UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS
GRADUAÇÃO EM DIREITO

RAFAEL AGUIAR DE ARAÚJO

PROTEÇÃO DE DADOS SENSÍVEIS EM CONTEXTOS DE CRISE: UMA ANÁLISE JURÍDICA DA LGPD E O INCIDENTE DO E-SUS NOTIFICA

Cidade de Goiás
2024

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): Rafael Aguiar de Araújo

Título do trabalho: Proteção de dados sensíveis em contextos de crise: uma análise jurídica da LGPD e o incidente do E-SUS notifica

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Bruna Pinotti Garcia**, **Professora do Magistério Superior**, em 17/02/2025, às 14:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Rafael Aguiar De Araújo**, **Discente**, em 19/02/2025, às 12:44, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5165105** e o código CRC **31316DDC**.

Referência: Processo nº 23070.004354/2024-81 SEI nº 5165105

RAFAEL AGUIAR DE ARAÚJO

PROTEÇÃO DE DADOS SENSÍVEIS EM CONTEXTOS DE CRISE: UMA ANÁLISE JURÍDICA DA LGPD E O INCIDENTE DO E-SUS NOTIFICA

Monografia jurídica apresentada à Unidade Acadêmica Especial de Ciências Sociais Aplicadas da Regional Goiás da Universidade Federal de Goiás, como trabalho de conclusão do curso de bacharelado em Direito, sob a orientação da Profa. Dra. Bruna Pinotti Garcia.

Cidade de Goiás
2024

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Araújo, Rafael Aguiar de
Proteção de dados sensíveis em contextos de crise: uma análise jurídica da LGPD e o incidente do E-SUS notifica [manuscrito] / Rafael Aguiar de Araújo. - 2024.
78 f.

Orientador: Profa. Dra. Bruna Pinotti Garcia.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas, Direito, Cidade de Goiás, 2024.

1. Lei Geral de Proteção de Dados. 2. Dados Sensíveis. 3. e-SUS Notifica. 4. Teoria Tridimensional do Direito. 5. Privacidade. I. Garcia, Bruna Pinotti, orient. II. Título.

CDU 34

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos trinta dias do mês de janeiro do ano de dois mil e vinte e quatro iniciou-se a sessão pública de defesa do Trabalho de Conclusão de Curso (TCC) intitulado “Proteção de dados sensíveis em contextos de crise: uma análise jurídica da LGPD e o incidente do E-SUS notifica”, de autoria de Rafael Aguiar de Araújo, do curso de Direito, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas da UFG. Os trabalhos foram instalados pela Bruna Pinotti Garcia – orientadora (UAECSA-CG/UFG) com a participação dos demais membros da Banca Examinadora: Profa. Dra. Sofia Alves Valle Ornelas (UAECSA-CG/UFG) e Profa. Dra. Renata Botelho Dutra (UAECSA-CG/UFG). Após a apresentação, a banca examinadora realizou a arguição do(a) estudante. Posteriormente, de forma reservada, a Banca Examinadora deliberou, tendo sido o TCC considerado aprovado.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Renata Botelho Dutra**, **Professora do Magistério Superior**, em 17/02/2025, às 11:21, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Bruna Pinotti Garcia**, **Professora do Magistério Superior**, em 17/02/2025, às 14:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Sofia Alves Valle Ornelas**, **Professora do Magistério Superior**, em 24/02/2025, às 17:50, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5165138** e o código CRC **B86A4E24**.

Referência: Processo nº 23070.004354/2024-81 SEI nº 5165138

AGRADECIMENTOS

Primeiramente, gostaria de expressar minha profunda gratidão à minha família, em particular aos meus pais, pelo amor incondicional, apoio e incentivo, sem os quais este trabalho não seria possível. Obrigado por acreditarem em mim, especialmente nos mais desafiadores.

À minha orientadora, Bruna Pinotti Garcia, minha sincera gratidão por sua paciência, sabedoria e orientação. Seu apoio e conselhos foram fundamentais para o desenvolvimento e conclusão deste trabalho.

Gostaria de dedicar um agradecimento muito especial à minha namorada, cujo apoio, compreensão e amor foram fundamentais ao longo desta jornada. Sua presença constante, incentivo e paciência não apenas aliviaram os desafios enfrentados durante a elaboração desta monografia, mas também trouxeram alegria e motivação nos momentos mais difíceis. Seu companheirismo incansável foi uma fonte de força e inspiração, e sou profundamente grato por cada momento compartilhado e cada palavra de encorajamento.

Aos meus amigos e colegas, agradeço por transformarem os dias de estudo em momentos inesquecíveis. Suas risadas, discussões enriquecedoras e companheirismo tornaram cada desafio mais leve. A cidade de Goiás ganhou um significado especial graças à presença de vocês. Cada um de vocês contribuiu não apenas para minha jornada acadêmica, mas também para quem sou como pessoa. Ensinaram-me que o mundo é mais belo quando compartilhado com as pessoas certas, independentemente das circunstâncias. Obrigado por serem meu porto seguro nos momentos difíceis

Cada um de vocês fizeram parte do que eu sou hoje, não somente academicamente, mas como pessoa, me ensinando como o mundo pode ser belo desde que esteja acompanhado pelas pessoas certas, independente de onde ou quão difíceis estão as coisas.

Este trabalho é uma manifestação do esforço conjunto e do apoio generoso de cada um de vocês. Muito obrigado por serem parte essencial desta conquista significativa em minha vida acadêmica.

“Numa psicanálise, descobre-se que a vida adulta é sempre menos adulta do que parece: ela é pilotada por restos e rastros da infância”.

(Contardo Calliris)

RESUMO

Esta monografia investiga a proteção de dados pessoais sensíveis no contexto da Lei Geral de Proteção de Dados (LGPD), com enfoque específico no incidente ocorrido no sistema e-SUS Notifica. O estudo se inicia com um exame das origens e fundamentos da LGPD, inserindo a legislação no panorama das mudanças globais relativas ao direito digital e à privacidade de dados. O texto analisa em profundidade o direito à privacidade conforme estabelecido na LGPD, discutindo as definições e o tratamento legal de dados pessoais e sensíveis, particularmente no setor de saúde. Utilizando o prisma da Teoria Tridimensional do Direito de Miguel Reale, o trabalho reflete sobre a necessidade de uma abordagem jurídica que integre normas, fatos e valores, visando a adaptabilidade e eficácia na proteção de dados em um ambiente digital em constante evolução. A monografia destaca a relevância da implementação efetiva de programas de governança em privacidade de dados, ressaltando as consequências da falta de medidas preventivas e os riscos associados à dignidade humana. Esta pesquisa contribui para o entendimento crítico da LGPD e suas implicações práticas, propondo reflexões sobre a adequação das normativas atuais frente aos desafios tecnológicos e sociais contemporâneos, e enfatizando a importância de um sistema jurídico que acompanhe a dinâmica da sociedade digital.

Palavras-chave: Lei Geral de Proteção de Dados; Dados Sensíveis; e-SUS Notifica; Teoria Tridimensional do Direito; Privacidade.

ABSTRACT

This monograph explores the protection of sensitive personal data under Brazil's General Data Protection Law (LGPD), focusing specifically on the incident in the e-SUS Notifica system. The study begins with an examination of the origins and underpinnings of the LGPD, placing the legislation within the context of global changes related to digital law and data privacy. It thoroughly analyzes the right to privacy as established by the LGPD, discussing the definitions and legal treatment of personal and sensitive data, particularly in the healthcare sector. Employing Miguel Reale's Three-Dimensional Theory of Law, the research contemplates the necessity for a legal approach that integrates norms, facts, and values to ensure adaptability and effectiveness in data protection in an ever-evolving digital environment. The monograph underscores the importance of effectively implementing data privacy governance programs, highlighting the consequences of a lack of preventive measures and the risks to human dignity. This research contributes to a critical understanding of the LGPD and its practical implications, offering insights into the adequacy of current regulations in the face of contemporary technological and social challenges, and emphasizing the need for a legal system that keeps pace with the digital society's dynamics.

Keywords: General Data Protection Law, Sensitive Data, e-SUS Notifica, Three-Dimensional Theory of Law, Privacy.

SUMÁRIO

INTRODUÇÃO

A proteção de dados pessoais e privacidade emergiu como um problema crucial em um mundo globalmente interconectado onde a interdependência digital tornou-se uma parte essencial da sociedade moderna. Isso afeta não apenas os marcos legais e tecnológicos, mas também o cotidiano das pessoas. Esta pesquisa examina as particularidades da Lei Geral de Proteção de Dados (LGPD) do Brasil e examina como ela é aplicável e eficaz em um caso particular de vazamento de dados sensíveis no sistema e-SUS Notifica. O trabalho é guiado pela Teoria Tridimensional do Direito de Miguel Reale. Essa teoria integra fatos, valores e normas jurídicas para fornecer uma compreensão mais profunda da paisagem jurídica digital.

A humanidade experimentou uma mudança sem precedentes desde o surgimento da internet até a sociedade da informação atual. A necessidade de regulamentação adequada tornou-se evidente à medida que a tecnologia avança em um ritmo incontrolável, especialmente após incidentes que mostram falhas na proteção de dados e vulnerabilidades dos sistemas. A LGPD foi promulgada como um marco na legislação brasileira, visando equilibrar a proteção da privacidade individual e a promoção de um acesso transparente e ético às informações. Desde o amanhecer da internet até o estado atual da sociedade da informação, a humanidade testemunhou uma evolução sem precedentes.

À medida que a tecnologia avança em um ritmo implacável, a necessidade de regulamentação adequada tornou-se evidente, particularmente na esteira de incidentes que expuseram lacunas na proteção de dados e destacaram a vulnerabilidade dos sistemas.

Este estudo busca compreender como a LGPD funciona como um instrumento normativo adaptado às necessidades contemporâneas, explorando suas origens, evolução e aplicabilidade em casos específicos de violações de dados, particularmente em situações de crise. A problemática central deste estudo envolve investigar como vazamentos de dados no setor de saúde, como os que ocorreram no sistema e-SUS Notifica, expõem lacunas existentes e desafios na proteção efetiva de dados pessoais sensíveis, destacando a necessidade da LGPD ser adaptada aos problemas atuais, de acordo com a Teoria Tridimensional do Direito.

A monografia em questão se divide em três capítulos principais, abordando diferentes aspectos da Lei Geral de Proteção de Dados (LGPD) e seu impacto na sociedade digital contemporânea.

No Capítulo 1 intitulado "Origens da LGPD" examina as origens e a necessidade de uma lei de proteção de dados no Brasil, contextualizando-a dentro das mudanças globais no direito digital e na privacidade de dados. Ele analisa o despertar do direito digital, a necessidade

de regulação e a importância do entendimento histórico e das influências internacionais que moldaram an LGPD, além de discutir o papel crucial da norma jurídica e a aplicação da Teoria Tridimensional do Direito na proteção de dados. Este capítulo também se aprofunda no debate da proteção de dados no direito europeu, traçando a evolução da regulação da privacidade e proteção de dados na União Europeia, desde as primeiras legislações relacionadas à proteção de dados até a atual RGPD (Regulamento Geral de Proteção Dados), haja vista a clara influência que esta exerceu para o desenvolvimento da LGPD. Além disso, enfatiza a necessidade de harmonizar normas, fatos e valores sociais, destacando a Teoria Tridimensional do Direito de Miguel Reale como um alicerce para an adaptação jurídica no ambiente digital.

O Capítulo 2 se intitula "O Direito à Privacidade e a LGPD", a monografia discute o imperativo jurídico e social da proteção de dados pessoais na era digital, aprofundando-se na LGPD no cenário jurídico brasileiro e internacional. Este capítulo aborda os fundamentos da LGPD, incluindo a importância do consentimento, transparência, e prestação de contas no tratamento de dados pessoais. Explora como an LGPD se alinha com os princípios constitucionais e éticos, destacando a responsabilidade dos agentes de tratamento e o reforço dodireito à privacidade e à não discriminação dos titulares dos dados. Além disso, discute-se a estrutura da LGPD e o novo paradigma que ela representa, aprofundando-se nos fundamentos e na estrutura da lei, e analisando como ela se relaciona com o desenvolvimento econômico e tecnológico, a inovação, e os direitos fundamentais. Em suma, o capítulo explora a resposta legal às transformações na era digital, sublinhando a interação entre a LGPD, princípios éticos, morais e legais existentes, e as responsabilidades e obrigações impostas pela legislação.

O Capítulo 3 da monografia intitulado "Delineando Dados Pessoais e Dados Pessoais Sensíveis: Uma Visão sob a LGPL" é uma análise sobre a complexidade dos dados pessoais, com ênfase particular nos dados sensíveis, dentro do contexto da Lei Geral de Proteção de Dados (LGPD).

do direito à privacidade e à não discriminação dos titulares dos dados. Além disso, discute-se a estrutura da LGPD e o novo paradigma que ela representa, aprofundando-se nos fundamentos e na estrutura da lei, e analisando como ela se relaciona com o desenvolvimento econômico e tecnológico, a inovação, e os direitos fundamentais. Em suma, o capítulo explora a resposta legal às transformações na era digital, sublinhando a interação entre a LGPD, princípios éticos, morais e legais existentes, e as responsabilidades e obrigações impostas pela legislação.

O Capítulo 3 da monografia intitulado "Delineando Dados Pessoais e Dados Pessoais Sensíveis: Uma Visão sob a LGPD" é uma análise sobre a complexidade dos dados pessoais,

com ênfase particular nos dados sensíveis, dentro do contexto da Lei Geral de Proteção de Dados (LGPD). Inicialmente se discute sobre a natureza e a classificação de dados pessoais e sensíveis, destacando sua relevância no cenário digital contemporâneo, especialmente os sensíveis como informações de saúde e genéticas, que evoluíram para além de simples identificadores para se tornarem ativos econômicos valiosos na era do capitalismo de vigilância. O texto aborda as implicações éticas, legais e sociais da gestão desses dados, especialmente no que se refere à saúde pública, destacando o incidente de vazamento de dados no sistema e-SUS Notifica como um estudo de caso para ilustrar os desafios e as vulnerabilidades presentes na proteção de informações sensíveis. A discussão se aprofunda na relação entre a coleta e o uso desses dados e os direitos fundamentais das pessoas, incluindo a privacidade e a autodeterminação informativa.

O método utilizado para a produção deste trabalho foi o método analítico-dedutivo, fazendo uso do pensamento hermenêutico para a análise das disposições legais da LGPD, complementada por uma revisão de literatura abrangente sobre teorias jurídicas, como a Teoria Tridimensional do Direito de Miguel Reale, e estudos de caso relevantes. Essa escolha se deu pelo fato de que o método analítico-dedutivo é uma abordagem lógica que parte de premissas gerais para chegar a conclusões específicas, sendo valioso para a investigação de questões objetivas e quantitativas. O pensamento hermenêutico, por outro lado, se concentra na interpretação de textos e significados sociais e culturais, sendo essencial para compreender a profundidade e a complexidade das questões sociais e culturais envolvendo o tema. Ao combinar essas abordagens, o estudo se beneficia de uma investigação mais completa e eficiente, permitindo uma compreensão detalhada dos fenômenos investigados.

Já se tratando da metodologia a ser utilizada, tendo a especificidade e contemporaneidade do tema proposto nos valermos da pesquisa documental, bibliográfica e do estudo de caso. Essa escolha se dá porque, de acordo com Yin (2014), a combinação de pesquisa bibliográfica, documental e estudo de caso é uma metodologia adequada para aprofundar o conhecimento sobre o assunto proposto e avaliar a sua aplicabilidade na realidade. A pesquisa bibliográfica permite revisar fontes escritas sobre o assunto, como livros, artigos científicos, dissertações e teses, para obter uma visão geral e detalhada do tema. Já a pesquisa documental é utilizada para analisar documentos oficiais, legislações e regulamentos relacionados ao tema. Por fim, o estudo de caso é uma abordagem que permite aprofundar o conhecimento sobre uma situação real, identificando as particularidades e as possibilidades de solução. Segundo Yin (2014), a combinação dessas três abordagens fornece uma base sólida para a compreensão do assunto proposto e sua aplicabilidade na realidade.

