DA LEI GERAL DE PROTEÇÃO DE DADOS**

Monografia Jurídica apresentada para obtenção do título de Bacharel em Direito no Curso de Direito do Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões – Campus de Erechim.

_____, ____ de _____ de 2024.

BANCA EXAMINADORA

Prof.^a M.e Simone Gasperin de Albuquerque
Universidade Regional Integrada do Alto Uruguai e das Missões

Prof.
Universidade Regional Integrada do Alto Uruguai e das Missões

Prof.
Universidade Regional Integrada do Alto Uruguai e das Missões

Dedico esse trabalho a minha mãe Katia, mulher referência de vida que escolheu viver minhas lutas, assumiu meus carmas para que eu tivesse minha vida facilitada em todos os espectros.

AGRADECIMENTOS

Agradeço a Deus, por me fornecer força para continuar, mesmo quando não via sentido.

Agradeço a meus pais Katia e Edison, que são fonte de amor, me deixando segura para permanecer em meus objetivos e me apoiando em todas as decisões.

Agradeço a minha irmã Ana, por quem tenho amor superior ao próprio, faço o meu melhor, para proporcionar a ela, tudo que o mundo tem a oferecer de mais lindo. Ela é minha base, meu porto seguro e minha aliança na terra.

Agradeço a minha Orientadora, primeiramente por aceitar me acompanhar nesse trabalho, além disso, por me direcionar ao tema, tirar dúvidas, respeitar meu espaço e meu processo criativo. Em todas as suas versões, és inspiração para mim. Não poderia ter feito escolha melhor como Orientadora. Te admiro. Obrigada.

Agradeço a minha tia Simone, que foi tia, amiga, mãe. Que me incentiva e impulsiona todos os dias. Minha maior apoiadora, obrigada por ser quem és.

Agradeço aos meus amigos que considero família, por estarem sempre ao meu lado, tornando meus dias cinzas coloridos.

Agradeço em especial, minhas irmãs não-sanguíneas, Laura, Amanda, Ingrid, Brenda, Isadora, Roberta que tornaram o caminho árduo, leve, que concederam seu tempo a mim, que em nenhum momento me fizeram duvidar da minha capacidade. No vemos no topo. Obrigada.

Agradeço ainda aos professores que tiveram paciência em momentos ruins e foram adoráveis em momentos bons. Que sempre foram prestativos, que concederam conhecimento, transmitiram conforto, apoio, que mesmo entre as adversidades, deram seu máximo para que eu pudesse aprender.

E por fim agradeço a universidade que se tornou minha segunda casa nesses cinco anos.

A finalidade da lei não é abolir ou conter, mas preservar e ampliar a liberdade. Em todas as situações de seres criados aptos à lei, onde não há lei, não há liberdade.

(John Locke)

RESUMO

O presente trabalho tem como objetivo apresentar uma análise da autodeterminação informativa prevista no inciso II, do art. 2º da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e do fundamento legal para o titular se opor a operações de tratamento de seus dados pessoais. Estudar os fundamentos da proteção de dados no Brasil, os direitos humanos e o desenvolvimento da personalidade. Analisar a Lei Geral de Proteção de Dados e suas definições legais, especificamente em relação aos dados pessoais, anonimização dos dados pessoais, o encarregado (data protection officer – dpo) e o consentimento. Apresentar as bases legais de tratamento de dados pessoais, trazendo as hipóteses taxativas do art. 7º da LGPD e o tratamento dos dados sensíveis. Esta pesquisa utiliza o método o indutivo e na perspectiva da abordagem o modo exploratório. Quanto aos procedimentos técnicos, baseou-se em pesquisa bibliográfica e pesquisa documental, dentre eles, artigos científicos, pesquisas on-line e obras literárias pertinentes ao estudo, além de legislação. Por fim, entende-se que a efetivação completa do direito à autodeterminação da informativa requer uma consideração cuidadosa sobre até que ponto o uso de dados pessoais mantém os direitos fundamentais do titular desses dados. Portanto, para garantir adequadamente esse direito, é fundamental estabelecer o poder do titular dos dados pessoais, em parceria com a legislação.

Palavras-chave: Autodeterminação; Dados pessoais; Privacidade; Consentimento; Legislação.

ABSTRACT

The present work aims to present an analysis of informational self-determination as provided for in article 2, section II of the General Data Protection Law (Law No. 13,709/2018) and the legal basis for the data subject to object to the processing of their personal data. It studies the fundamentals of data protection in Brazil, human rights, and personality development. It analyzes the General Data Protection Law and its legal definitions, specifically regarding personal data, anonymization of personal data, the Data Protection Officer (DPO), and consent. It presents the legal bases for the processing of personal data, bringing the exhaustive hypotheses of article 7 of the LGPD and the treatment of sensitive data. The methodology used in this research was based on the inductive method, from the perspective of an exploratory approach. Regarding technical procedures, it was based on bibliographic research and documentary research, including scientific articles, online surveys, and literary works relevant to the study, as well as legislation. Finally, it is understood that the full realization of the right to informational self-determination requires careful consideration of the extent to which the use of personal data maintains the fundamental rights of the data subject. Therefore, to properly ensure this right, it is essential to establish the power of the data subject, in partnership with legislation.

Keywords: Self-determination; Personal data; Privacy; Consent; Legislation.

SUMÁRIO

1 INTRODUÇÃO.....	10
2 OS FUNDAMENTOS DA PROTEÇÃO DE DADOS NO BRASIL.....	13
2.1 FUNDAMENTOS E AUTODETERMINAÇÃO INFORMATIVA.....	15
2.2 DIREITOS HUMANOS E DESENVOLVIMENTO DA PERSONALIDADE.....	19
3 A LEI GERAL DE PROTEÇÃO DE DADOS E SUAS DEFINIÇÕES LEGAIS.....	22
3.1 DADOS PESSOAIS.....	23
3.2 ANONIMIZAÇÃO DOS DADOS PESSOAIS.....	24
3.3 ENCARREGADO (DATA PROTECTION OFFICER – DPO)	26
3.4 CONSENTIMENTO.....	28
4 BASES LEGAIS DE TRATAMENTO DE DADOS PESSOAIS.....	29
4.1 AS HIPÓTESES TAXATIVAS DO ART. 7º DA LGPD.....	30
4.2 TRATAMENTO DOS DADOS SENSÍVEIS.....	32
5 CONCLUSÃO.....	35
REFERÊNCIAS.....	37

1 INTRODUÇÃO

Sabe-se que a Lei Geral de Proteção de dados (Lei nº 13.853, de 2019) Vigência predispõe sobre o cuidado de dados pessoais do indivíduo inclusive nos meios digitais, podendo ser por pessoa natural ou por pessoa jurídica de direito público ou privado. Além disso, essa lei garante proteção aos direitos fundamentais como o de liberdade, privacidade e o de desenvolvimento de indivíduo (pessoa natural) que possui a garantia a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, previsto também no rol dos Direitos humanos fundamentais da Constituição Federal Brasileira de 1988. Esses direitos e outros previstos na LGPD, como também dados sensíveis do usuário se tornam mais vulneráveis quando imersos a plataformas digitais.

A Lei Geral de Proteção de dados (LGPD) foi inspirada na General Data Protection Regulation (GDPR) europeia e tem a finalidade de instruir as pessoas sobre a importância de seus dados pessoais e a segurança e proteção dos mesmos em relação a quem entrar em contato com estes, principalmente os dados sensíveis. Apresenta a forma de usá-los de forma correta e que não se perda nas grandes plataformas digitais, em função de um algoritmo que busca incansavelmente por dados, principalmente para a publicidade e a venda de produtos online. Torna-se necessário entender até onde o desenvolvimento econômico e tecnológico, possui regras adequadas para lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais.

Cada vez mais os dispositivos digitais e automatizados ganham espaço na sociedade, assim, a tecnologia, as plataformas digitais, o algoritmo, etc, devem andar juntos a LGPD que também busca equilibrar interesses econômicos e sociais, garantindo a continuidade de decisões automatizadas e também limitando abusos. Na “era digital” é relevante que o processo seja cauteloso e a lei desenvolva melhorias para que seja possível evoluir sem prejudicar o ser humano que faz parte dessa revolução digital, que possui seus principais dados, seu direito à privacidade, imersos a esse processo.

A criação da Lei Geral de Proteção de Dados confirma a preocupação do Estado brasileiro com a proteção de informações importantes sobre a vida de cada indivíduo. Com a expansão da internet e seu fácil acesso por parte significativa da população, surgem questões relacionadas ao quão prejudicial esta pode ser aos seus

usuários no sentido da exposição de dados, violação de direitos humanos fundamentais como a privacidade, desenvolvimento da personalidade da pessoa e o consentimento sobre o uso de seus dados pessoais.

Na Europa por exemplo, após relatórios de espionagem e violação de dados de clientes envolvendo a *Cambridge Analytica* e o *Facebook*, iniciou discussões sobre regulamentos de segurança de dados, que inspiraram a formulação do Regulamento Geral de Proteção de Dados (GDPR), que regulamentava a União Europeia e impunha Medidas para aprovar legislação sobre segurança de dados pessoais (Raposô, 2019).