Em resumo, este trabalho não apenas destaca a importância crítica da proteção de dados pessoais sensíveis, mas também busca promover uma reflexão sobre a eficácia das respostas jurídicas atuais e futuras frente aos desafios impostos pela sociedade digital. Assim diante uma análise tridimensional, podemos entender que embora existam lacunas e desafios na proteção de dados pessoais sensíveis, especialmente em situações de crise de saúde pública, evidenciando uma necessidade de uma constante adaptação e evolução da LGPD e demais normas para garantir que a dignidade e a privacidade sejam preservadas em um mundo cada vez mais dominado pela tecnologia e pelos dados.

CAPÍTULO 1 – ORIGENS DA LGPD

Em um mundo onde a interconexão digital tornou-se a norma, a proteção e o tratamento de dados pessoais emergem como questões cruciais, moldando não apenas o panorama legal e tecnológico, mas também afetando profundamente a vida cotidiana dos indivíduos.

Este capítulo se propõe a explorar, dissecar e entender as múltiplas facetas da Lei Geral de Proteção de Dados (LGPD) no Brasil, situando-a no contexto mais amplo das mudanças globais no direito digital e na privacidade de dados. Através dos capítulos, mergulharemos em uma jornada que atravessa as origens históricas e influências internacionais que moldaram a LGPD.

1.1 Despertar do Direito Digital Rumo à Regulação

Inicialmente, ao começarmos a entender o direito digital precisamos falar sobre suas origens e necessidade para que assim possamos compreender sobre aquilo que ele versa, quais seus objetivos e as lacunas que enfrentamos no presente.

O que conhecemos hoje como Internet, na década de 50, não passava de uma concepção geral, um sonho a ser desenvolvido, porém, atualmente esta é considerada indispensável para o funcionamento da sociedade como conhecemos hoje, um avanço descomunal para o curto período que a Internet esta presente.

A Internet molda a sociedade em que vivemos, e é evidente que as atividades online estão se tornando cada vez mais predominantes em vários aspectos da vida. Como resultado, a maneira como interagimos, negociamos, estudamos e, no geral, nos comportamos na sociedade evoluiu. Essas mudanças que não começaram hoje são a principal razão pela qual precisamos proteger nossos direitos de individualidade e privacidade.

O profissional do direito atualmente, seja pela necessidade pratica de integrar-se no meio digital pelos sistemas de processo digital, estes sendo a maneira quase exclusiva pela qual o Judiciário tem exercido suas funções, ou pela necessidade de adequação aos novos conceitos e relação interpessoais dos quais o direito tece suas normas, tem a obrigação de estar em sintonia com as transformações que ocorrem na sociedade, esse novo papel do jurista na sociedade digital, reforça que este não pode tratar apenas dos fatos reais frios, as normas e burocracia do direito, mas deve ater-se também aos demais fatores sociais das quais versam as normas. (PECK, 2002)

Assim, visando a harmonia social, é crucial que os indivíduos e as instituições por eles criadas tenham acesso a direitos e cumpram deveres previamente estabelecidos. Desse modo, a

implementação e o subsequente cumprimento de normas legalmente estabelecidas surgem como meios socialmente legitimados para assegurar que cidadãos e órgãos institucionais permaneçam em equilíbrio na estrutura normativa da sociedade, incidindo então diretamente na teoria tridimensional do direito de Miguel Reale.

Isso se dá, pois sob o viés de Reale, tem-se que a norma somente tem uma eficácia real quando se encontra em conformidade com valores de uma sociedade, assim as normas são as regras jurídicas que estabelecem proteção a direitos que diante os fatos sociais, pelos quais uma comunidade está vivenciando, adquirem valor.

Nesse contexto, a elaboração de regimentos específicos se torna imperativa para mitigar riscos e proteger os direitos individuais no ambiente digital.

Assim, se o jurista fazer uso da Teoria Tridimensional do direito, fara com que as normas e decisões proferidas, sejam mais versáteis e maleáveis às condicionantes sociais, sendo esta uma necessidade intrínseca para solução dos conflitos no âmbito digital, pois como é concebido por Patricia Peck em sua obra "Direito Digital" (2021) autora está que nos acompanhara durante todo o capítulo: "Toda mudança tecnológica é uma mudança social, comportamental, portanto jurídica"

Portanto, seguindo as recomendações do historiador e geógrafo grego Heródoto, somente conhecendo o passado poderemos entender o presente, ou seja, para entender as condicionantes sociais, que vivenciamos hoje é necessário retornarmos ao passado. Desta forma devemos direcionar nossos pensamentos de volta ao ponto onde a sociedade começou a mudar pela influência das tecnologias de forma exponencial, momento esse reconhecido por Alvin Toffler em sua obra "*The third wave*" de 1980, como a Terceira Onda, sendo este um dos três momentos da evolução da sociedade humana. Ao examinar as mudanças sociais e econômicas ao longo do tempo, Toffler, passa a dividir a história do desenvolvimento humano em três ondas, divisão esta que passa a ser amplamente adotada e passou a estar presente no cotidiano da mídia, do meio acadêmico e empresarial. (PECK, 2020)

Para resumir, a Primeira Onda, também conhecida como a Era Agrícola, foi quando a terra era a principal forma de capital. Foi uma maneira de ganhar dinheiro cultivando a terra e exigia pouco conhecimento de plantio e trabalho físico. Começou com a Revolução Agrícola no Neolítico, que levou as pessoas a sedentarizar. A Segunda Onda começou com a Revolução Industrial e foi marcada pela industrialização dos meios de produção baseados em capital e bens tangíveis, como petróleo, aço e máquinas. A Segunda Guerra Mundial foi seu melhor momento. Finalmente, chegamos à Terceira Onda, o assunto que mais nos interessa neste estudo. Ela começou durante a Segunda Guerra Mundial com o surgimento da comunicação em massa. Isso

deu origem à Era da Informação, que teve como característica a grande disseminação de informações por meio dos meios de comunicação em massa. (PECK, 2020)

Foi nesse momento que a informação começou a ser o principal instrumento de poder e riqueza, pois nas concepções de Nicholas Negroponte, aqueles que detinham a informação ou faziam o tratamento dessas informações obtinham uma riqueza inesgotável, haja vista que uma informação poderia ser vendidas inúmeras vezes. (PECK, 2021)

Assim, aqueles que obtinham ou processavam as informações, ou dados mais rapidamente obtinham vantagem sobre os demais, é nesse contexto que a humanidade passou a buscar formas cada vez mais rápidas de processar essa matéria bruta que seriam os dados, para se obter um produto final que seria o conhecimento.

Este anseio da humanidade de tornar-se mais eficiente e rápido em uma tarefa específica, no caso deste estudo, o processamento de dados/informações, transcende a história da humanidade, sendo uma característica intrínseca do ser humano. Desejo este que culminou no ponto atual onde, diante os enormes avanços tecnológicos da humanidade, temos acesso aos computadores e a internet, que por mais que sejam questões que muitas vezes não damos a devida importância, em razão de estarem tão ligadas ao nosso cotidiano, tem uma profundidade inimaginável, haja vista que para que chegássemos nesse ponto precisamos passar por diversos avanços, passando por diversos outros instrumentos, haja vista que a busca pela eficiência no processamento de dados tem uma longa história a exemplo disso temos o ábaco, um instrumento matemático, com provável origem na Mesopotâmia há mais de 5500 anos a.C. (PECK, 2020)

Desde o ábaco passamos por diversas ferramentas de processamento de dados e a internet é uma dessas, esta pode ser conceitualizada como uma grande rede de dispositivos interligados entre si mediante protocolos. Pode ser considerado um conceito relativamente simples, porém a complexidade da internet se dá pelos efeitos causados pela mesma.

Orientados pelas lições de Manuel Castells, em suas reflexões sobre a Internet, cabe destacar não apenas sua evolução tecnológica, mas também suas implicações sociais, econômicas e culturais, transformando profundamente a sociedade contemporânea.(CASTELLS, 2006)

A Internet, originada no projeto *Arpanet* em 1969 pelo Departamento de Defesa dos Estados Unidos, surgiu com o propósito inicial de consolidar a comunicação entre computadores, impulsionada pela necessidade de superioridade tecnológica militar e pesquisas científicas. Ao longo do tempo, o projeto passou por reformulações, evoluindo até se transformar na Internet que conhecemos hoje.

No ano de 1990, a Internet, já com essa denominação, rompeu seus laços militares, adquirindo dimensões comerciais. A significância da Internet foi ampliada com o desenvolvimento da *World Wide Web* (www) no mesmo ano, um hipertexto que permitiu o compartilhamento de informações por meio da computação interativa. Tim Berners-Lee, seu criador, introduziu o conceito de *URL*, possibilitando o acesso e a contribuição de informações de qualquer computador conectado à Internet. (PAESANI, 2013).

A cultura hacker norte-americana e o desenvolvimento do *Internet Explorer* pela Microsoft em 1995 ampliaram ainda mais as capacidades da Internet. Sua intrínseca flexibilidade permitiu aos usuários remodelar aplicações, tornando-a versátil e complexa, abrangendo todas as atividades humanas.

A acelerada interconexão global, impulsionada pela facilidade de comunicação e pela abrangência da internet, tem resultado em um crescimento exponencial da globalização. Esse fenômeno permite que informações e eventos atinjam pessoas em todo o mundo simultaneamente, transformando não apenas as relações sociais, mas também os padrões econômicos.

A expansão acelerada das tecnologias da informação também trouxe à tona dilemas éticos, como a coleta massiva de dados por empresas de tecnologia, a inteligência artificial e a vigilância digital. O escopo global desses desafios destaca a importância de uma abordagem internacionalmente coordenada para o pensamento jurídico.

Contudo, as vantagens da globalização coexistem com desafios significativos. Oscilações econômicas e crises financeiras podem afetar indivíduos em qualquer parte do mundo, independentemente de sua localização geográfica. A vulnerabilidade a esses riscos é um aspecto intrínseco à natureza complexa e interdependente da economia globalizada.

A globalização se correlaciona com os avanços tecnológicos, haja vista que a sociedade contemporânea tem cada vez mais se tornado digitalizada, pois segundo o estudo "*Digital 2023: Global Overview Report*", publicado pelo site Datareportal, onde podemos averiguar que em outubro de 2023 já contamos com cerca de 65.7% da população mundial são usuários da internet, como consequência direta desta situação podemos ver que as atividades online tem se tornando cada vez mais predominantes nas mais diversas áreas, em razão disso houveram diversas mudanças na forma que nos interagimos, negociamos, estudamos e nos comportamos, em geral, dentro da sociedade.

É diante da globalização potencializada pela internet que surge a necessidade da globalização do pensamento jurídico, extrapolando os limites territoriais de cada país, numa tentativa de se ter o mesmo alcance da internet e é assim que surge o direito digital.

Certamente, a globalização oferece uma ampla gama de benefícios, abrangendo desde a diversidade de produtos até a promoção da interação cultural. No entanto, esse cenário também evidencia a urgência de adotar abordagens cuidadosas e estratégias regulatórias para atenuar os impactos negativos associados.

Nesse contexto, torna-se imperativo desenvolver regimentos específicos que considerem as complexidades da era digital. Essas medidas regulatórias são essenciais para mitigar riscos e, ao mesmo tempo, proteger os direitos individuais no ambiente online. A rápida evolução tecnológica e a interconexão global exigem respostas regulatórias ágeis e eficazes, garantindo que a experiência digital seja segura, ética e respeitosa dos direitos fundamentais de cada indivíduo.

Assim, visando a harmonia social, é crucial que os indivíduos e as instituições por eles criadas tenham acesso a direitos e cumpram deveres previamente estabelecidos. Desse modo, a implementação e o subsequente cumprimento de normas legalmente estabelecidas surgem como meios socialmente legitimados para assegurar que cidadãos e órgãos institucionais permaneçam em equilíbrio na estrutura normativa da sociedade, incidindo então diretamente na Teoria Tridimensional do Direito de Miguel Reale.

Isso se dá, pois sob o viés de Reale, tem-se que a norma somente tem uma eficácia real quando se encontra em conformidade com valores de uma sociedade, assim as normas são as regras jurídicas que estabelecem proteção a direitos que diante os fatos sociais, pelos quais uma comunidade está vivenciando, adquirem valor. (SOUZA, 2010)

Essa necessidade de compreensão e adaptação da norma jurídica se demonstra pelos enormes casos de vazamento de dados na última década que evidenciaram lacunas na proteção de dados e contribuíram para a urgência de estabelecer regimentos mais rigorosos.

O formalismo jurídico tradicional demonstra-se cada vez mais insuficiente diante da dinamicidade da globalização. A Teoria Tridimensional de Miguel Reale, que combina norma, fato e valor, emerge como uma nova perspectiva jurídica necessária para a contemporaneidade. Não basta olhar o Direito apenas como norma, fato ou valor isolado; é a combinação desses elementos que reflete as complexidades da sociedade digital.

1.2 Debate da Proteção de Dados no Direito Europeu

Na era da crescente digitalização global e diante dos iminentes riscos à privacidade e dignidade humanas, surge a necessidade premente de atualizar a Diretiva de Proteção de Dados 95/46/EC, culminando na promulgação da RGPD (Regulamento Geral de Proteção de Dados). Este conjunto normativo, com força de lei, visando regular práticas adequadas no uso de

informações no ambiente eletrônico, protegendo os direitos individuais e públicos nas redes de internet.

No entanto, é crucial destacar que por mais que a RGPD, na União Europeia, representa um marco significativo na história da proteção de dados, fundamentada em uma trajetória histórica que reflete a preocupação europeia com a privacidade e a necessidade de regulamentação, a raiz desse debate remonta às décadas de 1970 e 1980, quando começaram a surgir as primeiras legislações relacionadas à proteção de dados em alguns países europeus.

O sistema normativo da União Europeia (UE) é complexo, composto por fontes primárias e derivadas. As fontes primárias referem-se a atos jurídicos que criam disposições novas por acordo entre os Estados-membros, enquanto as fontes derivadas incluem regulamentos, diretivas, decisões, recomendações e ditames.

Regulamentos constituem medidas de abrangência ampla e mandatória para todos os Estados, ao passo que as diretivas obrigam ao objetivo pretendido, deixando aos Estados a liberdade de definir os métodos para sua realização. As decisões são mandatórias para aqueles a quem se destinam, incluindo indivíduos. Recomendações são essencialmente sugestões para uma ação específica, sendo diretamente aplicáveis aos Estados-membros. Por outro lado, ditames, avisos, comunicações e resoluções são formas de expressar avaliações ou orientações institucionais.

O processo envolve a proposta da Comissão, submetida ao Parlamento ou ao Comitê Econômico e Social, antes de ser decidida pelo Conselho, o órgão executivo da UE. Essa estrutura legal proporciona um arcabouço para o direito à proteção de dados pessoais na UE.

A Alemanha foi pioneira nesse cenário, estabelecendo, na década de 1970, uma legislação estadual em Hesse para lidar com questões de proteção de dados. Esse movimento refletia não apenas a preocupação com a privacidade dos cidadãos, mas também uma compreensão precoce da necessidade de regulamentar o tratamento de informações pessoais em um cenário de rápida evolução tecnológica.

A elaboração da Lei de Hesse, crucial para o estabelecimento das bases legais de proteção de dados na Alemanha, está intrinsecamente ligada à figura de Spiros Simitis. Em uma entrevista à Revista da Universidade de *Frankfurt*, *Forschung Frankfurt*, concedida em 2015, Simitis forneceu informações detalhados sobre os eventos que levaram à promulgação dessa legislação pioneira.(MENKE, 2021)

Simitis relata que no final dos anos 1960, a Alemanha Ocidental estava passando por um processo de modernização na área da saúde, construindo vários hospitais públicos. O Estado de Hesse, de maneira especialmente diligente, seguiu essa iniciativa. Considerando que esses

hospitais manejavam uma grande quantidade de dados, principalmente relacionados a pacientes, a automação do processamento de informações tornou-se uma necessidade oportuna. Assim, com o argumento de que com a coleta desses dados oportunizaria a melhora na eficiência do diagnóstico e tratamento dos pacientes foi formado um banco de dados centralizados. Esses hospitais tornaram-se os pioneiros e o epicentro do debate público sobre a proteção de dados na região. (MENKE, 2021)

O contexto histórico mencionado remonta há uma era onde a preocupação com a segurança de dados pessoais e a privacidade começou a tomar forma concreta, especialmente na região de Hesse, na Alemanha. Naquela época, a população estava cada vez mais consciente e preocupada com os riscos associados ao uso indevido de dados e informações, principalmente diante da expansão do uso de tecnologias e sistemas cibernéticos.