A interligação entre a comunicação de massa e o uso de dados tem sido amplamente abordada em pesquisas nas áreas de comunicação e ciências sociais, abrangendo uma variedade de perspectivas para que se edifique um modelo exemplar de proteção.

O presente trabalho trará o prisma da doutrina do direito de proteção de dados, sua concepção no Brasil, e suas consequências jurídicas.

Busca-se uma análise sobre a obrigatoriedade da autodeterminação informativa prevista no inciso II, do art. 2º da Lei Geral de Proteção de Dados e o fundamento legal para o titular se opor a operações de tratamento de seus dados pessoais.

O contexto histórico é chave mestra para adentrar-se ao tema, conhecer e debater sua essencialidade, principalmente no período que a sociedade está vivendo, com gigantesco avanço das tecnologias e suas vertentes, que buscam incansavelmente vender às custas dos dados fornecidos de forma direta ou indireta, com ou muitas vezes sem consentimento das pessoas.

Este trabalho está organizado em 3 capítulos, com o intuito de fornecer os objetivos propostos no item 1, escritos de maneira pontual e de fácil entendimento ao leitor, para que o tema seja esclarecido da melhor maneira aos interessados no assunto. No capítulo 2, serão abordados os conceitos teóricos utilizados como base para esta dissertação, iniciado com apresentação da lei seguindo das suas principais características para fácil entendimento, além de contextualizar historicamente e expor paradigmas da criação da LGPD. O capítulo 3 expõe as conclusões sobre o estudo detalhado do tema. Seguidamente, são apresentadas as referências bibliográficas, as quais foram fontes para os estudos.

Cabe mencionar que a construção de uma resposta ao questionamento proposto por esta pesquisa será pautada no método indutivo, com pesquisa

qualitativa, baseada em material bibliográfico disponível como livros, artigos, o Código Civil, a Constituição Federal e as Leis a serem mencionadas.

2 OS FUNDAMENTOS DA PROTEÇÃO DE DADOS NO BRASIL

Em 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) foi parcialmente sancionada pelo Ex-Presidente Michel Temer. Esta legislação estabelece uma série de disposições com o objetivo de garantir a proteção dos dados pessoais de indivíduos (pessoas naturais), seja em ambientes digitais ou em outros meios. Ela é de observância obrigatória tanto para entidades de direito público quanto para as de direito privado. A vigência de fato da lei iniciou-se em agosto de 2020 e as sanções passaram a valer apenas em agosto de 2021 e trouxe uma forma inovadora de proteger dados, apresentando-se de forma marcante no tema explicitado, assim é pertinente que se analise o texto da lei para entender sua fundamentação. (Supremo Tribunal Federal, 2018)

A premissa inicial do texto constitucional discorre sobre objetivos da lei (art. 1º), seus fundamentos (art. 2º), sua aplicabilidade (art. 3º e 4º), definições (art. 5º) e princípios (art. 6º). (Supremo Tribunal Federal, 2018)

O artigo 1º trata de preservar o direito essencial à liberdade, salva guardar o direito fundamental à privacidade e assegurar o pleno desenvolvimento da personalidade humana. A LGPD se aplica a todos os tipos de tratamento de dados pessoais, independentemente da origem (seja de indivíduos ou entidades jurídicas), com exceção das situações especificamente descritas no artigo 4º da lei. Além disso, as definições essenciais para uma compreensão abrangente da legislação estão apresentadas no artigo 5º da LGPD. (Brasil, 2018)

No artigo 2º o legislador transpassa a ideia de que a lei não possui o objetivo de estagnar a evolução da tecnologia e informação, e sim, torná-la exponencialmente segura a quem acessá-la. (Brasil, 2018)

O princípio da autodeterminação informativa é reconhecido como uma das ideias mais proeminentes. Esse conceito apesar de forte presença na Alemanha, não se limita à ela; o princípio exerceu influência em diversos sistemas legais estrangeiros e foi incorporado como um dos pilares fundamentais na Lei Geral de Proteção de Dados no Brasil, conforme estabelecido no artigo 2º, inciso II. (Brasil, 2018)

A trajetória histórica e conceitual da origem do princípio da autodeterminação informativa na jurisprudência alemã, explorando seus antecedentes, como o direito geral à liberdade de ação e o direito geral de personalidade. Compreender sua evolução é fundamental para uma compreensão abrangente tanto de sua essência

como de suas limitações e *reinterpretations*. Além disso, a análise da jurisprudência do Tribunal Constitucional em relação à maneira como terceiros lidam com dados e informações pode fornecer *insights* valiosos sobre aspectos cruciais da proteção de dados em geral.

O alicerce da questão da proteção de dados no Brasil é visivelmente apresentado por meio de disposições da LGPD. Os direitos do titular, conforme estabelecidos no artigo 18 da LGPD, demonstram a aplicação prática do princípio da autodeterminação informativa ao oferecerem meios que asseguram o controle dos dados pessoais pelo titular. Isso inclui a correção de dados que estejam incompletos, inexatos ou desatualizados (artigo 18, inciso III), bem como o direito à portabilidade dos dados para outro fornecedor (inciso V). Esse princípio é mais abrangente do que o simples conceito de consentimento, mas pode ser observado no direito do titular de revogar seu consentimento (inciso VIII) e na avaliação da legalidade do consentimento, que só é válido se for dado de maneira livre, informada e inequívoca. (Brasil, 2018)

No entanto, a aplicação desse princípio, como a de outros direitos fundamentais, não é absoluta. Portanto, é possível o tratamento de dados pessoais sem o consentimento do titular, desde que haja uma base legal para tal procedimento. Além disso, os princípios relacionados à matéria também oferecem uma maior capacidade de controle sobre os dados por parte dos titulares, garantindo que apenas os dados necessários para uma finalidade específica sejam tratados.

É importante destacar que o controle sobre os dados depende, em parte, da ação direta do titular, seja por meio de solicitações para exercer os direitos mencionados ou por meio de denúncias à Autoridade Nacional de Proteção de Dados (ANPD). O objetivo é garantir o direito à privacidade, considerando os modelos adotados pela sociedade da informação, capacitando o titular e garantindo o controle de seus próprios dados, aqui, surge a temática de como as solicitações de uso de dados são fornecidas aos usuários, sendo a que maioria das vezes aparecem em textos gigantescos e de difícil leitura. (Ministério da Justiça e Segurança Pública, 2021)

O cidadão desempenha um papel central ao fornecer suas informações, mas, por outro lado, assume uma posição secundária no que diz respeito ao seu uso. Ele não tem controle sobre quais informações estão em posse de terceiros, como essas

informações estão sendo coletadas e o nível de controle que ele exerce sobre o armazenamento desses dados.

Neste contexto, explica Stefano Rodotà (2008, p. 113): “[...] a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações”.

Fica claro o fundamento da lei, proteger, informar, cuidar e respeitar os dados das pessoas (físicas ou jurídicas), que por vezes encontram-se no tumulto das informações e aceitam termos de uso, *cookies*, etc no automático, deixando os interessados em dados, em posição confortável, para fazerem o que bem quiserem com estes.

2.1 FUNDAMENTOS E AUTODETERMINAÇÃO INFORMATIVA

A Lei Geral de Proteção de Dados Pessoais traz no seu art. 2º a previsão dos fundamentos que nortearão a disciplina de proteção dos dados pessoais. É possível observar na análise do dispositivo que o legislador optou por ressaltar, em sua maioria, princípios constitucionais, que muito provavelmente nem precisassem ter sua previsão expressa na Lei, visto que, as normas infraconstitucionais já retiram o seu fundamento de validade das normas constitucionais. Todavia, o legislador elencou de maneira pormenorizada estes fundamentos com o intuito de servir como fundação e base para interpretação de toda a legislação relativa à proteção dos dados pessoais. (Brasil, 2018)

Embora ocorra a repetição de ditames constitucionais, o legislador da LGPD trouxe uma inovação ao incluir no inciso II, do art. 2º, a chamada “autodeterminação informativa”. Este termo é alienígena e foi criado em sede jurisprudencial após decisão da Corte Constitucional Alemã no julgamento em 1983 da constitucionalidade da Lei do Censo Alemã. A referida lei alemã autorizava a coleta e tratamento de dados para fins estatísticos, bem como a transmissão anonimizada dos dados para a execução das atividades públicas. A Lei do Censo foi considerada parcialmente constitucional. O Tribunal alemão entendeu que a inconstitucionalidade da lei residia na troca de dados pessoais entre órgãos públicos, e esta troca seria incompatível com a dignidade humana e o direito ao livre desenvolvimento da personalidade, já que o indivíduo não era protegido contra essa coleta ilimitada, armazenamento, aproveitamento,

transferência e divulgação dos seus dados pessoais. (Sarlet; Marinoni; Mitidiero, 2018, p. 495)

Trata-se de um direito do indivíduo escolher como irá disponibilizar os seus dados pessoais, até porque, quando se fala sobre a proteção de dados, é importante contrabalancear a proteção do indivíduo, no sentido da sua privacidade informacional e o tratamento legítimo dos seus dados, seja pelo Estado ou por terceiros privados. Assim, a decisão alemã consolidou o entendimento da autodeterminação do cidadão perante o Estado no tocante à informação e dados, fixando a transparência no tratamento dos dados.