A publicação de Spiros Simitis, "Oportunidades de utilização de sistemas cibernéticos para o direito", emergiu como um trabalho pioneiro, destacando as implicações e necessidades em torno da proteção de dados. Sua visão e expertise levaram o chefe de Governo de Hesse a convocá-lo para desenvolver uma proposta de legislação que tratasse especificamente da proteção de dados pessoais. Esse movimento foi em resposta direta ao crescente desconforto e insegurança do público em relação à coleta, armazenamento e utilização de suas informações pessoais.(MENKE, 2021)

O resultado desse esforço foi um anteprojeto que pavimentou o caminho para a primeira lei de proteção de dados do mundo, promulgada em 1970 em Hesse. Essa legislação pioneira não apenas estabeleceu um precedente para leis de proteção de dados em outras regiões e países, mas também marcou o início de uma era de conscientização sobre a importância da privacidade e da segurança dos dados pessoais.(MENKE, 2021)

Em 1977, a Alemanha deu um passo adiante ao promulgar a Lei Federal Alemã de Proteção de Dados. Essa legislação nacional consolidou e expandiu as medidas já adotadas ao nível estadual, estabelecendo diretrizes mais abrangentes para a coleta, processamento e armazenamento de dados pessoais. A Lei Federal Alemã de Proteção de Dados tornou-se um marco jurídico essencial, influenciando não apenas as práticas dentro do país, mas também servindo como referência para futuras regulamentações ao nível internacional.

O ano de 1983 marcou outro momento crucial com a decisão do Tribunal Constitucional Federal (*Bundesverfassungsgericht*) no âmbito do censo. Nessa decisão, o tribunal reconheceu e reforçou o direito fundamental à autodeterminação informativa. Esse reconhecimento fundamentou-se na ideia de que os cidadãos têm o direito de controlar suas

informações pessoais, especialmente em um contexto de coleta massiva de dados, como era o caso do censo.

Essa decisão do Tribunal Constitucional Federal representou um avanço significativo na proteção dos direitos individuais no ambiente digital, estabelecendo um precedente importante para futuras discussões sobre privacidade e autodeterminação informativa. Assim, a Alemanha, ao longo da década de 1970 e início da década de 1980, não apenas estabeleceu bases legais sólidas para a proteção de dados, mas também contribuiu para a construção de um arcabouço jurídico internacional que reconhece a importância fundamental da privacidade na era da informação.

No mesmo período, outros países europeus, como França, Noruega, Suécia e Áustria, seguiram o exemplo, promulgando leis para regular o uso e a exportação de dados pessoais. Esse movimento refletia a conscientização crescente sobre a importância de estabelecer diretrizes para proteger a privacidade em um ambiente cada vez mais informatizado.

Já na década de 1980 a Europa tomou outro passo crucial para o desenvolvimento da proteção de dados como temos hoje com a criação da Convenção 108+ pelos países membros do Conselho da Europa em 1981. Essa convenção desempenhou um papel fundamental na unificação e melhoria das normas para o tratamento automatizado de dados pessoais. Ao estabelecer um regulamento abrangente, a Convenção 108+ proporcionou um sistema de governança para questões de proteção de dados pessoais, consolidando a base para futuras regulamentações internacionais.

O Parlamento Europeu e o Conselho da UE criaram um regulamento em outubro de 1995 que todos os membros da UE deveriam seguir, visando a harmonização do grau de proteção existente nas leis nacionais e para garantir o livre fluxo de informações pessoais entre os países-membros.

No texto, fica claro que a noção de proteção de dados, bem como a interpretação de seus propósitos, é muito mais complexa e muito mais próxima das leis atuais. A lei já inclui conceitos como o uso de dados para fins específicos, o direito do consumidor de acessá-los e a responsabilidade das empresas de proteger os dados armazenados.

A Diretiva 95/46/CE tem como objetivo equilibrar a proteção da vida privada e a livre circulação de dados pessoais. Estabelece limites rigorosos para a coleta e uso desses dados, garantindo o direito de buscar reparação por danos decorrentes de tratamento ilícito. Além disso, permite recorrer aos tribunais em caso de violação dos direitos garantidos pela diretiva. Essa legislação foi uma precursora importante para a proteção de dados na União Europeia.

A Diretiva 2002/58/CE do Parlamento e do Conselho Europeu é igualmente importante no que diz respeito à proteção da privacidade no setor de comunicações eletrônicas quando se trata do tratamento de dados pessoais. Essa legislação limita a livre circulação de informações, especialmente com os avanços da Internet e da tecnologia. Inclui um conjunto de medidas legislativas conhecidas como "pacote das telecomunicações", com o objetivo de fornecer uma estrutura jurídica consistente e coesa para o assunto em questão.

Com a crescente digitalização e globalização no século XXI, começamos a examinar os grandes vazamentos de dados e as consequências que podem ter para nossa sociedade. O incidente da *Cambridge Analytica* foi um dos maiores vazamentos de dados de todos os tempos.

O escândalo da *Cambridge Analytica* implicou a coleta não autorizada de dados de milhões de usuários do Facebook para fins políticos. A Cambridge Analytica, uma empresa de análise de dados, usou informações coletadas do Facebook para manipular votantes nas eleições presidenciais dos Estados Unidos em 2016 e no Brexit. A *Cambridge Analytica* coletou informações pessoais dos usuários do Facebook, incluindo dados políticos, que foram então usados com táticas de "*microtargeting*" consumidores de forma individual e específica para eleitores, fazendo uso de mensagens e publicações específicas para direcionar anúncios políticos e influenciar a opinião dos eleitores. (HUGHES, 2019)

Este caso foi amplamente divulgado na mídia e foi visto como um exemplo da importância de proteger a privacidade dos dados pessoais e de regulamentar o uso de dados pessoais para fins políticos. É importante destacar que o escândalo da *Cambridge Analytica* é uma das principais fontes de referência para a discussão sobre a importância de proteger a privacidade dos dados pessoais e regulamentar o uso de dados pessoais para fins políticos.

Além de todo o escândalo e implicações reais que esse acontecimento implica em como vemos a proteção e regulação da privacidade dos dados pessoais. A combinação de dados pessoais, tecnologia e estratégia política transformou os dados em algoritmos valiosos que influenciaram a política dos Estados Unidos e a política internacional.

Esta notícia teve um impacto significativo no Facebook e aumentou a preocupação com a segurança de dados. De acordo com Confessore do *The New York Times*, a rede social atravessou uma de suas maiores dificuldades. O CEO, Mark Zuckerberg, precisou se pronunciar imediatamente depois que um grande número de usuários começou a excluir suas contas. Mas, como Zuckerberg é hoje um dos maiores detentores de dados da sociedade digital, excluir o perfil individual não teria grande impacto. Conforme observado por Hughes (2019), Zuckerberg tem uma influência significativa no mundo virtual, pois é proprietário de vários aplicativos,

como Instagram, Facebook e WhatsApp, e tem a capacidade de controlar os algoritmos dessas redes para exibir apenas conteúdo que é de seu interesse.

Este caso mostra como a democracia está correndo um grande risco devido ao uso de dados pessoais para fins políticos e comportamentais. Assim, diante os perigos do uso não regulamentado de forma rígida e os potenciais riscos à privacidade e dignidade humana, surge a imperatividade de atualizar a Diretiva de Proteção de Dados 95/46/EC, resultando na promulgação da RGPD (Regulamento Geral de Proteção de Dados).

Isto posto, em 27 de abril de 2016, é aprovado o novo Regulamento (EU) 2016/679, o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*), conhecido como GDPR, que revogou a Diretiva 95/46/CE, mas manteve seus princípios.

1.3 Trajetória Brasileira: Caminhos para a Proteção de Dados Pessoais

Diante da eclosão da Terceira Onda da evolução humana, que marcou a transição para um mundo altamente globalizado e digitalizado, as discussões em torno do direito à privacidade, intimidade e regulamentações de proteção de dados tornaram-se urgentes. A situação foi agravada pelos eventos, como o incidente da Cambridge Analytica, que destacaram a necessidade de uma abordagem ética diante do uso massivo de dados pessoais. Nesse contexto, surge a Lei Geral de Proteção de Dados (LGPD) no âmbito nacional, inserida no que podemos denominar como a Sociedade da Informação.

A Sociedade da Informação, conforme definida por Soete e reproduzida por Marsden, caracteriza-se pela valorização de informações com custos reduzidos, armazenamento de dados e transmissão de tecnologia. Essa era coloca a informação e os dados no centro da coexistência e organização social, transformando significativamente o estilo de vida das pessoas (MARSDEN, 2000).

No entanto, a Sociedade da Informação também traz dilemas éticos, especialmente relacionados à coleta sistemática de dados dos cidadãos. Sob justificativas diversas, como a eficácia da publicidade, saúde e conservação dos princípios democráticos, os dados são analisados sistematicamente, gerando bancos de dados com o potencial de direcionar e moldar o pensamento individual. Isso levanta preocupações éticas, exemplificadas pelo caso da Cambridge Analytica, onde a manipulação de dados impactou a percepção e o comportamento das pessoas.

Os direitos à privacidade e à proteção dos dados, fundamentais em um Estado de Direito Democrático, demandam não apenas regulamentações, mas também a participação ativa da sociedade. A evidência do "capitalismo de vigilância" globalizado e neoliberal, cada vez

mais presente, com seus interesses mercadológicos e pessoais, reforça a necessidade de formular leis e políticas que considerem os dados pessoais como um bem comum de interesse público, indo além de uma abordagem exclusivamente governamental. (ZUBOFF, 2020)

O referido conceito “capitalismo de vigilância” pelas palavras de Shoshana Zuboff é a mercantilização de maneira unilateral da experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. (ZUBOFF, 2020)

A busca por um equilíbrio entre a proteção da privacidade individual e a promoção do acesso transparente e ético às informações torna-se crucial. Os deveres do poder público desempenham um papel central na criação de regulamentações que garantam a integridade dos dados pessoais, promovendo uma sociedade informada e protegida. Essa é uma jornada complexa em um mundo onde a informação é central para a transformação social e, ao mesmo tempo, apresenta desafios éticos significativos.

A necessidade de regulamentação da coleta e proteção de dados no Brasil não é algo recente, sendo estabelecida antes mesmo da Lei Geral de Proteção de Dados (LGPD). O conceito de proteção de dados no ordenamento jurídico brasileiro remonta a 1988, quando a Constituição estabeleceu, em seu artigo 5º, LXXII, a garantia constitucional do habeas data. Essa ação visa assegurar o acesso e conhecimento de informações armazenadas em bancos de dados, bem como a retificação, se necessário. Posteriormente, esse procedimento foi regulamentado pela Lei n° 9.507/97. (BRASIL, 1988)

Infraconstitucionalmente, diversas leis ordinárias disciplinam aspectos específicos relacionados à privacidade e proteção de dados. Destacam-se, entre elas, a Lei n.º 9.296/96 e a Lei n.º 10.217/01, que tratam da interceptação telefônica, gravação ambiental e fluxo de dados correlatos. Além disso, a Lei 10.703/03 regula o cadastro de usuários de telefones pré-pagos. A Lei Complementar 105/01 aborda a quebra do sigilo bancário em casos de grave delito, enquanto a Lei n.º 9.613/98 trata da lavagem de dinheiro. Essas normativas estabelecem parâmetros específicos para a coleta e uso de dados em contextos diversos.

Entretanto, ganha destaque em meio estas o Código de Defesa do Consumidor em específico Seção VI do Capítulo V desse código trata especificamente do banco de dados e do cadastro dos consumidores, destacando o artigo 43 como uma norma precursora no estabelecimento de direitos relacionados à proteção de dados. (BRASIL, 1997)

O artigo 43 vai além de simplesmente regular o uso de dados e determinar um prazo para armazenamento de informações negativas do consumidor para obtenção de crédito; ele também reconhece o direito do consumidor de controlar suas informações pessoais. Essa disposição legal não apenas estabelece limites temporais para o armazenamento de dados, mas

também enfatiza o aspecto do controle do consumidor sobre suas informações pessoais. (BRASIL, 1997)

Além disso, na mesma Seção do Código de Defesa do Consumidor, há uma clara exigência de que o consumidor seja notificado sobre a abertura de um banco de dados não solicitado em seu nome. Essa notificação representa um importante aspecto da transparência e do respeito aos direitos do consumidor em relação aos seus dados pessoais. (BRASIL, 1997)

Outra fonte normativa brasileira que versa sobre a proteção de dados é a Lei 12.414 de 2011, que também versa acerca da proteção de dados, aprofundando-se nas questões relativas a operações financeiras e de adimplemento para que se forme um histórico de crédito com a finalidade de fundamentar decisões das de concessão de crédito, assim facilitando a concessões de créditos àqueles consumidores que pagam suas dívidas pontualmente.

Ainda no ano de 2012 o Brasil teve outro avanço no que tange à proteção de dados, a Lei n.º 12.527, conhecida como Lei de Acesso à informação, esta regulamenta o direito constitucional de acesso às informações públicas, esta norma nos apresenta a conceitos como transparência ativa e passiva, assim como fortalece o conceito de informação nos processos legislativos nacionais, sendo conceitualizados pela Lei de Acesso à Informação como dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, registrados em qualquer suporte ou formato.

Com a Internet sendo amplamente disseminada na sociedade contemporânea, a sociedade passa a enfrentar os problemas advindos dessa, potencializados por uma falta de arcabouço jurídico que estabeleça os direitos dos usuários da Internet e deveres dos prestadores, assim diante as emergentes violações e riscos inerentes à Sociedade da Informação começam a produzir decisões contraditórias e injustas. E conforme leciona Damásio de Jesus:

> No Brasil, preferiu-se o caminho contrário. Adotando-se primeiramente a legislação criminal (que deveria ser a *ultima ratio*), de modo a punir condutas praticadas por intermédio ou contra sistemas informáticos. Os direitos dos usuários vieram depois com a Lei n. 12.965/2014, denominada "Marco Civil da Internet". Uma sociedade que não está preparada para entender o que pode caracterizar ou não um crime informático, mas que a despeito já o tipifica, inconsequentemente. (JESUS, 2016, p. 17)

Assim, apesar da presença marcante da Internet, a ausência de uma definição jurídica específica para o mundo cibernético resultou em decisões judiciais contraditórias, não só no âmbito penal, mas também no que diz respeito à difícil delimitação da responsabilidade civil em casos que envolvem a proteção de direitos individuais, muitas vezes colocando em conflito a privacidade e a liberdade de expressão.

A coleta deliberada de dados sigilosos, abrangendo tanto informações sensíveis quanto o histórico de navegação em sites da internet. Essa prática, frequentemente realizada por empresas e organizações, levanta questões cruciais sobre a privacidade e a segurança dos usuários. Além disso, a solicitação constante de dados por autoridades públicas sem a devida submissão à prévia análise judicial amplifica as preocupações relacionadas à proteção dos direitos individuais. (LEMOS, 2014).

Apesar da omissão normativa acerca do tema, o governo brasileiro já se mostrava preocupado com a necessidade de observar a evolução e riscos apresentados pela Internet já em 1995, demonstrando pela criação do Comitê Gestor da Internet no Brasil (CGI.br).

> O Comitê Gestor da Internet no Brasil – CGI.br tem sua história construída desde 1995, quando a Internet e a web no Brasil ainda eram dimensionadas em não muitos milhares de domínios e o número de conselheiros no comitê contava-se nos dedos da mão. Desde então só temos expandido para além do que se imaginava na ocasião. Não é muito tempo se considerarmos os nem 20 anos da história do comitê. Mas são milhões de domínios depois. Somos também muitos outros conselheiros. Muitos já exerceram seus mandatos em gestões passadas. E muitas são as cadeiras ocupadas pelos atuais 21 conselheiros, representantes de diferentes setores. (Relatório de Políticas da Internet, 2012)

Assim, diante da necessidade de ampliação de seu alcance e atuação, o CGI.br em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas no Rio de Janeiro (CTS/FGV) cria o Observatório Brasileiro de Políticas Digitais ou, como ficou conhecido, o Observatório da Internet Brasileira, produzindo relatórios anuais que relatavam os avanços ou projetos de leis que tramitavam no Brasil naquele ano.