Sobre autodeterminação informativa, Suzana Mendonça ensina que:

O núcleo da proteção de dados pessoais, por sua vez, também confere ao consentimento posição de destaque, de modo a ostentar a autodeterminação informativa como um de seus fundamentos. A comunicação eficiente em relação à coleta de dados adquire maior consistência em um cenário no qual o consentimento mostra-se essencial para desencadear o tratamento, enquanto o vício de consentimento trava exatamente a possibilidade de operação de dados pessoais. Garante-se ao titular, por meio da comunicação eficiente, o controle sobre a forma como seus dados serão manuseados, de modo a conferir maior segurança não somente quanto à autorização de uso, como também da medida em que serão utilizados. O consentimento informado, nesse sentido, insere-se no cenário atual como uma relevante ferramenta de participação ativa do usuário em todo o processo de conhecimento e posterior anuência de tratamento de dados pessoais. (Mendonça, 2019, documento eletrônico)

A Constituição Brasileira não possui uma previsão semelhante, embora a autodeterminação informativa esteja incorporada e prevista em diversas legislações e Constituições de outros países, uma vez que se trata de um fundamento marcadamente republicano e democrático, instituindo o poder de autodeterminação do cidadão perante o Estado, enquanto um aspecto individual e forte, além de necessário para o desenvolvimento da personalidade. Nesse sentido:

À míngua de expressa previsão de tal direito no texto da Constituição Federal e a exemplo do que ocorreu em outras ordens constitucionais, o direito à proteção dos dados pessoais pode ser associado ao direito à privacidade (no sentido de uma “intimidade informática”) e ao direito ao livre desenvolvimento da personalidade, que inclui o direito à livre disposição sobre os dados pessoais, de tal sorte que não se trata apenas de uma proteção dos dados contra o conhecimento e uso por parte de terceiros, razão pela qual – a exemplo do que se deu no direito alemão e espanhol – se fala em um direito à autodeterminação informativa. (Sarlet; Marinoni; Mitidiero, 2018, p. 496)

Finalmente, trata-se de tema relevante para a pesquisa e sociedade acadêmica, já que surge a possibilidade do titular se opor a operações de tratamento

dos seus dados pessoais invocando a autodeterminação informativa como fundamento da LGPD, e sua observância é diretamente relacionada ao consentimento deste titular.

O primeiro artigo da Lei Geral de Proteção de Dados, traz informações importantes sobre os fundamentos da proteção de dados no Brasil, com a chegada da lei, que teve está em vigência desde setembro de 2020. (Brasil, 2018)

A lei chegou para consolidar a proteção de dados no país. Para melhor entendimento:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Brasil, 2018, p.1)

A partir disso, nota-se, que a lei tem como fundamento principal a proteção de dados de pessoas naturais, nos meios físicos ou digitais, garantindo direito fundamental à liberdade, privacidade, além disso, permitir o livre desenvolvimento da personalidade humana. Na redação da lei referida, o verbo “proteger” ganha ênfase, quando precisa manter esses direitos fundamentais, em meio, a fragilidade da pessoa humana que é possuidora desses dados.

O artigo 2º da LGPD, apresenta, sete fundamentos de proteção, dentre eles, o foco desta pesquisa, é o inciso II, que trata sobre a autodeterminação informativa, que conceituada, trata-se do direito do titular dos dados ter controle, conhecimento e segurança sobre estes. Além de controlar como esses dados serão tratados, quando estiverem em poder de outras pessoas, empresas, plataformas digitais etc. (Brasil, 2018)

Em meio a isso, surge uma preocupação, em relação a evolução da tecnologia e dos meios digitais, onde empresas como *instagram*, *facebook*, *google*, possuem amplo acesso às informações dos usuários. Empresas como estas, sabem detalhadamente os seus gostos, em função do algoritmo que trabalha incansavelmente para te direcionar produtos que combinem com o que você busca nas redes, além saberem o seu tempo de uso, suas crenças, dados como localização (as vezes em tempo real) ideologias, relacionamentos, lugares que costuma frequentar e muitas vezes, até seu perfil político. Pode-se perceber, que grandes empresas de tecnologia com uma simples mensagem “li e aceito a política de

privacidade” conseguem retirar das pessoas, mais dados do que o próprio governo do país possui. Um exemplo é quando há uma investigação policial e existe uma extensa burocracia para o acesso de dados, notoriamente isso também é uma forma de proteção, porém se empresas que não estão preocupadas com o bem-estar social ou pelo menos não possuem a responsabilidade governamental sobre a população, possuem esse acesso, como que sites e empresas virtuais, conseguem ter de forma tão simples. (Almeida, Poliana (Uninter, 2021)

Com a análise desses fatos surge a necessidade de criar a LGPD, para que não haja a possibilidade da “terceirização” de dados pessoais. Onde não haja a possibilidade de dados tão importantes serem banalizados e expostos. Além da pressão internacional, que já vinha alertando sobre essa situação, inclusive, a LGPD foi baseada na lei GDPR¹, nos moldes europeus de proteção, mesmo que regulamentada e feita de uma forma mais simplificada, a lei tem a função de proteger a privacidade dos usuários digitais. Também foi exigido com a vigência da lei, que dados sensíveis tivessem uma atenção maior, visando a diminuição de golpes de criminosos digitais que se aproveitavam dessa fragilidade. A lei exige que as empresas, digitais ou não, criem políticas antivazamento e que tenham um profissional responsável sobre a segurança de dados, para fiscalizar, proteger e resguardar da melhor forma possível, o que a empresa tem acesso. Caso haja descumprimento, prevê-se multa de até 4% do faturamento anual da empresa, demonstrando assiduamente o comprometimento para com as pessoas e o marco legal na proteção de dados. (Koch, Richie (Gov.br, 2019).

Nesse viés, o Brasil está dando um passo em prol a regulamentação da proteção de dados, garantindo e respeitando direitos fundamentais previstos na Constituição Federal e assegurados pela Organização das Nações Unidas (ONU), além de estar em concordância com os moldes europeus de proteção que já avançaram muito nesse quesito.

Existem situações que boa parte da população passa diariamente, como preenchimentos de formulários, cadastros, onde não se sabe se os dados serão usados da maneira proposta ou se serão desviados para outros fins. Além, de ser

¹ O GDPR é um regulamento do Parlamento Europeu e Conselho da União Europeia que estabelece regras sobre a privacidade e proteção de dados de cidadãos da União Europeia e Espaço Econômico Europeu. A sigla significa General Data Protection Regulation, podendo-se traduzir como Regulamento Geral sobre a Proteção de Dados.

recorrente, vazamento de informações confidenciais na mídia, como por exemplo o caso da Atriz Klara Castanho, que teve sua vida exposta por um hospital, quando foi vítima de um estupro. Torna-se inadmissível que essas situações continuem acontecendo, ainda mais quando envolvem assuntos tão sérios. (Fachini, Thiago, ProJuris, 2022)

Um fator que também merece atenção, é que a LGPD não conseguirá ter controle dos dados anonimizados, eis que estudos vem demonstrando que existem mecanismos capazes de fazer com que esses dados saiam do anonimato.

Assim, entra a análise da razoabilidade como filtro à identificabilidade de dados. Diante isso, cria-se um pressuposto e um novo conceito de anônimo, que seria um dado incapaz de revelar a identidade de uma pessoa. Para que isso funcione, é necessário ver quais dados tem esse potencial de revelação e assim criar limites e possibilidades técnicas de anonimização. Um exemplo seria a supressão do Cadastro de Pessoas Físicas (CPF) que é um dado único de cada pessoa, logo, sendo sua disponibilização, sendo limitada a alguns dígitos, que não entreguem ou facilite para descobrir de quem se trata. Outra forma é a generalização do nome completo, localização e idade que podem ser usadas as faixas etárias, assim não haverá caracterização tão precisa do indivíduo. (Biani, 2019)

O objetivo é criar um filtro, que consiga delimitar dados que podem ou não serem generalizados, que delimitassem também, a elasticidade do conceito expansionista. Criando limites de dados. Com isso, o direito comunitário europeu e a LGPD valeram-se do critério da razoabilidade para delimitar esse espectro. Assim são estabelecidos critérios que tratem cada dado, do jeito correto.

Evidenciado isso, vale destacar, que a proteção de dados também possui forte papel na construção da personalidade humana e em seu livre desenvolvimento.