Diante do cenário nacional surge a discussão do Marco Civil da Internet, processo esse que foi um grande exemplo da participação popular nos processos legislativos brasileiros, tendo sido apresentado como projeto de Lei 2.126/2011, entrou sete vezes na pauta de votação da Câmara dos Deputados, sem conseguir o devido interesse dos parlamentares na sua aprovação.

Parado na Câmara dos deputados desde 2012, uma vez que não atendia as demandas dos grupos comerciais, o Projeto de Lei já tinha recebido 34 emendas parlamentares até 2013, e somente voltou a ser pauta do plenário da Câmara dos Deputados quando o governo brasileiro passou a ser alvo de espionagem americana.

A revelação do caso Snowden, conduzida pelo jornal britânico *The Guardian* e liderada pelo jornalista Glenn Greenwald, marcou um ponto crucial na discussão sobre a vigilância em massa. O caso expôs os programas de espionagem da *National Security Agency*, a Agência Nacional de Segurança dos Estados Unidos (NSA), que envolviam a coleta de dados de ligações telefônicas, além de informações de fotos, e-mails e videoconferências de usuários

ligados a serviços de internet fornecidos por empresas americanas como *Google, Facebook* e *Microsoft/Skype*. Edward Snowden, o colaborador das matérias, desempenhou um papel fundamental ao fornecer informações que revelaram a existência do sistema de vigilância secreto chamado *XKeyscore*. Esse sistema permitia aos órgãos de inteligência dos EUA supervisionar atividades cotidianas comuns à maioria dos usuários de internet em todo o mundo, sendo o governo brasileiro um desses alvos. (GREENWALD, 2013).

A Lei 12.965/14, conhecida como Marco Civil da Internet, foi votada e entrou em vigor em 23 de junho de 2014, tendo demorado 5 anos para ser votada, mas diante o contexto da realidade que os brasileiros estavam vivendo, esta finalmente foi promulgada, recebendo importância substancial.

O Marco Civil da Internet representou um significativo avanço no panorama normativo brasileiro, particularmente por recepcionar a compreensão jurídica da internet. Mais do que estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, estabeleceu que a disciplina do uso da internet no Brasil tem como fundamentos o respeito à liberdade de expressão; o reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; a finalidade social da rede (BRASIL, 2014).

Damásio Jesus destaca a importância dessa legislação ao considerá-la a "Constituição da Internet" no contexto brasileiro. Originado de um projeto colaborativo em 2009, esse marco legal estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Jesus, em sua obra "Manual de Crimes Informáticos" de 2016, sublinha que o Marco Civil busca evitar a insegurança jurídica, especialmente diante de decisões contraditórias relacionadas à tecnologia da informação.

Além disso, Damásio Jesus menciona a perspectiva de um Marco Civil Internacional, que poderia ser proposto na Assembleia das Nações Unidas. Essa proposta destaca a complementaridade dessa legislação em atividades relacionadas à repressão de crimes cibernéticos, oferecendo uma visão que pode ser integrada às leis abordadas em seus estudos. Portanto, o Marco Civil da Internet se consolida como um instrumento essencial na regulação do ambiente digital no Brasil, buscando equilibrar os direitos e deveres dos usuários e provedores de conexão no cenário online.

A análise da busca por regulamentação das relações jurídicas na Internet revela uma tendência no Brasil de adotar leis específicas para lidar com os desafios do ambiente digital. No entanto, é crucial adotar uma abordagem equilibrada, evitando interferências nas

características fundamentais da Internet, especialmente no que diz respeito à liberdade, e evitando estabelecer metas que possam se mostrar inatingíveis.

Patrícia Peck (2002) destaca a importância de evitar a criação excessiva de legislação específica, argumentando que tal abordagem pode não atender aos objetivos da sociedade da informação, que lida com a relativização dos conceitos de espaço e tempo. Em muitos casos, o excesso de normas específicas pode dificultar a adaptação constante do Direito a todas as situações sociojurídicas do ciberespaço. Em contrapartida, o uso da equidade e da analogia pode proporcionar uma maior efetividade na reparação de danos ocorridos na rede.

No entanto, Peck ressalta a necessidade de evitar uma abordagem radical, reconhecendo que, em determinadas situações, a criação de legislação específica é necessária. Um exemplo claro disso é a informatização do Poder Judiciário no Brasil, que se mostrou extremamente eficaz devido à implementação de uma legislação regulamentando a justiça informatizada. No entanto, a autora destaca que a criação de leis penais genéricas pode resultar em injustiças, uma vez que o tipo penal deve ser o mais específico possível para garantir a aplicação equitativa da lei em toda a sociedade.

Assim, a discussão sobre a regulamentação no ambiente digital requer uma abordagem cuidadosa, considerando a natureza dinâmica e complexa da Internet, bem como a necessidade de equilibrar a proteção dos direitos individuais com a liberdade inerente a esse espaço virtual.

Com efeito, em 2018, influenciado pelas diretrizes europeias, especialmente pelo Regulamento Geral de Proteção de Dados (GDPR), o Brasil sancionou e publicou a Lei Federal 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD). Essa legislação, que entrou em vigor em 2020, representa o ponto de convergência para os diversos conceitos e princípios discutidos anteriormente.

O marco regulatório da proteção de dados pessoais no Brasil representa um avanço significativo nas relações entre usuários e os setores público e/ou privado. Essa legislação se consubstancia em princípios fundamentais, destacando-se a preservação da liberdade, o livre desenvolvimento da personalidade e a proteção da privacidade.

Esses alicerces formam a base para uma abordagem mais ética e responsável no tratamento das informações pessoais dos cidadãos, promovendo um ambiente digital mais seguro e alinhado com as demandas contemporâneas de respeito aos direitos individuais.

CAPÍTULO 2 – O DIREITO A PRIVACIDADE E A LGPD

Em um mundo cada vez mais interconectado e digitalizado, a proteção de dados pessoais emerge como um imperativo jurídico e social. A Lei Geral de Proteção de Dados (LGPD) do Brasil representa um marco legal significativo, trazendo à tona discussões fundamentais sobre privacidade, segurança e direitos digitais. Este capítulo visa fornecer uma compreensão da LGPD, contextualizando-a no cenário jurídico brasileiro e internacional, e analisando não apenas os aspectos legais e regulatórios, mas também o impacto prático e as implicações éticas da lei.

O advento da LGPD é uma resposta direta às transformações tecnológicas e sociais que caracterizam a era moderna. A lei emerge como um esforço para equilibrar os avanços tecnológicos com a necessidade de proteger informações pessoais e garantir a privacidade dos cidadãos. Discutimos aqui os fundamentos da proteção de dados pessoais, a evolução do direito digital e como a LGPD se alinha com os princípios constitucionais e internacionais.

Porém há de se ressaltar que a LGPD não opera isoladamente; ela se integra ao arcabouço jurídico brasileiro, ressoando com os direitos fundamentais e a dignidade da pessoa humana. Examinamos como a lei interage com princípios éticos, morais e legais existentes, e destacamos as responsabilidades e obrigações que ela impõe.

A lei estabelece uma série de direitos e deveres que visam assegurar a proteção de dados pessoais, assim como conceitos que servem como pilares da própria norma, em destaque o papel do consentimento, a importância da transparência e a necessidade de prestar contas no tratamento de dados pessoais. A LGPD destaca a responsabilidade dos agentes de tratamento e reforça o direito à privacidade e a não discriminação dos titulares dos dados.

2.1 Fundamentos e Estrutura da LGPD: Um Novo Paradigma

Ante a globalização e os avanços dos meios comunicacionais, como a internet e, por conseguinte, estuda-se a legislação específica sobre a proteção de dados pessoais no Ordenamento Jurídico Brasileiro, a Lei 13.709 de 14 de agosto de 2018.

Ao longo da história, a necessidade humana de armazenar informações sempre foi evidente. Em suas primeiras manifestações, recorreu-se a estruturas físicas como papiro, papel e meios similares. Contudo, com o progresso científico e tecnológico, surgiu a viabilidade de criar suportes lógicos, notadamente os *softwares*, incluindo uma forma notável: os Bancos de Dados online.

Essa inovação, conjugada com a utilização de "hardwares", especialmente o emprego de computadores, abriu caminho para a implementação de programas específicos de Banco de Dados em organizações, tanto públicas quanto privadas. A finalidade primordial é reunir informações relacionadas a um mesmo assunto, como dados comerciais. Essa transformação não apenas aprimora a organização e acessibilidade das informações, mas também desempenha um papel fundamental na redução da necessidade de espaços físicos de armazenamento.

Na abordagem dos aspectos materiais, é essencial compreender certos conceitos que permeiam toda a análise e o texto normativo. Nesse contexto, a compreensão de termos como dados, informação e conhecimento é fundamental. Conforme Goldschmidt, Passos e Bezerra, em "*Data mining*: conceitos, técnicas, algoritmos, orientações e aplicações", os dados, na base da pirâmide, são interpretados como itens elementares captados e armazenados pela Tecnologia da Informação. São cadeias de símbolos sem semântica própria, destinados a expressar fatos do mundo real para tratamento no contexto computacional. As informações, por sua vez, são dados processados, dotados de significados e contextos bem definidos. No ápice da pirâmide está o conceito de conhecimento, representando padrões ou conjuntos de padrões que podem envolver e relacionar dados e informações. (GOLDSCHMIDT *et al.* 2015)

A Lei Geral de Proteção de Dados (LGPD) estruturada em 10 capítulos e 65 artigos, estabelecendo em seu Capítulo I as disposições gerais e apresenta, no artigo 2º, os princípios fundamentais que embasam a proteção de dados pessoais. No artigo 3º, são delineadas as diretrizes sobre a territorialidade de aplicação da lei. O artigo 4º trata da inaplicabilidade da lei em determinadas situações, enquanto o artigo 5º apresenta os conceitos gerais que fundamentam a legislação.

Considerando a estrutura, objetivos e conceitos abordados na Lei Geral de Proteção de Dados (LGPD), é possível aprofundar nossa compreensão. No primeiro capítulo, que trata das disposições gerais, o legislador demonstra preocupação com o desenvolvimento econômico e tecnológico, alinhado à defesa dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade. Assim, conforme dispõe o art. 1º:

> 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. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (BRASIL, 2018)

Em seguida, temos a inteligência do artigo 2º em conexão com o artigo anterior, pois disciplina sobre os fundamentos da proteção de dados pessoais:

> Art. 2º. A disciplina da proteção de dados pessoais tem como fundamentos: I - A respeito à privacidade; 30 II - A autodeterminação informativa; III - A liberdade de expressão, de informação, de comunicação e de opinião; IV - A inviolabilidade da intimidade, da honra e da imagem; V - O desenvolvimento econômico e tecnológico e a inovação; VI - A livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018)

Os fundamentos da liberdade de expressão, informação, comunicação, opinião, assim como a inviolabilidade da intimidade, honra e imagem, já são previstos pela Constituição Federal. A LGPD reforça a importância desses fundamentos, repetindo-os em incisos separados, indicando que estão no mesmo grau de relevância que abrange a privacidade.

Como bem expõe Lara Rocha Garcia, et al., sobre os fundamentos:

> Os fundamentos da disciplina de proteção de dados são descritos no artigo 2º e têm grande importância na estrutura da lei. É nesse artigo que se defende o éthos da lei, ou seja, o que não se pode perder de vista ao interpretar a lei. Dessa forma, qualquer interpretação que porventura venha a ferir tais fundamentos se torna inadequada. (GARCIA; et al., 2020, p. 16-17).

A análise desse artigo torna-se crucial, uma vez que, ao proteger o indivíduo, a LGPD reconhece sua inserção em uma sociedade em constante desenvolvimento econômico e tecnológico. Essa perspectiva reconhece a existência de limites, tanto individuais quanto coletivos, demandando interpretações abrangentes e a necessidade de compreender ambos os lados da equação. (GARCIA; et al., 2020)

Em continuidade, o artigo 3º da Lei Geral de Proteção de Dados (LGPD) trata da territorialidade de aplicação da lei. Neste artigo, a legislação brasileira estabelece as condições sob as quais a LGPD será aplicada, delimitando sua abrangência no que diz respeito ao território nacional.

> Art. 3º. Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III - os dados pessoais objeto do tratamento tenha sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta8 . § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei. (BRASIL, 2018)

O texto do artigo 3º destaca que a LGPD se aplica ao tratamento de dados pessoais realizado no território brasileiro, independentemente dos meios utilizados para o tratamento, bem como ao tratamento de dados pessoais de titulares que se encontrem no Brasil, ou ainda quando o tratamento tenha o propósito de oferecer bens ou serviços, ou o tratamento de dados de indivíduos localizados no Brasil. Essa abordagem alinha-se com a natureza globalizada das transações online e das relações comerciais modernas, reconhecendo que as fronteiras nacionais não são barreiras absolutas para o tratamento de dados. A LGPD, portanto, busca proteger os cidadãos brasileiros independentemente de onde ocorra o processamento de seus dados pessoais. (BRASIL, 2018)

No seu artigo 4º, a LGPD explicita as situações em que o tratamento de dados pessoais não se aplica. Em resumo, a lei não se destina exclusivamente a atividades jornalísticas e artísticas, tampouco a fins relacionados à segurança pública, defesa nacional, segurança do Estado, investigação e repressão de infrações penais de natureza particular. Em outras palavras, a lei se aplica apenas a pessoas físicas ou jurídicas que gerenciem dados com finalidades econômicas. Além disso, a LGPD não abrange dados localizados fora do Brasil, que não sejam objeto de transferência internacional.

O artigo 5º da Lei Geral de Proteção de Dados (LGPD) desempenha um papel fundamental ao estabelecer as definições essenciais que orientam a aplicação e compreensão dos princípios e diretrizes da LGPD no contexto da proteção de dados no Brasil. Entre as definições fundamentais, destaca-se o conceito de "dado pessoal", que se entende como dados pessoais toda informação que está atrelada a uma pessoa natural, identificável ou identificada, de direito público ou privado, inclusive pessoas de outras nacionalidades, há de se pontuar a existência de tratamento especial aos dados pessoais provenientes de crianças e adolescentes, haja vista a condição jurídica destas no ordenamento brasileiro. Esse é um ponto que precisa ser destacado devido à quantidade de empresas que lidam com dados de consumidores e organizações parceiras devido ao número quantitativamente alto de consumo de serviços e bens materiais que nem sempre são adquiridos em territórios brasileiros.

Além disso, a LGPD introduz o conceito de "dado pessoal sensível", abrangendo informações mais delicadas sobre a vida do indivíduo, as quais serão tratadas posteriormente. O artigo 5º também traz o conceito de "dado anonimizado", referindo-se a dados que não podem ser identificados, mesmo utilizando meios técnicos razoáveis.

Ademais, esse artigo apresenta os papéis fundamentais no contexto da Lei Geral de Proteção de Dados (LGPD). Cada um desempenha uma função específica para garantir a proteção dos dados pessoais e o cumprimento da legislação

No cerne da estrutura da LGPD encontra-se o Titular, que representa a pessoa natural a quem os dados se referem. Essa figura é o ponto focal das preocupações e regulamentações estabelecidas pela legislação. A LGPD tem como um de seus objetivos centrais conferir mais controle ao titular sobre o uso de seus dados, alinhando-se aos fundamentos de respeito à privacidade e à autodeterminação. Nesse contexto, a legislação confere uma série de direitos ao titular, destacando-se especialmente no 18º artigo. Esses direitos são fundamentados nos princípios constitucionais e internacionais dos direitos fundamentais de liberdade, intimidade e privacidade, conforme estabelecido pela Declaração Universal dos Direitos do Homem. Essa abordagem reflete a preocupação em garantir que o titular exerça um papel ativo e decisivo no tratamento de suas informações pessoais.

No contexto do artigo 5º da Lei Geral de Proteção de Dados (LGPD), destaca-se um direito crucial que merece atenção especial: o direito da autodeterminação. Esse direito, fundamentado na Constituição, ganha concretude com as disposições da LGPD, conferindo ao titular dos dados o poder de requisitar informações específicas ao controlador. O titular pode demandar o acesso, a correção, a anonimização, a eliminação ou a portabilidade dos seus dados, entre outros pontos relevantes. Além disso, possui o direito de revogar a qualquer momento o consentimento para o uso de seus dados, introduzindo-nos a outro ponto de grande importância na Lei n.º 13.709/2018: o consentimento.

O consentimento, como delineado no artigo 5º, inciso XII, da LGPD, é definido como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Esse princípio reflete a ênfase da legislação na garantia de que o tratamento dos dados ocorra de maneira transparente, com o consentimento do titular sendo obtido de forma clara e consciente. Essa abordagem reforça a importância da autonomia e da decisão informada do titular sobre como seus dados serão utilizados. (Brasil, 2018)

O Controlador, um dos agentes de tratamento previstos pela Lei Geral de Proteção de Dados (LGPD), desempenha um papel crucial no processo de tratamento de dados. Essa entidade, que pode ser uma pessoa física ou jurídica, de natureza pública ou privada, é responsável por tomar as decisões fundamentais sobre como os dados serão tratados. Essas decisões abrangem desde a coleta até o descarte das informações, sendo essenciais para orientar o curso do processamento.

Juntamente com o Operador, o Controlador forma a categoria dos agentes de tratamento, papéis centrais dentro do contexto da LGPD nos termos do seu artigo 5º, inciso º, IX. O Operador, por sua vez, atua efetivamente na execução do tratamento dos dados em nome

do controlador. Se uma empresa está coletando dados em nome de outra, ela está desempenhando o papel de operador. É crucial que as atividades do operador estejam alinhadas às diretrizes estabelecidas pelo controlador, garantindo o cumprimento das normas de proteção de dados.

Para fortalecer a proteção e comunicação, a figura do Encarregado de Dados é outro dos papéis fundamentais estabelecidos. Designado pelo controlador e operador, o Encarregado atua como o ponto de ligação entre as partes envolvidas: o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Essa designação visa estabelecer uma abordagem transparente e acessível à proteção de dados.

O Encarregado de Dados, também conhecido como *Data Protection Officer* (DPO), desempenha várias funções cruciais. Ele é responsável por aceitar as solicitações dos titulares dos dados, responder às demandas da ANPD, orientar os servidores e garantir o comprimento das diretrizes da LGPD. É importante ressaltar que o cargo de DPO não precisa ser ocupado por uma única pessoa, permitindo certa flexibilidade nas organizações.

A presença do Encarregado de Dados é uma das mudanças mais significativas introduzidas pela LGPD. Sua atuação contribui para a implementação eficaz das normas de proteção de dados, assegurando que as organizações estejam em conformidade e que os direitos dos titulares sejam respeitados de maneira efetiva.

Autoridade Nacional de Proteção de Dados (ANPD) é outro papel fundamental instituído na LGPD, essa assume um papel central na implementação e fiscalização da Lei Geral de Proteção de Dados (LGPD) em âmbito nacional. Como órgão regulador, sua responsabilidade fundamental é assegurar que todas as entidades sujeitas à legislação estejam em conformidade, promovendo a proteção dos direitos dos titulares de dados.

A atuação da ANPD envolve não apenas a supervisão, mas também a fiscalização rigorosa do cumprimento das normas estabelecidas pela LGPD. Em casos de tratamento de dados em desacordo com a legislação, a ANPD possui o poder de aplicar sanções, buscando garantir a aderência estrita às diretrizes de proteção de dados.

Além disso, a ANPD desempenha um papel consultivo e propositivo na definição da Política Nacional de Proteção de Dados Pessoais e da Privacidade. Sua participação na elaboração dessas políticas contribui para direcionar as estratégias nacionais no que diz respeito à proteção de dados, considerando os aspectos cruciais como privacidade, segurança e ética no tratamento das informações pessoais.

Dessa maneira, a ANPD emerge como um elemento-chave na construção de um ambiente digital no Brasil que equilibre a inovação tecnológica com a salvaguarda dos direitos

individuais, garantindo que a proteção de dados seja uma prioridade em todas as esferas da sociedade. Acerca do tema, Patricia Peck afirma:

> A ANPD tem um papel fundamental como elo entre diversas partes interessadas que vão do titular ao ente privado e ao ente público, passando pela necessidade de alinhamento com demais autoridades reguladoras e fiscalizadoras, bem como os três poderes Executivo, Legislativo e Judiciário que deverão continuar a compreender a temática da dinâmica dos dados pessoais em um contexto não apenas nacional, mas principalmente internacional para que o Brasil saiba se posicionar no mercado digital global (Pinheiro, 2023, p. 21).

Encerrando o Capítulo I, temos o art. 6º, da Lei Geral de proteção de dados, mas antes de adentrarmos ao conhecimento dos princípios norteadores dessa lei, vale frisar as lições de Miguel Reale ao definir princípios como verdades ou juízos fundamentais. Com esse raciocino em mente passamos a analisar os princípios da LGPD. A princípio o art. 6º, da Lei Geral de proteção de dados, estabelece com ênfase principal que o tratamento de dados deve respeitar o princípio da Boa-fé. A boa-fé encontra-se em diversos momentos do nosso Código Civil/2002 bem como, de forma subjetiva, apresenta-se em toda a LGPD.

O princípio da finalidade é encontrado no artigo 6º, inciso I da LGPD e quer dizer que é a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.". Assim, abstrai-se que é devedor do provedor informar acerca dos dados coletados e em casos de mudança na forma, conteúdo ou método de tratamento de dados, o titular dos dados deve ser informado previamente.

Ao realizar a leitura do artigo 6º, inciso II da LGPD, esse abrange o princípio da adequação, que aponta que deverá haver "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Assim, deve-se estabelecer uma relação lógica entre o tratamento, a finalidade do tratamento e a comunicação dessas ações ao titular dos dados.

Ao que tange o princípio da necessidade, o mesmo é encontrado no artigo 6º, inciso III da LGPD e estabelece que deverá ter a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". A norma geral estabelecida pela LGPD preconiza a não realização do tratamento de dados, sendo a exceção a realização desse tratamento, desde que a consecução de uma finalidade específica seja considerada relevante. Nesse contexto, apenas os dados pertinentes, ou seja, aqueles que se revelem indispensáveis para alcançar o objetivo previamente estabelecido, devem ser tratados.

O princípio do livre acesso se apresenta no artigo 6º, inciso IV da LGPD, onde se refere a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais". Consequentemente, é dever do responsável pelo tratamento de dados pessoais disponibilizar, mediante solicitação, informações sobre quais dados foram coletados, como são processados, a finalidade do tratamento, a periodicidade, entre outras informações relevantes.

Denotado artigo 6º, inciso V da LGPD, o princípio da qualidade dos dados aponta ser a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento". Esse princípio preconiza a garantia de que as informações do titular dos dados sejam sempre atualizadas e fidedignas. Portanto, os responsáveis pelo tratamento devem adotar medidas para assegurar a precisão e a atualização das informações, respeitando a finalidade para a qual os dados foram coletados e processados.

O princípio da transparência é retratado no artigo 6º, inciso VI da LGPD e visa "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Tal princípio visa garantir que o titular dos dados tenha acesso claro e compreensível a informações sobre o tratamento de seus dados pessoais. Essa transparência engloba aspectos como a finalidade da coleta, a duração do armazenamento dos dados e a eventual compartilhamento com terceiros. Ao adotar práticas transparentes, os controladores de dados promovem a confiança dos titulares e possibilitam que estes compreendam como suas informações serão utilizadas, contribuindo para uma relação mais ética e equitativa no tratamento de dados pessoais.

Porém, o legislador, ao formular a LGPD, reconheceu a importância da proteção de segredos comerciais e industriais. Isso é especialmente evidente quando se considera o princípio da transparência, que não deve comprometer informações confidenciais que possam ser classificadas como segredos comerciais. Assim, embora a lei busque promover a transparência nas práticas de tratamento de dados pessoais, ela também estabelece limites para proteger informações sensíveis que são essenciais para a competitividade e inovação das empresas.

Disposto no artigo 6º, inciso VII da LGPD, o princípio da segurança requer a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". Aqui somos apresentados a ideia de que o protetor dos dados

coletados tem a responsabilidade objetiva em casos de acesso e manuseio indevido dos dados das pessoas naturais objeto do tratamento.

Com previsão no artigo 6º, inciso VIII da LGPD, o princípio da prevenção determina a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais". Esse princípio impõe a responsabilidade de garantir medidas eficazes para proteger os dados pessoais contra acessos não autorizados, vazamentos ou qualquer forma de tratamento inadequado, reiterando aquilo que fora estabelecido no princípio anterior.

O princípio da não discriminação, exposto no artigo 6º, inciso IX da LGPD da seguinte forma: "impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos". Em outros termos, o uso dos dados pessoais não pode trazer para os titulares, situações discriminatórias ou então facilitar abusos, para uma melhor compreensão Cintia Rosa Pereira D. Lima, nos traz um exemplo:

> Exemplo plausível de violação ao princípio da não discriminação é o de um determinado usuário que utiliza um aplicativo para controlar suas performances em exercícios físicos. Este aplicativo pode armazenar dados como batimentos cardíacos, doenças vasculares, se o indivíduo possui um hábito sedentário, etc. Não será possível que este aplicativo forneça tais dados para empresas de seguros informando o hábito e questões pessoais do usuário para que elas calculem os riscos e aumentem, por exemplo, o valor do seguro de vida desta pessoa, pois estaria violando o princípio da não discriminação do usuário. (LIMA, 2020, p. 136)

Por fim, temos o princípio da prestação de contas, no artigo 6º, com o inciso X da LGPD, exigindo que "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". Assim, sob a visão de Marcio Pestana, o requisito da demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais é essencial. Nesse contexto, destaca-se a importância da rastreabilidade, uma palavra de ordem atualmente, que demanda a comprovação de procedimentos e atos realizados. No contexto da proteção de dados pessoais, esse requisito ganha ainda mais relevância, exigindo fácil acessibilidade à evidência da eficácia dessas medidas adotadas pelo agente de tratamento. (PESTANA, 2020)

O Capítulo II da LGPD, iniciado pelo artigo 7º, estabelece as hipóteses de tratamento dos dados pessoais, apresentando um rol taxativo e estrito. O inciso I desse artigo delineia a base legal do consentimento, permitindo que o tratamento de dados pessoais ocorra mediante a manifestação nos termos do artigo 5º, inciso XII. É relevante destacar que, embora o consentimento seja uma base legal crucial, não é a única prevista pela LGPD. As bases legais

geralmente não se sobrepõem umas às outras, sendo necessário avaliar qual delas será aplicada em casos específicos, levando em consideração as circunstâncias e finalidades do tratamento de dados.

O artigo 7º, inciso II da LGPD, estabelece outra base legal para o tratamento de dados, permitindo-o "para o cumprimento de obrigação legal ou regulatória pelo controlador". Essa base legal proporciona flexibilidade ao controlador ao realizar suas atividades de negócio, autorizando o tratamento de dados quando necessário para cumprir obrigações impostas por leis ou regulamentações. Essa interpretação está alinhada com o princípio fundamental da LGPD, conforme estabelecido no artigo 2º, que visa respeitar o desenvolvimento econômico e tecnológico, a inovação, a livre iniciativa e a livre concorrência.

No artigo 7º, inciso III da LGPD permite à Administração Pública o tratamento e compartilhamento de dados pessoais, nos casos de: “para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei”. Esse dispositivo estabelece uma base legal ampla e abrangente, que permite o uso de dados necessários para a execução de políticas públicas, consoante as disposições do Capítulo IV da LGPD. Essa abordagem reflete a consideração da supremacia do interesse público e a necessidade de adotar medidas para a efetivação das políticas públicas.

No artigo 7º, inciso IV da LGPD, o legislador discorre que está autorizado o tratamento de dados “para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais”. A lei define órgão de pesquisa como uma entidade da administração pública direta ou indireta, ou pessoa jurídica de direito privado, sem fins lucrativos, legalmente constituída sob as leis brasileiras, que tenha em sua missão institucional ou objetivo social ou estatutário a realização de pesquisa básica, ou aplicada de caráter histórico, científico, tecnológico ou estatístico, conforme o artigo 5º, inciso XVIII. Essa disposição visa facilitar a condução de estudos e pesquisas, promovendo o avanço do conhecimento, desde que seja respeitada a privacidade dos indivíduos por meio da anonimização, procedimento esse descrito no artigo 12 da LGPD.

No artigo 7º, inciso V da LGPD, versa sobre o tratamento de dados “quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados”.

Abordado no artigo 7º, inciso VI da LGPD, esta base legal visa tratamento dos dados “para o exercício regular de direitos em processo judicial, administrativo ou arbitral.”. Desta forma, o texto da lei resguarda o direito do agente de tratamento ao possibilitar o tratamento de

dados em casos como forma de resguardar o exercício regular de algum direito em processos judiciais, administrativos ou arbitral.

Inclusa no artigo 7º, inciso VII da LGPD, esta base legal pondera: “para a proteção da vida ou da incolumidade física do titular, ou de terceiro”.

Apresentado no artigo 7º, inciso IX da LGPD, autoriza o tratamento de dados “quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”

Conciso no artigo 7º, inciso X da LGPD, esta base autoriza o tratamento de dados “para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente”. Essa disposição visa equilibrar a proteção dos dados pessoais com a necessidade de garantir a integridade do sistema financeiro e a segurança nas transações.

O artigo 11º da LGPD destaca as hipóteses para o tratamento de dados pessoais sensíveis. Essas hipóteses são aplicáveis apenas nos seguintes casos: consentimento específico e destacado, para finalidades específicas; e as situações que não exigem o consentimento, tais como obrigação legal ou regulatória, pesquisa, políticas públicas, exercício regular de direitos em processo, proteção à vida, tutela da saúde, garantia de prevenção à fraude e segurança do titular. Essas disposições visam assegurar que o tratamento de dados sensíveis seja feito com a devida cautela, considerando a sensibilidade dessas informações.

O Capítulo II finaliza abordando o encerramento do uso dos dados, estabelecendo que isso ocorrerá quando a finalidade do tratamento for alcançada, quando o período previsto para tal tratamento terminar ou mediante solicitação do titular, ou da Autoridade Nacional de Proteção de Dados (ANPD). Nos casos mencionados, os dados devem ser eliminados. No entanto, há exceções, como a obrigação legal de manutenção, a realização de pesquisas, a transferência a terceiros ou o uso exclusivo pelo Controlador. Essas disposições visam garantir a transparência e o controle sobre o uso e o destino dos dados pessoais.

2.2 Relação do direito a privacidade na LGPD com o Arcabouço Jurídico Brasileiro

O atual cenário tecnológico e globalizado tem permitido uma circulação rápida e abrangente das informações pessoais de indivíduos. Em questão de segundos, dados podem ser captados, compartilhados e utilizados em diferentes partes do mundo, muitas vezes sem o pleno conhecimento ou consentimento dos titulares dessas informações.

Esse fenômeno é impulsionado pelo avanço das tecnologias de comunicação, redes sociais, comércio eletrônico e outras plataformas digitais. As informações, uma vez

digitalizadas, podem ser transmitidas instantaneamente, transcendendo fronteiras geográficas e alcançando diversos destinatários.

Esse fluxo rápido de dados traz consigo desafios significativos relacionados à privacidade e segurança das informações pessoais. A exposição indevida ou o uso não autorizado desses dados podem resultar em consequências sérias para os titulares, incluindo ameaças à privacidade, fraudes e outros tipos de violações.

É no contexto da era do capitalismo de vigilância que nos encontramos, onde os dados pessoais pertencentes às pessoas físicas ou jurídicas deixaram de ser usados apenas para fins triviais, de identificação, sendo a representatividade do âmbito privado de uma pessoa para passarem a ser uma coisa alienável, sujeito ao mercado, assim a captação, exploração e conversão dos dados pessoais passou a ser uma das atividades econômicas mais lucrativas na atualidade. (ZUBOFF, 2020)

Nessa perspectiva, nota-se um processo de objetificação em relação aos dados pessoais, embora não se configure como uma patrimonialidade. A regulação visa disciplinar não apenas a ligação do dado pessoal ao sujeito de direito, mas também a circulação da informação em si. Assim, ao buscar uma tutela dinâmica para acompanhar os dados em circulação, revela-se que a informação pessoal, ao mesmo tempo, assume um caráter objetivo do sujeito de direito, tornando-se um atributo de sua personalidade.