2.2 DIREITOS HUMANOS E DESENVOLVIMENTO DA PERSONALIDADE

O Direito da Personalidade é um ramo do direito civil que se dedica a proteger os atributos inerentes à pessoa humana, resguardando sua integridade física, psicológica e moral. Este campo do direito busca assegurar a dignidade da pessoa, reconhecendo seus direitos inalienáveis e intransmissíveis. Neste contexto, destacam-se a vida, a liberdade, a privacidade, a honra e a imagem como direitos fundamentais. (Brasil, 2002)

A fundamentação teórica do Direito da Personalidade encontra respaldo em diversas correntes filosóficas e jurídicas. A obra de Immanuel Kant, notadamente a ética kantiana, destaca-se ao fundamentar a dignidade humana como um fim em si mesma. A autonomia da vontade, central para Kant, é essencial para a compreensão dos direitos da personalidade. (Kant, 2012)

Outro alicerce filosófico relevante é a teoria dos direitos fundamentais de Ronald Dworkin. Para Dworkin, os direitos individuais são dimensões fundamentais da liberdade e igualdade, sendo responsáveis por delinear os limites da atuação estatal e proteger o espaço vital do indivíduo. (Dworkin, 2002)

O Direito da Personalidade encontra respaldo no ordenamento jurídico por meio de normas constitucionais e infraconstitucionais. A Constituição Federal de 1988, por exemplo, consagra a inviolabilidade da vida, liberdade, igualdade, intimidade e imagem como cláusulas pétreas, conferindo máxima proteção a esses direitos. No âmbito do Código Civil brasileiro, o artigo 11 reconhece a personalidade jurídica desde o nascimento com vida, atribuindo direitos e garantias aos nascituros, consolidando a proteção desde o início da existência. O advento da tecnologia trouxe desafios e novas dimensões ao Direito da Personalidade. O direito à privacidade, por exemplo, enfrenta novas questões com a proliferação de dispositivos eletrônicos e redes sociais. A proteção contra a divulgação não autorizada de informações pessoais e o direito ao esquecimento tornaram-se temas centrais nos tribunais. (Brasil, 1988)

A Jurisprudência, nesse contexto, desempenha um papel crucial na adaptação do Direito da Personalidade às transformações sociais. Decisões judiciais recentes têm ampliado a proteção à imagem, inclusive nas situações envolvendo exposição não consentida em meios digitais. (Brasil, 2002)

O Direito da Personalidade é um ramo essencial do direito civil que busca preservar os atributos inalienáveis e intransmissíveis da pessoa humana. Fundamentado em correntes filosóficas como a ética kantiana e a teoria dos direitos fundamentais de Dworkin, e respaldado por normas constitucionais e infraconstitucionais, este campo do direito continua a evoluir para enfrentar os desafios trazidos pela sociedade contemporânea, especialmente no contexto da revolução tecnológica. (Dworkin, 2002)

Os Direitos Humanos e os Direitos da Personalidade representam dois pilares fundamentais no arcabouço jurídico que visa proteger a dignidade e a liberdade individual. Ambos compartilham a finalidade de salvaguardar a essência humana,

embora atuem em esferas distintas do ordenamento jurídico. Os Direitos Humanos são uma expressão de valores fundamentais inerentes a todos os seres humanos, independentemente de sua nacionalidade, etnia, gênero ou religião. O marco histórico da Declaração Universal dos Direitos Humanos de 1948 consagrou princípios como a liberdade, a igualdade, a justiça e a dignidade como fundamentais para a convivência pacífica e o desenvolvimento humano. (Declaração Universal dos Direitos Humanos, 1948)

Os Direitos da Personalidade, por sua vez, focam na proteção dos aspectos mais íntimos e singulares da vida de uma pessoa. A vida, a integridade física e psicológica, a privacidade, a honra e a imagem são elementos resguardados por esse ramo do direito civil. A obra de Jhering, em "A Finalidade do Direito," destaca a importância de proteger a personalidade como uma defesa contra interferências externas (Jhering, 2013).

Outra obra de valor para o tema de Gustavo Radbruch, em "Introdução à Filosofia do Direito," discute a evolução dos direitos da personalidade à medida que a sociedade se transforma, chamando atenção para a necessidade de adaptação jurídica diante das mudanças sociais e tecnológicas (Radbruch, 2008).

O diálogo entre Direitos Humanos e Direitos da Personalidade é evidente na medida em que ambos se entrelaçam na proteção da dignidade e liberdade individuais. A privacidade, por exemplo, é um direito da personalidade que encontra respaldo nos Direitos Humanos, principalmente no direito à vida privada consagrado no artigo 12 da Declaração Universal dos Direitos Humanos. O direito à liberdade de expressão, presente nos Direitos Humanos, também dialoga com os Direitos da Personalidade, especialmente quando se trata de encontrar um equilíbrio entre a liberdade de expressão e a proteção da honra e da imagem. (Declaração Universal dos Direitos Humanos, 1948)

Os Direitos Humanos e os Direitos da Personalidade são dimensões complementares na proteção da condição humana. Enquanto os Direitos Humanos estabelecem um conjunto de princípios universais, os Direitos da Personalidade operam em nível individual, resguardando a singularidade de cada pessoa. O diálogo entre essas esferas é essencial para construir um sistema jurídico que promova uma sociedade justa, igualitária e que respeite a diversidade humana.

3 A LEI GERAL DE PROTEÇÃO DE DADOS E SUAS DEFINIÇÕES LEGAIS

A Lei Geral de Proteção de Dados representa um avanço significativo no cenário jurídico brasileiro ao estabelecer regras claras e abrangentes para o tratamento de dados pessoais. Inspirada em legislações europeias a LGPD visa proteger a privacidade dos cidadãos e regular o uso de informações pessoais por parte de entidades públicas e privadas. (Brasil, 2018)

A LGPD define "dado pessoal" como qualquer informação relacionada a uma pessoa natural identificada ou identificável. Já os "dados sensíveis" referem-se a informações sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dados genéticos, biométricos, entre outros. (Gov.br, 2023)

O tratamento de dados, conforme a LGPD, abrange uma série de operações realizadas com as informações pessoais, como coleta, armazenamento, uso, compartilhamento e exclusão. (Nogueira, 2018)

A lei diferencia o "controlador", responsável pelas decisões sobre o tratamento de dados, do "operador", que efetua o processamento em nome do controlador. Essa distinção busca estabelecer responsabilidades claras entre as partes envolvidas no tratamento de dados. (Wang, 2019)

A LGPD exige o consentimento do titular dos dados para o tratamento, salvo em situações específicas previstas em lei, como a execução de contratos e o cumprimento de obrigações legais. As bases legais para o tratamento são fundamentais para garantir a legalidade e a transparência nas operações (Frozza, 2020).

A lei prevê a figura do Encarregado, ou Data Protection Officer (DPO), responsável por intermediar a comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), quando esta for criada. (Reis, Jessica Cabreira, 2020)

A LGPD representa um marco legal crucial para o Brasil, alinhando-o às tendências globais de proteção de dados pessoais. As definições legais contidas na legislação são essenciais para orientar as práticas das organizações, garantindo que o tratamento de dados seja realizado de maneira ética e respeitando os direitos fundamentais dos indivíduos.

3.1 DADOS PESSOAIS

A sociedade contemporânea está intrinsecamente conectada à tecnologia, gerando uma crescente produção e circulação de dados pessoais. Nesse contexto, a LGPD surge estabelecendo diretrizes para o tratamento dessas informações e garantindo a privacidade e segurança dos indivíduos. Este capítulo explora as definições, princípios e implicações da LGPD na proteção de dados pessoais, bem como seus reflexos na sociedade e nas práticas empresariais.

A LGPD define dados pessoais como qualquer informação relacionada a uma pessoa identificada ou identificável, e dados sensíveis como informações sobre características íntimas do titular. A lei estabelece a necessidade de consentimento para o tratamento desses dados, salvo em casos específicos, fundamentando-se em bases legais previstas. Autores como Moraes (2018) e Nogueira (2018) enfatizam a importância das definições precisas da LGPD para proporcionar clareza e segurança jurídica, contribuindo para a harmonização das práticas de tratamento de dados.

A LGPD baseia-se em princípios essenciais para o tratamento ético dos dados pessoais. A finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização são os pilares fundamentais destacados pela legislação. A obra de Wang (2019) destaca a relevância desses princípios na construção de uma cultura de proteção de dados, influenciando desde a concepção de produtos e serviços até a conscientização dos usuários.

A LGPD representa uma mudança significativa na forma como a sociedade lida com a privacidade e segurança dos dados. Indivíduos passam a ter maior controle sobre suas informações, enquanto empresas enfrentam desafios para se adequar às novas exigências legais. O manual de Frozza (2020) analisa os impactos econômicos da LGPD nas organizações, ressaltando a necessidade de investimentos em infraestrutura e treinamento para garantir a conformidade.

A criação da Autoridade Nacional de Proteção de Dados (ANPD) reforça a importância do Estado na fiscalização e aplicação da LGPD. O Encarregado (DPO) torna-se uma figura-chave para garantir a conformidade das organizações com a legislação. A LGPD emerge como uma resposta necessária ao ambiente digital contemporâneo, reforçando os direitos individuais e promovendo a responsabilidade no tratamento de dados pessoais. Sua implementação representa um desafio para as

organizações, mas também uma oportunidade para consolidar práticas éticas e transparentes.

3.2 ANONIMIZAÇÃO DOS DADOS PESSOAIS

A sociedade da informação atinge seu ponto máximo em um cenário onde a coleta e o processamento em larga escala de dados, dados que de fato abrangem uma maior diversidade, apresentam volumes em constante crescimento e são processados com maior velocidade. Esses atributos dão origem ao conceito de Big Data, que evidenciam um movimento irreversível com impactos nas esferas política, econômica e social. É responsabilidade do Direito regulamentar essas situações para reinterpretar os efeitos dos novos meios de comunicação nas esferas sociais. Com o crescente uso de dados pessoais para diversas atividades, como identificação, classificação e autorização, torna-se essencial a implementação de marcos regulatórios para a adequada proteção dos direitos, promoção da dignidade humana e fortalecimento da unidade do ordenamento jurídico.