Rony Vainzof acrescenta ao tema ao pontuar que os dados pessoais: “deixaram de ser insumo básico para a criação e o desenvolvimento de qualquer negócio, para servirem como commodities ao possuírem grande valor comercial e estratégico de acordo com a quantidade, qualidade e capacidade de tratamento.” (VAINZOF, 2020, p. 40)

Com efeito, a sociedade contemporânea vive em uma era de rápida digitalização e interconexão, onde a facilidade com que os indivíduos compartilham seus dados pessoais apresenta desafios significativos para a preservação da individualidade e a segurança dos grupos aos quais pertencem. A coleta, agrupamento e tratamento dessas informações podem ter impactos profundos tanto no nível individual quanto coletivo.

Ao entregar seus dados, muitas vezes de maneira inadvertida ou sem plena compreensão das consequências, os indivíduos podem estar expondo elementos essenciais de sua identidade. Essas informações podem abranger desde dados básicos, como nome e endereço, até detalhes mais sensíveis, como preferências pessoais, histórico de compras, localizações frequentes e interações online.

Quando esses dados são agregados e processados, seja por empresas, governos ou outras entidades, eles podem ser usados para criar perfis detalhados e prever comportamentos

futuros. Essa prática levanta preocupações sobre a privacidade e a autonomia dos indivíduos, pois suas ações e preferências podem ser objeto de análises detalhadas.

Além disso, a agregação de dados em larga escala pode ter implicações para grupos inteiros. Por exemplo, algoritmos que analisam padrões comportamentais podem inadvertidamente perpetuar preconceitos e discriminações, afetando comunidades inteiras com base em características compartilhadas.

Nesse contexto, a regulamentação e as normas éticas desempenham papéis cruciais para equilibrar a inovação tecnológica com a proteção dos direitos individuais, buscando assegurar que, mesmo em um mundo altamente conectado, a privacidade e a segurança dos dados sejam preservadas.

A interseção entre ética, moral e direito na era digital destaca-se como um ponto crucial, especialmente ao considerarmos as diretrizes para a ação ética na Internet. Em sua essência, as normas éticas permeiam tanto o campo da moral quanto o do Direito, refletindo a interconexão dessas esferas.

A aplicação da teoria tridimensional das leis éticas, que compreende os elementos fato, valor e norma, torna-se pertinente nesse contexto. Os fatos representam a realidade objetiva, enquanto os valores inserem a dimensão subjetiva e axiológica, e as normas delineiam as regras que regem o comportamento humano. (REALE, 2002)

Assim, ao estabelecer diretrizes éticas para a Internet, é imperativo reconhecer a complexidade dessa tríade: fatos que refletem a realidade digital, valores que orientam as escolhas éticas e normas que regulam o comportamento online. Essa exposição sistemática visa criar um arcabouço que não apenas promova a ética individual, mas também contribua para o desenvolvimento de padrões éticos coletivos que sustentem uma sociedade digital justa e equitativa. A tridimensionalidade das leis éticas, para Reale, pode ser resumida da seguinte forma:

> A lei ética ou, de maneira especial, a lei jurídica é a compreensão de um fato enquanto cultural, que se realiza em virtude de uma tomada de posição volitiva, de que resultam juízos de valor, que implicam responsabilidade e sanção". Em outras palavras, a experiência ética apresenta uma tensão necessária, sempre renovada, entre circunstâncias de fato e o plano estimativo, o que se reflete em suas normas. Os fatos, que podem ser físicos, econômicos, estéticos ou jurídicos, cercam o homem no meio social e histórico e lhe impõem o limite de ação. Por sua vez, o valor é atingido ou negado conforme a ação do agente. Então, a norma representa a tensão entre fato e valor, pois esses dois elementos não se resolvem entre si, da mesma forma que a norma depende de pressupostos fáticos e axiológicos. (REALE, 2002, apud GARCIA, 2010, p. 392-393).

Nesse mesmo sentido versa Patricia Peck, nos dizeres:

> Compete ao Sistema Legislativo fazer o filtro de todas as valorações e expectativas de comportamento da sociedade, mediante processos decisórios, para que elas possam adquirir validade jurídica. A capacidade da norma de refletir a realidade social determina o grau de eficácia jurídica de um ordenamento. Eficaz é aquilo que é capaz de efetivamente produzir efeitos, ou seja, o conceito de eficácia envolve aceitação e obediência. (PECK, 2021, p. 36)

É nesse contexto que leis como a Lei Geral de Proteção de Dados (LGPD) se tornam cruciais. Elas buscam estabelecer diretrizes claras para o tratamento de dados pessoais, garantindo que os titulares tenham mais controle sobre suas informações e que as entidades que as processam estejam sujeitas a padrões éticos e legais. Ademais, a valoração das normas em razão dos fatores sociais analisados para sua promulgação a tornam mais eficaz, haja vista a preocupação crescente que as relações no âmbito digital respeitem os direitos humanos e os direitos a privacidade.

No dinâmico contexto atual, onde os valores éticos e morais desempenham um papel crucial na elaboração e interpretação das normas jurídicas, a LGPD estabelece ressalvas ao direito à privacidade, à personalidade e aos direitos humanos em seus fundamentos.

Ao abordar o direito à privacidade, destaca-se que, mesmo diante de comportamentos pouco responsáveis por parte dos titulares desse direito no âmbito virtual, este ainda desfruta de garantia constitucional, sendo considerado um direito fundamental (art. 5º, X, da CF/88) e integrando o rol dos direitos da personalidade, conforme disposto no art. 21 do Código Civil (BRASIL, 2002).

Ferraz Júnior apresenta que a vida privada é composta de:

> (...) um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos - como nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc., condicionam o intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido. (FERRAZ JÚNIOR, 2005, p. 28 apud VAINZOF, 2020, p. 26)

Marcel Leonardi, ao compilar diversas doutrinas sobre a proteção de dados e intimidade, define a intimidade como o:

> (...) direito de o indivíduo ser deixado em paz parar viver sua própria vida com um grau mínimo de interferência"; "o direito de subtrair-se à publicidade para recolher-se na própria reserva"; "o direito à intimidade é o direito de o indivíduo não ser arrastado para a ribalta contra a sua vontade, de subtrair-se à publicidade e de permanecer recolhido na sua intimidade, o direito de manter olhos e ouvidos indiscretos afastados dessa esfera de reserva, bem como o

> direito de impedir a divulgação de palavras, escritos e atos realizados nessa esfera de intimidade"; e "espaço íntimo intransponível por intromissões ilícitas externas." (LEONARDI, 2012, p. 51-56 apud VAINZOF, 2020, p. 34-35).

Vainzof esclarece que os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil brasileiro, são expressões da cláusula geral de tutela da pessoa humana, de forma dinâmica, para minimizar o risco de deixar de atingir situações até então inexistentes, oriunda da evolução tecnológica, sempre com o foco no livre desenvolvimento da pessoa. Ele destaca que personalidade é "características ou conjunto de características que distingue uma pessoa da outra. Assim, os direitos da personalidade, como nome, imagem e honra, conforme Carlos Alberto Bittar, são aqueles reconhecidos à pessoa humana tomada em si e em suas projeções na sociedade". (VAINZOF, 2020)

A definição destacando a natureza do espaço íntimo como intransponível por intromissões ilícitas externas ressalta que, ao controlar os dados que formam os atributos da personalidade, ocorre o domínio sobre a pessoa. Isso implica na retirada da possibilidade do livre desenvolvimento da sua personalidade, violando o inciso VII do art. 2º da LGPD.

Atualmente, a proteção de dados conta com respaldo constitucional, representando uma novidade no ordenamento jurídico brasileiro. A Proposta de Emenda à Constituição (PEC) 17/2019 eleva a proteção de dados pessoais, inclusive nos meios digitais, à categoria de direito fundamental. Essa PEC atribui exclusivamente à União a competência para legislar sobre o tema. Por meio de acordo entre as lideranças, os dois turnos foram votados na mesma sessão. (SENADO FEDERAL, 2021)

No contexto da dignidade da pessoa humana, a Constituição Federal de 1988 estabelece como um de seus fundamentos o princípio da dignidade (art. 1º, inc. III). A Lei Geral de Proteção de Dados (LGPD), por sua vez, também incorpora a dignidade como um de seus sustentáculos, art. 2º, VII. Assim, a dignidade permeia todo o ordenamento jurídico, exigindo que tanto o Estado quanto os particulares considerem o indivíduo como o centro do sistema legal.

Quanto aos Direitos Humanos, é possível observar a abrangência de proteção proporcionada pelas legislações internacionais, especialmente no que diz respeito à privacidade de dados em ambientes online. A Declaração Universal dos Direitos Humanos, da Organização das Nações Unidas, garante, no art. 12º, que: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques, toda pessoa tem direito à proteção da lei." (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948.)

Apesar das transformações na privacidade devido às inovações tecnológicas, a LGPD mantém a preocupação com o desenvolvimento saudável da personalidade humana, destacando-a como fundamento (art. 2º, VII). Dessa forma, qualquer ação, seja no mercado ou no âmbito individual, deve respeitar o princípio de que a pessoa é o foco central. O desenvolvimento econômico deve estar a serviço do indivíduo, reforçando a importância do princípio da dignidade da pessoa humana.

Isso também se aplica ao direito ao desenvolvimento econômico que, embora fundamentado no artigo 2º da LGPD, deve operar dentro dos limites e em conformidade com os direitos da dignidade humana. Os itens V e VI do artigo 2º da LGPD estabelecem bases para o desenvolvimento econômico e tecnológico, inovação, livre iniciativa, livre concorrência e defesa do consumidor. Esses elementos refletem a necessidade de equilibrar o desenvolvimento econômico com a proteção dos direitos individuais e a defesa do consumidor, havendo assim uma preocupação com o indivíduo, com seu desenvolvimento, com questões ligadas aos direitos fundamentais e direitos da personalidade, o que demonstra respeito ao estado democrático.

Porém, e quando estamos debatendo acerca do direito ao desenvolvimento econômico que encontramos um dos principais embates da LGPD, quem deve prevalecer entre o direito ao desenvolvimento econômico e o direito a personalidade e privacidade? Segundo Vainzof (2020, p. 41), há fundamento jurídico para a abertura do mercado de dados pessoais a todos que busquem empreender, conforme preconizado pelo art. 170 da Constituição Federal, que estabelece a ordem econômica com base na valorização do trabalho humano e na livre iniciativa, visando assegurar a todos uma existência digna, em consonância com os princípios da justiça social, incluindo a livre concorrência e a defesa do consumidor. Por outro lado, estabelece o art. 170 da CF/88 que:

> A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: I - soberania nacional; II - propriedade privada; III - função social da propriedade; IV - livre concorrência; V - defesa do consumidor; VI - defesa do meio ambiente, inclusive mediante tratamento diferenciado conforme o impacto ambiental dos produtos e serviços e de seus processos de elaboração e prestação; VII - redução das desigualdades regionais e sociais; VIII - busca do pleno emprego; IX - tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no País. Parágrafo único. É assegurado a todos o livre exercício de qualquer atividade econômica, independentemente de autorização de órgãos públicos, salvo nos casos previstos em lei. (BRASIL, 1988).

Sem dúvida que o acesso a dados pessoais até um determinado limite é necessário. O desenvolvimento econômico atual tem condições de criar a partir de tais bens, estratégias que gerarão mais consumo, empregos, renda, enfim. Porém, a interpretação extensiva do art. 170 da CF/88 efetuada por Vainzof é perigosa, uma vez que extrapola os perímetros do próprio texto constitucional, que em momento algum alude que "o mercado de tratamento de dados pessoais (...) deve estar aberto a todos que busquem empreender." (VAINZOF, 2020). O dispositivo legal, como pode ser observado, menciona quais os fundamentos da ordem econômica, seus princípios e o que assegura. Livre-iniciativa ou concorrência não implica autorização para a manipulação indiscriminada de dados pessoais de uma população. Não é sem razão que a LGPD foi recentemente criada.

Certamente, o acesso a dados pessoais é crucial para o desenvolvimento econômico, permitindo a criação de estratégias que impulsionam o consumo, geração de empregos e renda. A interpretação extensiva do artigo 170 da Constituição Federal, conforme destacada por Vainzof, pode ser perigosa, pois extrapolaria os limites do texto constitucional, a menção aos fundamentos da ordem econômica, princípios e garantias não implica uma autorização indiscriminada para manipulação de dados pessoais. Assim, ressalta-se a importância de se estabelecer limites claros para garantir que essa manipulação de dados ocorra de maneira ética e respeitosa aos direitos individuais.

Ainda mais, percebe-se que o artigo 170 deve ser interpretado considerando outros princípios fundamentais, como aqueles consagrados no artigo 5º. Este último estabelece a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. Essa interconexão entre os artigos reforça a necessidade de um equilíbrio entre o desenvolvimento econômico, a livre iniciativa e a proteção dos direitos fundamentais, como a privacidade e a dignidade da pessoa humana. (BRASIL, 1988)

A conformidade com a LGPD e outras regulamentações relevantes, é um passo essencial, mas não o único. Devemos considerar como as normas jurídicas interagem com os fatos reais e os valores éticos da sociedade para criar um sistema de saúde mais seguro e confiável. A teoria tridimensional nos encoraja a ver a legislação não como uma série de prescrições isoladas, mas como parte de um tecido maior de práticas sociais e expectativas éticas

CAPÍTULO 3 – DELINEANDO DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS: UMA VISÃO SOB A LGPD

Na era digital, onde cada clique e cada interação deixam rastros digitais, a proteção de dados pessoais e sensíveis assume um papel central na salvaguarda da privacidade e da dignidade humana. O Capítulo 3 desta monografia se dedica a explorar a complexa trama que envolve a definição, o tratamento e a proteção de dados pessoais, com foco particular nos dados sensíveis relacionados à saúde no contexto brasileiro, especialmente iluminado pela vigência e aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD).

Este capítulo se inicia com uma exploração conceitual dos dados pessoais, estabelecendo a base para entender as particularidades dos dados sensíveis, que pela sua natureza íntima ou potencial discriminatória, demandam um olhar ainda mais cauteloso e regulamentações específicas. Neste contexto, os desafios e implicações desses dados no setor de saúde são analisados, especialmente em períodos críticos como o da pandemia de COVID-19, onde a necessidade de processamento rápido e massivo de informações de saúde coloca em evidência as vulnerabilidades e os riscos associados a essas práticas.

A investigação adentra na complexidade das regulamentações, com ênfase na LGPD, e discute como a lei brasileira aborda a proteção de dados sensíveis, estabelecendo diretrizes para seu tratamento seguro e ético. Serão discutidos casos e incidentes de vazamento de dados, revelando as camadas de complexidade técnica, organizacional e regulatória que compõem o cenário atual de proteção de dados no Brasil.

Este capítulo não apenas desenha o cenário atual e os desafios enfrentados pela proteção de dados pessoais sensíveis no Brasil, mas também promove uma reflexão crítica sobre como a lei e as práticas de governança de dados estão evoluindo para atender às exigências de um mundo cada vez mais digital e interconectado. É uma viagem que busca compreender a intersecção entre a tecnologia, a lei e os direitos fundamentais, com o objetivo de propor caminhos para uma sociedade mais segura e justa.

3.1 Um Olhar Expandido sobre Dados Pessoais e Sensíveis

O propósito da LGPD, conforme o artigo 1º, é proteger os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural, visando, portanto, resguardar dados e informações que possibilitem a identificação da pessoa natural. (BRASIL, 2018)

Schaefer destaca que a identificação de dados como pessoais ou não depende significativamente dos métodos razoavelmente empregados para associá-los a uma pessoa. A relação entre o dado e a pessoa fica mais tênue à medida que aumenta o esforço necessário para estabelecer essa conexão. Dados são considerados não anônimos e, portanto, pessoais quando existem métodos razoáveis para associá-los a um indivíduo, refletindo uma abordagem expansionista na definição de dados pessoais que contempla tanto indivíduos já identificados quanto aqueles potencialmente identificáveis. (SCHAEFER, 2010)

Neste contexto, um dado é classificado como pessoal quando há uma ligação direta com um indivíduo, e essa associação não excede um esforço considerado razoável. Isso significa que se a identificação de um indivíduo requer esforços excessivos ou impraticáveis, o dado não entra na categoria de pessoal. Bioni reforça essa visão ao estabelecer a razoabilidade como critério determinante para definir quais dados associados a indivíduos identificáveis são tratados como dados pessoais. Portanto, a análise da identificabilidade de um dado passa necessariamente pela avaliação do esforço razoável necessário para vinculá-lo a uma pessoa específica, mantendo um equilíbrio entre proteção de dados e pragmatismo operacional. (BIONI, 2019)

Em complemento as lições de Goldschmidt, Passos e Bezerra, conforme já estabelecemos anteriormente, a Lei Geral de Proteção de Dados (LGPD) estabelece conceitos fundamentais essenciais para compreendermos a proteção de dados no contexto brasileiro em seu artigo 5º. No âmbito dessa legislação, a definição de dados pessoais é central. A categoria de dados dentro da LGPD pode ser dividida em três opções: os dados pessoais, os dados pessoais sensíveis e os dados anonimizados. (GOLDSCHMIDT *et al.* 2015)

Delineando os contornos dos dados pessoais conforme o artigo 5º da LGPD, consideram-se dados pessoais as informações relacionadas a uma pessoa natural identificada ou identificável. Esse conceito abrange uma ampla gama de informações, desde aquelas mais básicas, como nome e endereço, até dados mais complexos que, quando combinados, podem levar à identificação de uma pessoa, dai que temos a necessidade de diferenciação do que são os dados e o que é informação. Consoante lição de Danilo Doneda:

> Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular a ser levado em conta (...). O dado estaria associado a uma espécie de "pre-informação" anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição e mesmo nos efeitos que esta pode apresentar ao seu receptor. (DONEDA, 2020, p. 152)

Diante esse critério expansionista que podemos entender que a finalidade da Lei Geral de Proteção de Dados, pois entendemos o que se tem por proteção e tratamento de dados. De forma imperiosa e indispensável, a proteção de dados decorre da necessidade de proteção ao livre desenvolvimento da personalidade assim como os direitos fundamentais, é nesse sentido que Doneda assevera: “A proteção de dados pessoais, em suma, propõe o tema da privacidade, porém, modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão” (DONEDA, 2020, p. 165).

A proteção de dados pessoais, derivada da cláusula geral de tutela da pessoa humana e do direito à privacidade, configura-se como um requisito essencial para a preservação da democracia. A tutela jurídica de dados pessoais, como decorrência do direito à privacidade ou à identidade, enfatiza a importância da autodeterminação informativa, concedendo controle ao titular sobre seus dados, expressamente elencada no artigo 2º, inciso II da LGPD (BRASIL, 2018) . Esse princípio torna-se crucial na proteção de dados sensíveis, pois essas informações podem resultar em tratamentos desiguais.

Sob o viés tridimensional da norma, podemos notar que a proteção das informações pessoais transcende a simples questão técnica e penetra profundamente no tecido da dignidade humana, um valor fundamental que nos orienta na constante evolução da sociedade digital. Neste cenário em rápida transformação, onde a tecnologia altera continuamente a paisagem dos dados (Fato), a salvaguarda da privacidade se adapta, refletindo uma compreensão mais ampla de seus objetivos e métodos. (REALE, 2002)

Portanto, é crucial reconhecer que a proteção de dados pessoais, embora fundamental para a preservação da privacidade, vai além da mera concepção de propriedade dos dados. Esta visão ampliada reflete uma compreensão mais profunda de que os dados pessoais estão intrinsecamente ligados à identidade e ao bem-estar dos indivíduos (DONEDA, 2006). Consequentemente, o propósito mais profundo e verdadeiro por trás da proteção de dados é assegurar não somente a segurança e confidencialidade das informações, mas principalmente proteger a dignidade e os direitos fundamentais das pessoas associadas a esses dados. Assim, o foco recai sobre a manutenção da integridade pessoal e da autonomia, enfatizando a necessidade de práticas éticas e responsáveis no manuseio de informações pessoais.

Essa dinâmica, impulsionada pela inovação tecnológica, não apenas expande o alcance da proteção de dados, mas reforça a necessidade de um compromisso com a dignidade individual e coletiva (Valor). A privacidade, portanto, não é mais vista apenas como um direito isolado, mas como uma questão intrinsecamente ligada ao respeito pela humanidade de cada pessoa. E é aqui que a norma (Norma) entra, não como uma entidade rígida, mas como um

princípio vivo e adaptável que busca harmonizar as capacidades tecnológicas com os direitos humanos fundamentais.

À medida que avançamos na era digital, torna-se claro que a proteção de dados pessoais é uma jornada contínua, marcada pela interação entre os avanços tecnológicos (Fato), os valores humanos (Valor) e a resposta normativa (Norma). Não se trata apenas de implementar medidas técnicas, mas de cultivar um ambiente onde a tecnologia serve à humanidade, e não o contrário.

As leis e regulamentos que regem a proteção de dados, portanto, não são estáticos; eles são responsivos e se moldam às novas realidades e expectativas. Ao reconhecer a natureza mutável tanto da tecnologia quanto dos valores sociais, essas normas procuram oferecer uma proteção que é tanto robusta quanto respeitosa, garantindo que a integridade e a privacidade sejam preservadas em um mundo cada vez mais conectado.

Com esse entendimento, a proteção de dados pessoais se revela não como uma série de medidas defensivas, mas como uma expressão de nossa dedicação coletiva à dignidade e ao respeito mútuo. Ela representa um compromisso contínuo em adaptar, inovar e proteger, guiados por uma visão tridimensional que considera a interdependência entre a evolução tecnológica, os valores humanos e a necessidade de uma governança eficaz e empática.

Assim, a proteção de dados pessoais passa a ser um conceito multifacetado, englobando uma diversidade de práticas e preocupações centradas no bem-estar do indivíduo e na integridade da sociedade na totalidade (DONEDA, 2006).

Nesse sentido a LGPD oferece uma proteção extraordinária ao mesmo, sendo uma dessas formas a anonimização, conforme prevista no artigo 12º da LGPD, que é uma medida adotada para minimizar ou proteger a privacidade do titular dos dados. Esse procedimento consiste na eliminação de identificadores que possam diferenciar indivíduos, transformando os dados em dados anonimizados. Segundo a legislação, os dados anonimizados deixam de ser considerados dados pessoais, assemelhando-se à abordagem adotada pela GDPR. Essa iniciativa visa mitigar os riscos associados à identificação pessoal, oferecendo uma camada adicional de proteção à privacidade dos titulares de dados. (BRASIL, 2018)

Diante da falibilidade da anonimização e da possibilidade de reidentificação, somos compelidos a considerar as repercussões práticas desse procedimento na proteção da privacidade do titular dos dados. Essa questão destaca a necessidade de uma abordagem mais abrangente na definição de dados pessoais, como proposto por Bruno Bioni, que sugere considerar como dado pessoal qualquer informação com potencial para identificação, mesmo que remotamente. Essa abordagem expansionista busca abarcar as diferentes formas pelas quais

os dados podem ser utilizados para identificar indivíduos, reconhecendo a complexidade e os desafios associados à proteção da privacidade em um cenário de constante evolução tecnológica. (BIONI, 2019)

Enquanto navegamos pelas disposições da LGPD podemos notar uma tratativa de diferentes tipos de dados, tanto quanto à sua coleta quanto ao seu conteúdo. Em um primeiro momento, quanto à coleta, os dados podem se referir a uma pessoa, física ou jurídica, ou a um grupo de pessoas indeterminadas. Quanto ao conteúdo dos dados, muito se discutia antes da LGPD, a respeito de uma classificação que diferenciaria os tipos de informações pessoais.

Essa diferenciação conceitual, é uma das grandes contribuições da LGPD, onde somos apresentados à determinação de dados pessoais sensíveis, em virtude de uma potencial utilização discriminatória ou particularmente lesiva não somente a um indivíduo como a uma coletividade, como, por exemplo, informações referentes à raça, orientação sexual, crenças religiosas, dados sobre saúde.

A concepção de uma categoria distinta e autônoma para dados pessoais sensíveis emergiu da compreensão crescente de que determinados dados, quando armazenados, processados ou circulados, representam riscos significativos à integridade da personalidade individual. Este reconhecimento surge especialmente em resposta às potenciais práticas discriminatórias que podem ser alimentadas ou exacerbadas por um uso indevido dessas informações. Assim, a separação desses dados em uma categoria própria visa a proteger os indivíduos e a promover um manejo mais consciente e seguro de informações sensíveis (MENDES, 2014).

Identifica-se, pois, que o tratamento desses dados sensíveis extrapola a privacidade e busca fundamentação sob o manto do princípio da igualdade, podendo ser entendido até mesmo como uma nova leitura desse mesmo principio, buscando-se uma proteção maior e evitando situações de desigualdade.

Conforme visto, uma das características que definem um dado pessoal como sensível é a possibilidade de contribuir para a ocorrência de “processos sociais de exclusão e segregação” (KORKMAZ, 2019).

O desequilíbrio de forças causado pelo uso de dados sensíveis armazenados em bancos de dados é causa suficiente para que essa categoria tenha a atenção especial apresentada na LGPD. Nas palavras de Rodotà:

> É necessário enfatizar, de fato, que os dados sensíveis são aqueles relativos à saúde e vida sexual, as opiniões e ao pertencimento étnico ou racial, com uma lista semelhante às encontradas nas normas relativas a casos de discriminações. Assim, somos confrontados com algo que vai além da simples

> proteção da vida privada e se apresenta como defensor da mesma igualdade entre as pessoas. (RODOTÀ, 2019, p. 36 *apud* KORKMAZ, 2020)

Porém esse conceito não é novo no contexto jurídico brasileiro. A Lei n.º 12.414/2011, em seu artigo 3º, parágrafo 3º, inciso II, menciona informações consideradas sensíveis. Essas informações sensíveis referem-se à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas. Em razão dos perigos apresentados pelo uso indiscriminado dos dados pessoais sensíveis à Lei n.º 12.414/2011, apresenta uma proteção extraordinária ao mesmo.

Em sentido semelhante, a legislação brasileira passou a conceituar dados sensíveis (art. 5º, II, LGPD) como sendo: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". (BRASIL, 2018)

Ademais, a legislação brasileira abre o rol de dados que podem ser considerados sensíveis, por meio do §1 º, do artigo 11 da LGPD, ao aplicar-se a tratamentos que revelem dados sensíveis, destaca-se pela vinculação à geração de dano. A interpretação do primeiro parágrafo do referido artigo, sugere que, sempre que houver tratamento de dados pessoais sensíveis fora das hipóteses previstas, haverá um dano presumido devido à violação dos direitos fundamentais, como privacidade, liberdade e identidade. Demonstrando que tal categoria diferenciada de dados pessoais está diretamente relacionada com o alto risco existente quando da sua utilização, que podem causar dano como discriminação e violação ao foro íntimo da pessoa.

Desta forma, podemos concluir que a proteção dos dados sensíveis evita possíveis danos a direitos fundamentais, determinados pela qualidade e pela natureza dessa categoria de dados pessoais (MULHOLLAND, 2018).

A discriminação na sociedade da tecnologia tem sua problemática exemplificada pelo sistema de Crédito Social Chinês, trata-se de um sistema que ranqueia e classifica os cidadãos em razão de hábitos e comportamentos, utilizando alta tecnologia e massiva coleta e tratamento de dados. Cada cidadão ganha ou perde pontos de acordo com suas ações e crenças. O sistema ainda não funciona em todo o país, mas o governo já declarou que busca disseminar o programa ao nível nacional, mas busca categorizar e taxar os comportamentos dos cidadãos como positivos ou negativos, indicando uma classificação daquela pessoa, servindo, inclusive, para determinar se aquele individuo poderá usufruir de serviços públicos como transportes públicos.

O sistema faz uso das chamadas “Listas Negras” e “Listas Vermelhas”, a competência para manutenção e elaboração das “Listas Negras” não é centralizada ao governo central, ou seja, cabe a cada órgão governamental elaborar suas próprias listas atendendo a finalidade desejada. As chamadas “Listas Negras” são mecanismos de coerção direcionados aos processos judiciais de execução em curso e são divulgadas e disponibilizadas em sítio eletrônico, mídias sociais oficiais estatais e exibidas em locais públicos, como estações de trens. (RITO; GUEIROS; 2020)

As listas são utilizadas para estabelecer um sistema de recompensas e punições, podendo cada autoridade local estabelecer seus próprios mecanismos, assim existem diversos aplicativos e aplicações que fazem uso desses dados, um exemplo dado por Fernanda Rito e Pedro Teixeira Gueiros na obra“ O *Social Credit System* na Era dos Dados” é:

> Já a plataforma *Laolai Checker*, por sua vez, fornece dados à “Lista Negra dos Infratores” mantida pela Supremo Tribunal Popular, contendo informações de indivíduos e companhias que falharam em cumprir decisões judiciais. Os usuários podem pesquisar pelo nome dos inadimplentes, visualizar detalhes do histórico jurídico e ver o status atual de cumprimento. Além disso, disponibiliza-se um mapa, em tempo real, com a localização dos devedores de “Listas Negras” mais próximos às pessoas. Ou seja, trata-se de um monitoramento em tempo real e, inclusive, da localização dos cidadãos, o que além de violar em larga escala a privacidade, possibilita confrontos sociais indesejáveis. (RITO; GUEIROS; 2020, p. 25)

Assim se torna inegável a semelhança à distopia “1984”, escrita por George Orwell, que por mais que tenha sido escrito no final da década de 1940, tem sido citada cada vez mais no âmbito da proteção de dados, haja vista que na obra o Estado controla todos os aspectos da vida das pessoas, incluindo seus dados pessoais. Na sociedade de "1984", o Partido controla a população mediante uma rede de vigilância constante, incluindo câmeras de segurança, microfones e teletelas. Os cidadãos são constantemente monitorados e suas atividades são registradas.

Esse controle sobre os dados pessoais é usado pelo Partido para manipular a população e manter o *status quo*. Por exemplo, o Partido usa as informações pessoais para identificar e reprimir qualquer dissenso.

O sistema de crédito social chinês representa uma forma de gamificação da obediência social, onde pontuações são utilizadas para exercer controle social autoritário pelo governo. Nesse contexto, as pessoas são transformadas em dados, que, uma vez coletados, processados, combinados e compartilhados de diversas maneiras, são utilizados para classificar e condicionar o exercício de direitos e interações sociais. Com as informações pessoais dos cidadãos, as

entidades governamentais rotulam e relacionam cada indivíduo a padrões de hábitos e comportamentos, contribuindo para o fenômeno de marginalização social.

É nesse contexto que entendemos que na Era Digital, ao proporcionar vastas oportunidades de inclusão, também amplifica a crueldade da exclusão. A ausência de presença virtual coloca desafios significativos para a sobrevivência no mundo real, evidenciando uma das preocupações mais marcantes da era atual. A visibilidade e acessibilidade de todos geram uma competição intensa por oportunidades de trabalho, negócios, produtos e ativos e com a marginalização social proporcionada em casos como esse a situação se torna cada vez mais precária. (PECK, 2020)

3.2 Desafios e Implicações na Proteção de Dados Pessoais Sensíveis no Setor de Saúde Brasileiro Durante a Crise Pandêmica

A era digital, com todas as suas inovações revolucionárias, prometeu transformar o campo da saúde, promovendo a eficiência e melhorando a prestação de cuidados. Entretanto, essa transição para o armazenamento digital e o processamento de dados sensíveis acarreta riscos inerentes, como evidenciado pelos recorrentes incidentes de vazamento de dados, que expõem falhas críticas no sistema de proteção da saúde pública brasileira.