A LGPD representou um avanço significativo. No entanto, o longo período de *vacatio legis*, além de indicar a complexidade da adaptação às suas exigências, provocou revisões críticas que resultaram em alterações legislativas. A Medida Provisória nº 869, de 27 de dezembro de 2018, foi inicialmente editada para reformular densamente o texto original da norma. Consolidada posteriormente pela Lei nº 13.853, de 08 de julho de 2019, após diversas audiências públicas e intensos debates, essa legislação manteve alguns ajustes realizados, efetivou outros e recompôs o texto original em certos pontos. (Brasil, 2018)

A anonimização de dados pessoais emerge como uma prática essencial na LGPD, buscando equilibrar a necessidade de utilização de informações para diversas finalidades com a preservação da privacidade dos indivíduos. Este capítulo explora os conceitos, métodos e implicações da anonimização na LGPD, destacando as contribuições acadêmicas e práticas desse processo. A LGPD define anonimização como processo de utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Essa técnica visa permitir a utilização de dados para diversas finalidades sem comprometer a privacidade dos titulares. (Brasil, 2018)

Diversos métodos são empregados para a anonimização de dados pessoais, variando em complexidade e eficácia. A pseudonimização, técnica que substitui dados identificadores por códigos ou pseudônimos, é uma abordagem comum. Outras técnicas incluem generalização, perturbação, supressão e tokenização (Cabral, 2019):

- a) Pseudonimização: Substituição de dados identificadores por códigos ou pseudônimos, mantendo uma chave de correspondência segura.
- b) Generalização: Redução da precisão dos dados, agrupando informações mais específicas em categorias mais amplas.
- c) Perturbação (ou Ruído): Introdução de pequenas alterações nos dados para dificultar a identificação, sem comprometer a utilidade dos dados.
- d) Supressão: Remoção de partes dos dados que poderiam ser usadas para identificar uma pessoa, como remoção de colunas ou registros.
- e) Tokenização: Substituição de dados sensíveis por um token, um identificador único que não revela diretamente a informação original.

Além desses, encontra-se também:

- f) Hashing: Conversão irreversível de dados em uma sequência de caracteres alfanuméricos fixa, garantindo que o dado original não possa ser recuperado.
- g) Máscaras de Dados: Substituição de caracteres em uma string, preservando o formato geral da informação.
- h) Encriptação: Uso de algoritmos de criptografia para proteger os dados, sendo uma forma mais robusta de pseudonimização.
- i) Randomização: Introdução de variações aleatórias nos dados, tornando difícil a correlação com informações reais.
- j) Amostragem: Trabalhar com apenas uma parte representativa dos dados, reduzindo o escopo das informações disponíveis.

É importante notar que a escolha do método de anonimização depende do contexto específico, do tipo de dados e dos requisitos de privacidade. Com frequência, uma combinação de métodos é utilizada para garantir uma proteção mais eficaz. Além disso, é fundamental considerar a legislação de proteção de dados vigentes para garantir conformidade legal.

Apesar dos benefícios da anonimização, a LGPD reconhece que existem limites para sua eficácia, especialmente em um contexto de avanços tecnológicos. Desafios como a reidentificação, técnica que permite a associação de dados anonimizados a indivíduos, representam uma preocupação constante. Por isso, a LGPD incentiva a adoção de boas práticas na anonimização de dados, incluindo a realização de avaliações de impacto, a documentação adequada dos processos e a revisão periódica da eficácia das técnicas aplicadas.

A anonimização de dados pessoais representa uma ferramenta crucial na busca pelo equilíbrio entre a utilidade das informações e a proteção da privacidade na era digital. Embora desafios persistam, a LGPD fornece um arcabouço legal robusto que incentiva práticas transparentes e responsáveis na gestão de dados.

A anonimização de dados pessoais é uma prática que levanta uma série de considerações éticas e legais fundamentais, além de princípios norteadores, que tornam o processo mais correto e seguro.

A transparência é um princípio-chave da governança de dados e desempenha um papel crucial na construção da confiança dos usuários. Como afirmado por Cavoukian (2009):

[...] as organizações que realizam a anonimização de dados devem ser transparentes em relação aos métodos utilizados, assegurando que os indivíduos compreendam os processos pelos quais seus dados serão protegidos. Isso inclui a divulgação de informações sobre as técnicas de anonimização empregadas, os objetivos do processo e às potenciais limitações ou riscos associados à anonimização.

As organizações que coletam, processam e armazenam dados pessoais têm a responsabilidade de garantir a proteção da privacidade dessas informações. Isso inclui a implementação de medidas adequadas de segurança e privacidade, bem como a adoção de práticas de anonimização eficazes. Como destacado por Floridi e Taddeo (2016), as organizações devem realizar avaliações de risco para identificar e mitigar potenciais vulnerabilidades no processo de anonimização, além de estabelecer políticas claras e procedimentos para o tratamento responsável de dados pessoais.

3.3 ENCARREGADO (DATA PROTECTION OFFICER – DPO)

Neste item será abordado o papel fundamental do Encarregado de Proteção de Dados (DPO) no contexto da proteção e privacidade de dados pessoais. Serão discutidas suas responsabilidades, habilidades necessárias e sua importância na

conformidade com as regulamentações de proteção de dados, como o Regulamento Geral de Proteção de Dados e legislações correlatas.

O DPO, conforme apontado por Cate e Mayer-Schönberger (2013), é designado para desempenhar um papel crucial na organização, atuando como um ponto focal para questões relacionadas à proteção de dados. Suas responsabilidades incluem, mas não se limitam a:

- a) Monitorar a conformidade com o GDPR e outras leis de proteção de dados.
- b) Oferecer orientação e aconselhamento sobre práticas de privacidade de dados.
- c) Gerenciar solicitações de acesso a dados e direitos de indivíduos.
- d) Coordenar com autoridades de supervisão em questões relacionadas à proteção de dados.
- e) Conduzir avaliações de impacto à proteção de dados (DPIAs).
- f) Atuar como ponto de contato para comunicação com os titulares de dados e autoridades regulatórias.

O DPO deve possuir um conjunto específico de habilidades para desempenhar suas funções de forma eficaz. Segundo Schwartz, Solove e Citron (2016), algumas das habilidades essenciais incluem: conhecimento substancial das leis de proteção de dados, incluindo o GDPR e outras legislações locais; experiência em questões de conformidade e governança de dados; capacidade de comunicar-se eficazmente com partes interessadas internas e externas; competências analíticas para avaliar riscos à proteção de dados e propor medidas mitigatórias; capacidade de gerenciar conflitos e resolver problemas relacionados à privacidade de dados de forma ética e legal.

A presença de um DPO em uma organização desempenha um papel crítico na conformidade com o GDPR. De acordo com Van Alsenoy et al. (2018), sua *expertise* ajuda a garantir que a organização esteja alinhada com os princípios e requisitos estabelecidos no regulamento, minimizando assim o risco de violações de dados e possíveis penalidades.

Além disso, conforme destacado por Warren e Brandeis (1890), o DPO atua como um defensor da privacidade de dados dentro da organização, promovendo uma cultura de proteção de dados e garantindo que as políticas e práticas internas estejam em conformidade com as leis de proteção de dados aplicáveis.

3.4 CONSENTIMENTO

Um dos princípios fundamentais da proteção de dados pessoais é o consentimento informado do indivíduo. Como aponta Solove (2007), a anonimização de dados pode, em alguns casos, eliminar a necessidade de consentimento para o uso dessas informações, uma vez que os dados não podem mais ser atribuídos a um indivíduo específico. No entanto, é crucial considerar que nem todas as técnicas de anonimização garantem uma proteção completa da privacidade. Portanto, como delineado nas diretrizes do European Data Protection Board (2020), o consentimento dos indivíduos deve ser obtido sempre que possível, especialmente quando há dúvidas sobre a eficácia da anonimização ou quando os dados anonimizados ainda podem conter informações sensíveis que possam impactar a privacidade dos indivíduos.

Além disso, o consentimento é central para estabelecer uma relação de confiança entre as organizações e os titulares de dados, promovendo a transparência e a prestação de contas no tratamento das informações pessoais.

Apesar de sua importância, a obtenção do consentimento pode ser um processo complexo e desafiador. Diversos autores, como Acquisti (2004) e McDonald (2016), ressaltam que o consentimento nem sempre é obtido de forma genuína e voluntária, podendo ser influenciado por diversos fatores, como falta de transparência, linguagem complexa nos avisos de privacidade e a pressão social para aceitar termos de serviço. Ademais, com o avanço das tecnologias de rastreamento e coleta de dados, como observado por Turow (2012), torna-se cada vez mais difícil para os indivíduos compreenderem e controlarem o uso de seus dados, levantando questões sobre a eficácia do consentimento como mecanismo de proteção da privacidade.

É de suma importância reconhecer que o consentimento não é uma solução única para todos os desafios de privacidade de dados. Como salientado por Westin (1967), o consentimento pode ser limitado em sua eficácia, especialmente quando os indivíduos não têm alternativas reais ou quando a coleta e o uso de dados são considerados indispensáveis para a prestação de serviços. Além disso, como mencionado por Cavoukian (2009), o consentimento pode não ser suficiente para proteger os indivíduos em situações em que ocorrem práticas de processamento de dados prejudiciais ou abusivas.

4 BASES LEGAIS DE TRATAMENTO DE DADOS PESSOAIS

As bases legais de tratamento de dados pessoais são os fundamentos jurídicos nos quais uma organização pode se apoiar para realizar o processamento de dados pessoais de forma legítima, conforme estabelecido pela LGPD no Brasil. Existem diversas bases legais previstas na LGPD que legitimam o tratamento de dados pessoais, e cada uma delas deve ser analisada caso a caso para garantir que o processamento seja realizado de acordo com os princípios e diretrizes estabelecidos pela legislação. Algumas bases são de maior utilização, apresentam-se assim:

- a) **Consentimento:** O consentimento do titular dos dados é uma das bases legais mais conhecidas e utilizadas para o tratamento de dados pessoais. Para que o consentimento seja válido, deve ser fornecido de forma livre, informada e inequívoca pelo titular, mediante uma manifestação específica para a finalidade determinada. (Moraes, 2020)
- b) **Execução de Contrato:** O tratamento de dados pessoais é permitido quando necessário para a execução de um contrato do qual o titular dos dados é parte ou para a realização de diligências pré-contratuais a pedido do titular. (Lima, 2020)
- c) **Cumprimento de Obrigação Legal ou Regulatória:** O tratamento de dados pessoais é autorizado quando necessário para o cumprimento de obrigação legal ou regulatória pelo controlador.
- d) **Interesse Legítimo:** O tratamento de dados pessoais também pode ser realizado com base no legítimo interesse do controlador ou de terceiros, exceto nos casos em que os direitos e liberdades fundamentais do titular dos dados prevaleçam sobre esse interesse.
- e) **Proteção da Vida ou da Incolumidade Física:** O tratamento de dados pessoais é permitido quando necessário para a proteção da vida ou da incolumidade física do titular ou de terceiros.
- f) **Tutela da Saúde:** O tratamento de dados pessoais pode ser realizado para tutela da saúde, exclusivamente, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- g) **Estudos por Órgão de Pesquisa:** O tratamento de dados pessoais para fins de pesquisa acadêmica, científica ou estatística pode ser realizado por órgão de

pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

- h) Exercício Regular de Direitos em Processo Judicial, Administrativo ou Arbitral:
O tratamento de dados pessoais pode ser realizado para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Essas são algumas das bases legais de tratamento de dados pessoais previstas na LGPD. É importante ressaltar que o tratamento de dados pessoais deve sempre observar os princípios de boa-fé, transparência, finalidade, adequação, necessidade, livre acesso, segurança, prevenção, não discriminação e responsabilização, conforme estabelecido pela legislação.

4.1 AS HIPÓTESES TAXATIVAS DO ART. 7º DA LGPD

A Lei Geral de Proteção de Dados (LGPD), promulgada no Brasil em 2018, estabelece um marco regulatório abrangente para o tratamento de dados pessoais. Entre suas disposições, o artigo 7º enumera as hipóteses taxativas nas quais o tratamento de dados pessoais é permitido, mesmo sem o consentimento do titular. Este artigo se propõe a uma análise detalhada dessas hipóteses, destacando sua importância e implicações para a proteção da privacidade e dos direitos dos indivíduos. São elas:

- a) Cumprimento de obrigação legal ou regulatória pelo controlador (Alves, 2018):
permite que os controladores de dados processem informações pessoais quando necessário para cumprir obrigações legais ou regulatórias. Essa base legal é fundamental para garantir que as organizações possam operar dentro dos limites estabelecidos pela legislação vigente, assegurando o cumprimento de normas e regulamentos aplicáveis.
- b) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (Bioni, 2019): O artigo 7º também prevê a possibilidade de tratamento de dados pessoais para fins de pesquisa, desde que seja garantida a anonimização sempre que possível. Isso visa promover avanços científicos e tecnológicos, ao mesmo tempo em que protege a privacidade dos indivíduos envolvidos.
- c) Execução de políticas públicas previstas em leis e regulamentos (Vainzof, 2021): autoriza o processamento de dados pessoais para a execução de

políticas públicas estabelecidas por leis e regulamentos. Isso inclui medidas governamentais relacionadas à saúde, educação, segurança pública, entre outras áreas de interesse público.

- d) Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados. O tratamento de dados pessoais é permitido quando necessário para a execução de um contrato do qual o titular seja parte, ou para a realização de procedimentos preliminares relacionados a esse contrato. Isso garante que as partes envolvidas em transações comerciais possam cumprir seus compromissos contratuais de forma eficaz.
- e) Exercício regular de direitos em processo judicial, administrativo ou arbitral: autoriza o tratamento de dados pessoais no contexto de processos judiciais, administrativos ou arbitrais, garantindo o exercício regular de direitos por parte dos envolvidos nessas instâncias.
- f) Proteção da vida ou da incolumidade física do titular ou de terceiros: o tratamento de dados pessoais é permitido quando necessário para proteger a vida ou a integridade física do titular dos dados ou de terceiros. Essa base legal é crucial em situações de emergência ou de risco iminente à segurança das pessoas.
- g) Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias: autoriza o tratamento de dados pessoais no contexto de procedimentos relacionados à saúde, conduzidos por profissionais da área de saúde ou por entidades sanitárias. Isso inclui o diagnóstico, tratamento e monitoramento de condições médicas.
- h) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos: o tratamento de dados pessoais é permitido para garantir a prevenção à fraude e a segurança do titular, especialmente em processos de identificação e autenticação de cadastros em sistemas eletrônicos. Essa base legal visa proteger os indivíduos contra atividades fraudulentas e garantir a integridade e segurança de sistemas de informação.
- i) Proteção do crédito, inclusive quanto ao disposto na legislação pertinente: a LGPD permite o tratamento de dados pessoais para proteção do crédito,

conforme estabelecido na legislação pertinente. Isso inclui a análise de crédito, a prevenção à inadimplência e a gestão de riscos financeiros.

As hipóteses taxativas do artigo 7º da LGPD estabelecem as bases legais nas quais o tratamento de dados pessoais é permitido, mesmo sem o consentimento do titular. Essas disposições são fundamentais para garantir um equilíbrio entre a proteção da privacidade dos indivíduos e a promoção de atividades legítimas que dependem do uso de dados pessoais.

4.2 TRATAMENTO DOS DADOS SENSÍVEIS

Na era digital, a coleta, o armazenamento e o uso de dados são elementos essenciais para inúmeras atividades, desde transações comerciais até serviços de saúde e pesquisas científicas. No entanto, junto com os benefícios da tecnologia, surge uma preocupação crescente com a proteção da privacidade e dos direitos individuais, especialmente no que diz respeito aos chamados "dados sensíveis".

Os dados sensíveis referem-se a informações que, quando utilizadas de maneira inadequada ou não autorizada, podem causar danos significativos aos indivíduos, incluindo discriminação, violações de privacidade e riscos à segurança. Segundo a Lei Geral de Proteção de Dados (LGPD) brasileira, dados sensíveis são definidos como informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (Brasil, 2018).

A proteção dos dados sensíveis apresenta desafios significativos para empresas, governos e instituições em todo o mundo. Além das preocupações comuns relacionadas à segurança cibernética e à conformidade legal, existem implicações éticas e sociais a serem consideradas.

Na sequência aponta-se alguns desses desafios:

- a) Riscos à Privacidade e à Autonomia Individual: O uso indevido de dados sensíveis pode comprometer a privacidade e a autonomia dos indivíduos, tornando-os vulneráveis a práticas discriminatórias ou invasivas. Autores como Brunetto et al. (2020) destacam a importância de proteger a privacidade como um direito fundamental na era digital.

b) Desafios na Coleta e Armazenamento Seguro de Dados: A coleta e o armazenamento de dados sensíveis exigem medidas robustas de segurança cibernética para evitar violações e vazamentos de informações. Autores como Vainzof (2019) discutem a necessidade de implementar práticas de segurança eficazes para proteger os dados pessoais contra ameaças externas e internas.

c) Ética e Responsabilidade no Uso de Dados Sensíveis: O uso ético de dados sensíveis envolve considerações sobre consentimento informado, transparência e finalidade do uso. Autores como Biondi (2019) argumentam que as organizações devem adotar políticas e práticas que respeitem os direitos e interesses dos titulares de dados, promovendo a confiança e a legitimidade das operações de processamento de dados.

d) Regulamentação e Conformidade Legal: A LGPD e outras legislações de proteção de dados estabelecem diretrizes e obrigações para o tratamento de dados sensíveis. Autores como Alves (2018) analisam as disposições legais relacionadas à proteção de dados sensíveis, destacando a importância da conformidade e do monitoramento contínuo das práticas organizacionais.

A proteção dos dados sensíveis é um desafio complexo e multifacetado que requer ações coordenadas e abordagens holísticas por parte das organizações, governos e sociedade em geral. Ao adotar práticas de segurança cibernética robustas, promover uma cultura de ética e responsabilidade no uso de dados e garantir conformidade com as leis de proteção de dados, podemos avançar na construção de um ambiente digital seguro e confiável para todos.

O tratamento de dados sensíveis emerge como um desafio complexo, exigindo uma abordagem multidisciplinar que integre aspectos legais, éticos e técnicos. Questões éticas relacionadas ao tratamento de dados sensíveis são amplamente discutidas na literatura acadêmica. Autores como O'Neil (2016) e Noble (2018) destacam a importância de abordagens éticas e responsáveis na coleta e análise de dados, especialmente em contextos onde o uso de algoritmos pode perpetuar injustiças sociais.

Sabe-se que práticas de segurança da informação são fundamentais para proteger dados sensíveis contra ameaças internas e externas. A criptografia, o

controle de acesso e a anonimização são algumas das técnicas recomendadas. Além disso, a Gestão de Riscos e *Compliance* são abordagens proativas de gestão de riscos e conformidade com regulamentações são essenciais para garantir a conformidade no tratamento de dados sensíveis. Isso inclui a realização de avaliações de impacto à proteção de dados e a implementação de medidas adequadas de segurança e privacidade (ICO, 2018).

O tratamento de dados sensíveis requer uma abordagem abrangente que leve em consideração as dimensões legal, ética, técnica e de segurança. A literatura acadêmica e os marcos regulatórios fornecem orientações valiosas para organizações e profissionais que buscam garantir a proteção e a privacidade dos dados sensíveis em suas operações.

5 CONCLUSÃO

Observou-se que a eficácia da autodeterminação informativa prevista no inciso II, do art. 2º da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) é plausível, mas como direito fundamental não é absoluta. Portanto, é possível o tratamento de dados pessoais sem o consentimento do titular, desde que haja uma base legal para tal procedimento.

Mesmo sob esse ponto, a autodeterminação informativa marca o cenário da proteção de Dados no Brasil de forma positiva, sendo a LGPD exemplo para a proteção de dados, que desde 2018 (vigência) vem cumprindo o papel de esclarecer e consentir ao detentor de dados pessoais escolha sobre o uso dos dados ou não. Fazendo com que todos que entrem em contato com estes os usem de forma assertiva e dentro dos parâmetros estabelecidos pela lei 13.709. Já que antes dessa não havia uma lei específica sobre o tratamento de dados.

A lei referida no texto concede ao cidadão protagonismo no uso de seus dados com o objetivo de garantir o direito à privacidade, considerando os modelos adotados pela sociedade da informação. Ainda é passível de destaque, O artigo 18 da Lei Geral de Proteção de Dados (LGPD) estabelece a base legal que permite ao titular se opor ao tratamento de seus dados pessoais. De acordo com esta disposição, os titulares dos dados têm o direito de retirar o seu consentimento para o tratamento de dados pessoais a qualquer momento, mediante declaração clara, sendo garantido ao examinador facilitar o exercício desse direito. Isto significa que o titular dos dados pode opor-se ao tratamento dos seus dados pessoais se não consentir com as finalidades específicas do tratamento ou se já não desejar que os seus dados sejam tratados.

Mediante a uma preocupação, em relação a evolução da tecnologia e dos meios digitais, onde empresas como instagram, facebook, google, possuem amplo acesso às informações dos usuários, lei oferece proteção tanto em meio físico quanto digital, adaptando-se ao cenário atual onde o avanço da tecnologia acontece rapidamente. A introdução da lei também exige maior atenção aos dados sensíveis, a fim de reduzir o número de criminosos que aproveitam esta vulnerabilidade para cometer fraudes. A lei exige que as empresas (digitais ou não) desenvolvam políticas antivazamento e que a segurança da informação monitorize, proteja e preserve melhor

as informações às quais a empresa tem acesso. O descumprimento deverá resultar em multas de até 4% do faturamento anual da empresa, demonstrando rigorosamente o compromisso com as pessoas e o arcabouço legal de proteção de dados.

Nesse sentido, o Brasil dá um passo em direção à regulamentação da proteção de dados, das garantias e do respeito aos direitos fundamentais consagrados na Constituição Federal e garantidos pelas Nações Unidas, além de cumprir os padrões europeus de proteção por eles estabelecidos.

O assunto em destaque não finda-se aqui, visto a que a LGPD é recente no Brasil, ainda podendo ser otimizada baseada nas questões particulares do cidadão brasileiro, já que a Lei foi inspirada pela GPDR europeia. Fica pendente também na LGPD o controle dos dados anonimizados, visto os existentes estudos que vem demonstrando que existem mecanismos capazes de fazer com que esses dados saiam do anonimato. Tem-se o objetivo de criar um filtro para contrapor essa lacuna, que por hora está em aberto.

Perfaz-se, portanto, que a lei 13.709/2018, principalmente quando se trata da autodeterminação informativa, demonstra sim um marco satisfatório na proteção de dados pessoais, mas como toda lei, pode ser objeto de aprimoração.

REFERÊNCIAS

ACQUIST, Alessandro. Privacy in electronic commerce and the economics of immediate gratification. **Journal of Consumer Policy** 27.4 (2004): 395-418. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/30777892/Acquisti04-libre.pdf?1363437945=&response-content-disposition=inline%3B+filename%3DPrivacy_in_electronic_commerce_and_the_e.pdf&Expires=1717856828&Signature=E7g~s9DKypAaArr4JFLQ7Z39-dN2Tf0q32YOXaR-yFtibpQpuUQzpbO-cPCS8nBGyNLEuFW3E9pPTW01OhLYeLWTEfDivM307nl2C2J3mIMRDED~d69cy8LVk8sDbkpMRpRn2OMQ9ZQVT8HBG2V4AbgJgIDUPUvBgY2~IBJS8By4LuXwhVU7sfeSiosi16L-ssfaZ4uHuSGC1Vhp16PMtAb6UwNGCz4zeUaJu7ZOQirXyXaH2bUqKKhTBqjqCL2qIY9IJssQwT-3IJn-VAcWteDGthlCRlu7RmL8X3HZ1zGVLXI7pX5jJh8-92~kWszl8k7YfwSUd~gD6XBF8z8yXw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA Acesso em: 10 jun. 2024.

ALMEIDA, Poliana. **O limite da privacidade na internet durante uma investigação criminal**. Central de notícias Uninter, 2021. Disponível em: <https://www.uninter.com/noticias/existe-privacidade-na-internet-durante-uma-investigacao-criminal> Acesso em: 10 jun. 2024.

ALVES, Fabrício da Mota. **Artigo: Por que o debate sobre a regulação em proteção de dados já mudou tudo no Brasil**. ArpenPR, 2019. Disponível em: <https://www.arpenpr.org.br/site/conteudo-artigo/269> Acesso em: 10 jun. 2024.

BARROSO, Luís Roberto. A Nova Interpretação Constitucional: **Ponderação, Direitos Fundamentais e Relações Privadas**. Editora Renovar, 2003. Disponível em: <https://bdjur.stj.jus.br/jspui/handle/2011/26638?mode=full> Acesso em: 10 jun. 2024.

BIANI, Bruno. **Dados “anônimos” como antítese de dados pessoais**: o filtro da razoabilidade. Jus Brasil, 2019. Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/769068733/dados-anonimos-como-antitese-de-dados-pessoais-o-filtro-da-razoabilidade?ref=feed> Acesso em: 14 abr. 2023.

BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 1 ed. 2 Reimp. Rio de Janeiro: Forense, 2019.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. São Paulo: Forense, 2018.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: Set, 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 nov. 2023.

CIARELLI, Patrícia de Castro. **Entenda a lei geral de proteção de dados pessoais (LGPD)**. Migalhas, 2019. Disponível em: <https://www.migalhas.com.br/depeso/306801/entenda-a-lei-geral-de-protecao-de-dados-pessoais--lgpd> Acesso em: 14 abr. 2023.

CABRAL, Renato. **Anonimização de Dados Pessoais: Métodos e Desafios**. Editora Lumen Juris, 2019.

CATE, Fred H., e VICTOR Mayer-Schönberger. **Notice and consent in a world of big data**. International Data Privacy Law 3.2 (2013), p 67-73.

CAVOUKIAN, A. (2009). **Privacy by Design: The 7 Foundational Principles**. Information and Privacy Commissioner of Ontario, Canada. Disponível em: <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf> Acesso em: 10 jun. 2024.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS de 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos> Acesso em: 06 jun. 2024.

DWORKIN, Ronald. **Levando os Direitos a Sério**. São Paulo: Martins Fontes, 2002.

EUROPEAN DATA PROTECTION BOARD. (2020). **Guidelines 05/2020 on consent under Regulation 2016/679**. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf Acesso em: 03 jun. 2024.

FACHINI, Tiago. **LGPD: o vazamento de dados no caso Klara Castanho**. ProJuris, 2022. Disponível em: <https://www.projuris.com.br/blog/lgpd-caso-klara-castanho-2/> Acesso em: 10 jun. 2024.

FERRAZ, João Pedro Teixeira. **LGPD 101 - Comentários à Lei Geral de Proteção de Dados**. Jus Brasil, 2019. Disponível em: <https://joaopedrofteixeira.jusbrasil.com.br/artigos/753086549/lgpd-101-comentarios-a-lei-geral-de-protecao-de-dados?ref=feed> Acesso em: 14 abr. 2023.

FLORIDI, L., & Taddeo, M. **What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**. 2016. Disponível em: <https://royalsocietypublishing.org/doi/10.1098/rsta.2016.0360> Acesso em: 01 jun. 2024.

FROZZA, Alberto. **Manual da Lei Geral de Proteção de Dados: Aspectos Teóricos e Práticos da LGPD**. São Paulo: Thomson Reuters, 2020.

GARDE, Guilherme. **O paradoxo da privacidade e a LGPD**. Convergência digital, 2019. Disponível em: <https://www.convergenciadigital.com.br/OpiniaO/O-paradoxo-da-privacidade-e-a-LGPD-51507.html?UserActiveTemplate=site>
Acesso em: 14 abr. 2023.

GARRUTE, Mateus Mello; SCHIMIDT, Estela. **A proteção de dados pessoais no Brasil e as perspectivas na importação internacional de dados da Europa**. Migalhas, 2018. Disponível em: <https://www.migalhas.com.br/depeso/286440/a-protecao-de-dados-pessoais-no-brasil-e-as-perspectivas-na-importacao-internacional-de-dados-da-europa> Acesso em: 14 abr. 2023.

GOMES, Renan Macedo. **A Proteção da Privacidade na Era Digital: Desafios e Perspectivas no Direito Constitucional Brasileiro**. JusBrasil, 2024. Disponível em: <https://www.jusbrasil.com.br/artigos/a-protecao-da-privacidade-na-era-digital-desafios-e-perspectivas-no-direito-constitucional-brasileiro/2493085233> Acesso em: 10 jun. 2024.

ICO. **Guide to the General Data Protection Regulation (GDPR)**. Information Commissioner's Office. 2018. Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf> Acesso em: 10 jun. 2024.

JHERING, Rudolf von. **A Finalidade do Direito**. São Paulo: RT, 2013.

JUNIOR, José. M. F; MARTINS, Guilherme. M. **Proteção de dados e anonimização :perspectivas à luz da lei nº 13.709/2018**. Revista Estudos Institucionais, 2021. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/476/681>
Acesso em: 10 jun. 2024.

KANT, Immanuel. **Fundamentação da Metafísica dos Costumes**. Petrópolis: Vozes, 2012.

LIMA, Ana.. **Revista de Privacidade e Proteção de Dados**, 2021. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf Acesso em: 10 jun. 2024.

LIMA, E. de O. **Lei Geral de Proteção de Dados: Comentários Artigo por Artigo** (1ª ed.). Rio de Janeiro: Lumen Juris, 2020.

LIMA, Victor Henrique Pereira. **LGPD análise dos impactos da implementação em ambientes corporativos**: estudo de caso. Trabalho de Conclusão de Curso apresentado à Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás. Orientador: Fábio Barbosa Rodrigues. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/108/1/LGPD%20-%20ANALISE%20DOS%20IMPACTOS%20DA%20IMPLEMENTAC%CC%A7A%CC%83O%20-%20003-12%20-%20final.pdf> Acesso em: 10 nov. 2023.

MCDONALD, Andrew M. **Consent**: An unacceptable privacy risk. Ethics and Information Technology 18.1 (2016): p. 5-14.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. Disponível em: <https://ojs.unifor.br/rpen/article/view/10828/pdf> Acesso em: 10 nov. 2023.

MENDONÇA, Suzana. **A autodeterminação informativa no contexto de proteção de dados pessoais**. Disponível em: <https://www.conjur.com.br/2019-out-20/suzana-mendonca-autodeterminacao-informativa-protecao-dados> Acesso em: 25 mar. 2023.

MICHELETTI, Miquéias; BORGES, Túlio Tito. **LGPD: o abismo entre a teoria e a prática: comentada, artigo por artigo**. 1. Ed. Paulínia: Ed. Do Autor, 2021. (Livro eletrônico) Disponível em: https://cdljundiai.com.br/wp-content/uploads/2021/09/LGPD-O-ABISMO-ENTRE-A-TEORIA-E-A-PRATICA_202102231600.pdf Acesso em: 10 nov. 2023.

MORAES, Ronaldo. **Lei Geral de Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018**. São Paulo: Revista dos Tribunais, 2018.

MORAES, G. C. **LGPD: Lei Geral de Proteção de Dados comentada**. 1ª ed. São Paulo: Revista dos Tribunais, 2020.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP**. Cadernos Adenauer, Rio de Janeiro, n. 3, p. 113-136, out. 2019.

NOGUEIRA, Octavio. **Proteção de Dados Pessoais: A Lei nº 13.709/2018**. Salvador: Juspodivm, 2018.

NUSSBAUM, Martha. **A Fragilidade da Liberdade: Ensaios sobre Direitos, Igualdade e Reivindicações**. São Paulo: Martins Fontes, 2004.

O QUE É BIG DATA. OCI. Disponível em: <https://www.oracle.com/br/big-data/what-is-big-data/#:~:text=A%20defini%C3%A7%C3%A3o%20de%20big%20data,de%20novas%20fontes%20de%20dados>. Acesso em: 10 jun. 2024.

PERGUNTAS FREQUENTES – ANPD. Gov.br, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd> Acesso em: nov, 2023.

POLLA, Rafael Montilla. **A proteção dos dados pessoais como fundamento do livre desenvolvimento da personalidade**. Dspace. Disponível em: <https://acervodigital.ufpr.br/handle/1884/67831> Acesso em: 14 abr. 2023.

KOCH, Richie. **LGPD: a versão brasileira do regulamento europeu**. Gov.br, 2019. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais> O conteúdo desse site foi traduzido do inglês com autorização do GDPR.EU, portal que originalmente publicou o conteúdo. Disponível em: <https://gdpr.eu/gdpr-vs-lgpd/> Acesso em: 10 jun. 2024.

QUEIROZ, João Quinelato de. **Cidadão tem direito de ter controle sobre coleta de dados pessoais**. Conjур, 07.2015. Disponível em: https://www.conjur.com.br/2015-jul-26/joao-queiroz-cidadao-direito-controle-coleta-dados-pessoais#_ftn12 Acesso em: 03 nov. 2023.

RADBRUCH, Gustav. **Introdução à Filosofia do Direito**. São Paulo: Forense, 2008.

RAPÔSO, Cláudio F L et al. LGPD: Lei geral de proteção de dados pessoais em tecnologia da informação. Revisão Sistemática. **RACE Revista da Administração**, v. 4, p. 58-67, 2019.

RAPÔSO, Cláudio F L et al. LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática. **RACE Revista da Administração**, v. 4, p. 58-67, 2019.

REIS, Jessica Cabrera. **O encarregado de proteção de dados na lei geral de proteção de dados sob o paradigma da general data protection**. Repositório institucional Univem, 2020. Disponível em: <https://aberto.univem.edu.br/handle/11077/1939> Acesso em: 10 jun. 2024.

ROCHA, Fernando. **Anonimização de Dados Pessoais: Diretrizes para Implementação**. São Paulo: Forense, 2018

RODOTÀ, Stefano. **A vida na sociedade da vigilância**. (coord. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, 2008, p. 113.

ROZA, Thiago. **Proteção de Dados Pessoais: Aspectos Teóricos e Práticos da Lei Geral de Proteção de Dados**. Salvador: Juspodivm, 2020.

SANCIONADA COM VETOS LEI GERAL DA PROTEÇÃO DE DADOS PESSOAIS. Agência Senado, 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais> Acesso em: 10 jun. 2024.

SARLET, Ingo Wolfgang. **Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado, 2016.

Schwartz, Paul M., Daniel J. Solove, e Daniel J. Citron. **Data protection law: An overview**. Congressional Research Service, 2019, p. 7. Disponível em: <https://crsreports.congress.gov/product/pdf/R/R45631> Acesso em: 10 jun. 2024.

SOLOVE, D. J. "I've Got Nothing to Hide" and Other Misunderstandings of **Privacy**. San Diego Law Review, 44(4), p. 745-772. 2007.

SOLOVE, Daniel J. **A taxonomy of privacy**. University of Pennsylvania Law Review (2006): p. 477-564.

TEIXEIRA, João Pedro Ferraz. **LGPD 101: Comentários à Lei Geral de Proteção de Dados**. 2019. Disponível em: <https://www.jusbrasil.com.br/artigos/lgpd-101->

comentarios-a-lei-geral-de-protecao-de-dados/753086549 Acesso em: 10 nov. 2023.

TUROW, Joseph. **The daily you: How the new advertising industry is defining your identity and your worth.** Yale University Press, 2012. Disponível em: <file:///C:/Users/Ana%20Carolina/Downloads/ReviewofTheDailyYou-Peters.pdf> Acesso em: 10 jun. 2024.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119 (2016): p. 1-88.

VAN ALSENOY, Brendan, et al. **Dealing with data breaches under the General Data Protection Regulation:** Towards a new equilibrium in favour of data subjects?." *International Data Privacy Law* 8.4 (2018): p. 263-284.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard law review** 4.5 (1890): p. 193-220.

VAINZOF, Rony. Direito Digital: Lei Geral de Proteção de Dados Pessoais (LGPD). *Conjur*, 2021. Disponível em: <https://www.conjur.com.br/2021-jun-28/rony-vainzof-lgpd-relatorio-impacto-protecao-dados/> Acesso em: 10 jun. 2024.

WANG, Daniel D. **Lei Geral de Proteção de Dados:** Manual Jurídico para a LGPD. Leme: Mundo Jurídico, 2019.

WESTIN, Alan F. **Privacy and freedom.** 1967. Disponível em: <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr> Acesso em: 10 jun. 2024.