Estes incidentes não são meras violações da privacidade individual; eles ressoam profundamente, afetando a confiança pública, a integridade do sistema de saúde e a segurança dos cidadãos. Este capítulo pretende desvendar a complexa teia de falhas técnicas, lacunas organizacionais e desafios regulatórios por trás desses incidentes, focando no turbulento período pandêmico e nas implicações da Lei Geral de Proteção de Dados (LGPD) na proteção de dados sensíveis na saúde.

Os dados pessoais sensíveis, conforme definidos e tratados pela Lei Geral de Proteção de Dados (LGPD) do Brasil, compreendem categorias específicas de informações que devido à sua natureza íntima ou potencialmente discriminatória, exigem proteção e cuidado adicionais no seu tratamento. A LGPD, em seu Artigo 5º, Inciso II, caracteriza dados sensíveis como aqueles relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Devido ao fato de que os dados relacionados à saúde têm uma conexão direta com a personalidade do indivíduo que os mantém, eles são classificados como dados sensíveis e podem ter consequências significativas para aqueles que os usam.

Em contraste com outros tipos de dados sensíveis como crenças religiosas ou opiniões políticas, que frequentemente refletem escolhas pessoais e são compartilhadas publicamente, dados sensíveis relacionados à saúde, genética e biometria possuem uma natureza intrinsecamente diferente. De acordo com Korkmaz, esses dados não estão ligados a escolhas conscientes e passíveis de proteção, mas estão profundamente enraizados na constituição física e biológica do indivíduo, refletindo aspectos íntimos e inerentes da sua identidade. Portanto, enquanto algumas informações sensíveis podem ser vistas como expressões externas de preferências e crenças, dados de saúde e biometria são essenciais para compreender a singularidade biológica e a privacidade pessoal, exigindo um nível elevado de proteção e consideração.(KORKMAZ, 2019)

Assim podemos concluir que os dados de saúde são categorizados como dados pessoais sensíveis que fornecem informações críticas sobre o bem-estar físico ou mental do indivíduo, abrangendo condições de saúde passadas, atuais e potenciais futuras. Esses dados são distintivos porque podem revelar detalhes íntimos sobre o estado físico e psíquico do titular, que, se divulgados indevidamente, podem expor a pessoa a situações discriminatórias ou provocar danos significativos. Portanto, o entendimento de dados de saúde abrange não apenas informações médicas diretas, mas também qualquer dado que, ao ser conhecido, possa influenciar a percepção ou tratamento da pessoa de uma maneira que afete sua dignidade e privacidade.

Esses dados incluem uma ampla gama de informações, desde identificadores pessoais até detalhes íntimos de saúde, históricos médicos e diagnósticos. O tratamento inadequado desses dados pode levar a repercussões severas, afetando a privacidade, a dignidade e a segurança do indivíduo. A regulamentação desses dados é crítica, pois o tratamento inadequado pode levar a consequências severas, incluindo discriminação e violações de direitos humanos e liberdades fundamentais.

É importante pontuar que as normas refletem e moldam os valores sociais. A proteção de dados na saúde não é apenas uma questão legal, mas um reflexo das prioridades éticas de uma sociedade que valoriza a dignidade e a privacidade do indivíduo. As políticas e regulamentações devem, portanto, ser formuladas e implementadas em diálogo com a comunidade, considerando as nuances culturais e sociais.

No ambiente de saúde, cada interação e procedimento médico gera dados sensíveis. A crescente digitalização dessas informações aumentou a eficiência e o alcance dos serviços de saúde, mas também ampliou os riscos de violações de dados (Diniz et al., 2019). A violação dessas informações pode resultar em danos irreparáveis, incluindo discriminação, estigma

social, perda financeira e até riscos à vida, quando informações cruciais são manipuladas ou expostas.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes rígidas para a proteção de dados pessoais, com disposições ainda mais estritas para dados sensíveis relacionados à saúde. Portanto, entender e implementar medidas eficazes de proteção de dados é essencial para garantir a conformidade legal e manter a confiança e a segurança dos pacientes.

Neste sentido, é importante ressaltar que o Regulamento Geral de Proteção de Dados Europeu foi o primeiro a definir dados relacionados à saúde: "deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro" (UNIÃO EUROPEIA, 2016).

É evidente que os dados pessoais na saúde desempenham um papel adicional além da proteção da privacidade, conforme demonstrado. O conceito de bem comum está profundamente arraigado no bem-estar da coletividade, que estabelece padrões para a manipulação e distribuição de dados protegidos por lei com o objetivo principal de atender às necessidades da coletividade. Para redefinir o direito à privacidade e ao acesso à informação no âmbito da saúde, são necessários regulamentos e sistemas de governança cuidadosamente ajustados para garantir que a privacidade dos indivíduos seja protegida e que o acesso à informação seja facilitado conforme os avanços tecnológicos. (VENTURA; COELI, 2018)

Assim no que tange a proteção de dados sensíveis à saúde o alcance da LGPD engloba todo o sistema público de saúde brasileiro, sendo notável os impactos da referida lei no próprio Sistema Único de Saúde (SUS), já que este coleta, classifica, armazena, acessa, utiliza, processa, avalia, arquiva e tramita diversos tipos de informações referentes à higidez e/ou adoecimento de seus usuários, à vida sexual, aos aspectos genéticos e biométricos.

Não há como falar da emergente necessidade da proteção de dados sensíveis à saúde sem comentar da pandemia de COVID-19 que marcou um período sem precedentes na história contemporânea, afetando todas as esferas da vida humana. Uma das consequências mais significativas foi a aceleração da digitalização em vários setores, especialmente na saúde pública. No Brasil, como em muitos outros países, a urgência de gerenciar a crise sanitária impulsionou a adoção de tecnologias digitais para coletar, processar e analisar dados de saúde em uma escala nunca vista antes.

No coração da crise, o sistema de saúde foi pressionado a se adaptar rapidamente. A coleta de dados se tornou uma parte essencial no combate à pandemia, desde o rastreamento de contatos de indivíduos infectados até a implementação de campanhas de vacinação. Esses

dados, muitas vezes sensíveis e pessoais, passaram a ser uma ferramenta crucial na tomada de decisão. No entanto, essa rápida transição para o digital veio com seus próprios riscos e desafios, particularmente em relação à segurança dos dados dos cidadãos.

O significativo aumento na coleta de dados sensíveis no âmbito da saúde, impulsionado pela crise pandêmica do COVID-19, realmente ressalta a necessidade premente de uma abordagem abrangente e resiliente na proteção desses dados. Com a emergência do SARS-CoV-2 e a subsequente crise sanitária global, as instituições de saúde se viram inundadas de informações, necessitando urgentemente de métodos eficientes para gerenciar o crescente volume de dados.

Em meio a esta pressão, a adoção de tecnologias avançadas de informação e comunicação se tornou uma estratégia vital para lidar com a demanda ampliada. Eis a relevância da aplicação das diretrizes trazidas pela LGPD nos procedimentos hospitalares os quais têm como combustível dados pessoais de seus respectivos pacientes. Na prática, para atender tal prerrogativa, é necessário estabelecer termos de adesão nos prontuários que apontem, por exemplo, a integração dos respectivos dados para estudos científicos e análises estatísticas. Uma vez ferido esse princípio, fere-se também o Princípio da Adequação (LGPD, Art. 6º, II) e o da Limitação ao Tratamento Mínimo (LGPD, Art. 6º, III).(ROCHA; PIVETO; 2020)

Logo, o tratamento de dados dos pacientes titulares tem como fonte basilar as concepções supracitadas, isto quer dizer que, é levado em conta os efeitos para a privacidade e proteção de dados de todos os mecanismos utilizados dentro do estabelecimento de saúde com o intuito de evitar eventuais riscos à privacidade do paciente. (ROCHA; PIVETO; 2020)

Os incidentes de vazamento de dados, aumentados durante a pandemia, não são meramente eventos isolados; eles são indicativos de um sistema de saúde em constante evolução tecnológica e regulatória. Compreender esses incidentes como fatos dentro da teoria tridimensional nos permite analisar suas causas e consequências de forma mais holística.

Considerando o exposto, a proteção especial outorgada às informações sensíveis engloba especificamente aquelas pertinentes à saúde, tal como garantido pelo artigo 6º da Lei Geral de Proteção de Dados Pessoais (LGPD). Além disso, a referida legislação estabelece medidas preventivas e restritivas contra a divulgação indevida desses dados, visando coibir a comercialização ou utilização indevida que possa fomentar práticas discriminatórias ou preconceituosas.(BRASIL, 2018)

A LGPD, no seu artigo 11º, enfatiza a necessidade de informar os titulares a respeito do processamento de seus dados pessoais sensíveis, com especial atenção aos dados de saúde. A lei reconhece, porém, situações excepcionais onde a ponderação entre direitos fundamentais

se faz necessária, permitindo, em determinadas circunstâncias, que a prerrogativa da integridade física seja relativizada em favor do direito à vida. É importante ressaltar que tais exceções aplicam-se estritamente em contextos de procedimentos executados por profissionais, serviços de saúde ou autoridades sanitárias. Nestes casos, a obtenção do consentimento dos titulares é mandatória para o compartilhamento de dados entre entidades da saúde. Mesmo em contextos excepcionais, onde o tratamento ocorre sem consentimento explícito, a lei destaca a importância da transparência e da informação adequada sobre a utilização desses dados sensíveis. (BRASIL, 2018)

Os dados abordados pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709/2018, no que concerne à saúde, são primordialmente categorizados como sensíveis, demandando um nível elevado de proteção em comparação aos dados pessoais comuns. Profissionais da saúde requerem acesso a informações detalhadas dos pacientes, como histórico médico, medicação, resultados de exames e diagnósticos precedentes, para proporcionar uma assistência adequada e eficiente. A privacidade desses dados representa o principal desafio, necessitando que seu tratamento seja realizado de forma transparente e segura, assegurando a confidencialidade e integridade das informações coletadas, e prevenindo vazamentos ou usos não autorizados e inconsistentes com o consentimento do titular.

Rodotà sensivelmente observa que os dados pessoais de saúde capturam o indivíduo em sua mais pura e vulnerável humanidade, expondo as fragilidades físicas e psíquicas inerentes a cada pessoa. Esta percepção enfatiza o elevado grau de sensibilidade desses dados, bem como sua íntima conexão com aspectos privados e pessoais. Decorrente dessa compreensão, emerge o imperativo ético e jurídico do sigilo profissional na gestão de dados pessoais de saúde, visando proteger a privacidade e a dignidade do paciente. (RODOTÀ, 2008)

O respeito pela confidencialidade dos dados de saúde não só salvaguarda as informações pessoais contra usos indevidos que possam levar a discriminações ou abusos, mas também promove uma relação de confiança entre paciente e profissional da saúde. Esta confiança é fundamental, pois encoraja o paciente a compartilhar informações cruciais para um diagnóstico preciso e tratamento efetivo, abordando sem receios suas dores, sintomas e preocupações.

O compromisso com o sigilo está codificado no Código de Ética Médica do Brasil (Resolução CFM n.º 1.931/2009), que coloca o sigilo como um dos pilares éticos da profissão médica, além de ser reforçado por disposições específicas sobre a confidencialidade. Adicionalmente, a proteção do sigilo profissional é amplamente respaldada pelo ordenamento

jurídico, incluindo a Constituição Federal em seu artigo 5º, X, (BRASIL, 1988) e sua violação constitui crime, conforme estabelecido nos artigos 153 e 154 do Código Penal. (BRASIL, 1940)

Ainda assim, o compartilhamento de dados entre médicos e instituições de saúde é essencial para a prestação de um atendimento eficiente e completo. Isso se deve ao fato de que os profissionais de saúde precisam de um histórico completo do paciente em qualquer procedimento médico para garantir que a saúde do paciente seja protegida de forma adequada, por exemplo, evitando exames repetidos. Como resultado, pode-se concluir que a cadeia hospitalar precisa e deve processar dados de saúde. No entanto, existem questões significativas em relação à segurança e privacidade dos dados dos pacientes.

Isso ocorre porque, apesar da necessidade, esse fluxo de dados não exige o consentimento do paciente titular. Em casos excepcionais, o consentimento é obtido quando o objetivo é proteger a saúde, proteger a vida ou proteger o titular ou terceiros de perigo físico.

Neste aspecto, a Lei Geral de Proteção de Dados Pessoais (LGPD) determina a adoção de mecanismos de autorização e controle de acesso, garantindo que apenas pessoal qualificado e autorizado possa acessar tais dados. É essencial que as entidades de saúde estabeleçam diretrizes claras e eficazes para prevenir e administrar eventuais incidentes de segurança, protegendo assim os pacientes e a confidencialidade de suas informações. Igualmente, é necessário adaptar os sistemas e processos existentes para assegurar a conformidade com as normativas da LGPD.

Essas medidas de proteção e gestão de dados pessoais sensíveis são essenciais e devem ser enfaticamente aplicadas no sistema público de saúde. Os órgãos governamentais têm o dever de cumprir estritamente as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD). A administração de dados de saúde pelo setor público, embora compartilhe muitos dos objetivos do setor privado em termos de qualidade e eficiência do atendimento, difere substancialmente no que tange aos propósitos de coleta, que são voltados para fins não lucrativos, tais como estatística, epidemiologia e planejamento de políticas públicas de saúde, além de contribuir significativamente para a pesquisa científica e o desenvolvimento dos serviços de saúde.

Ademais, é imperativo que o sistema de saúde pública reconheça e aborde as desigualdades e vulnerabilidades sociais, especialmente porque informações relacionadas à saúde podem expor indivíduos a riscos de preconceito e discriminação, particularmente ligados a etnia, gênero e identidade sexual. A legislação brasileira, ciente dessas questões, procura mitigar o uso discriminatório de dados de saúde. Isso é ilustrado, por exemplo, pela Súmula 443 do Tribunal Superior do Trabalho, que considera discriminatória a demissão de empregado portador do vírus HIV ou de outra doença grave que suscite estigma ou preconceito.

A privacidade dos dados é um valor inerente à dignidade humana e ao direito individual. Dentro do contexto da teoria tridimensional, reconhecemos que a proteção desses valores é fundamental para manter a confiança no sistema de saúde e para garantir o respeito aos direitos dos cidadãos. A adoção de valores éticos e morais na gestão de dados de saúde é imperativa para a integridade do atendimento médico.

Por essas razões, as políticas públicas de saúde devem integrar considerações éticas e de direitos humanos, focando na proteção de dados sensíveis. A implementação dessas políticas é crucial não apenas para a conformidade legal, mas também para sustentar a confiança do público no sistema de saúde e garantir um atendimento digno e respeitoso a todos.

A Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil estabelece princípios rigorosos sobre a coleta, uso e compartilhamento de dados pessoais, incluindo dados sensíveis relacionados à saúde. Segundo a LGPD, a coleta de dados deve atender a propósitos específicos, legítimos e claramente informados aos pacientes, que devem estar cientes de como suas informações são utilizadas e com quem são compartilhadas.

A preocupação com a exploração e violação da privacidade dos pacientes é um aspecto central da LGPD, especialmente considerando o risco de que os indivíduos possam permanecer desinformados sobre o uso de seus dados ou que estes sejam comercializados sem o consentimento explícito dos titulares. Esse cenário é particularmente preocupante em contextos onde informações sensíveis, como dados de saúde, podem ser utilizadas de forma imprópria, levando a consequências adversas para os indivíduos.

Em primeiro lugar, o artigo 5o, inciso X da Constituição Federal declara que o direito à privacidade é um direito fundamental e inalienável de qualquer pessoa, protegendo elementos como a privacidade, a vida privada, a honra e a imagem de uma pessoa. Além disso, este dispositivo constitucional garante a possibilidade de reparação por danos morais ou materiais causados por qualquer violação desses direitos. Além disso, o inciso XII do mesmo artigo enfatiza a proteção do sigilo de dados, enfatizando a proteção dos dados privados dos cidadãos.

Além das salvaguardas estabelecidas pela Constituição, a Lei Geral de Proteção de Dados (LGPD) oferece proteção adicional para dados sensíveis, especialmente no âmbito da saúde. De acordo com a legislação, a manipulação desses dados pode ocorrer de maneira específica e regulamentada, principalmente em duas situações. Primeiramente, o artigo 11, inciso II, alínea "c" da LGPD, permite a utilização de dados sensíveis para a realização de estudos por órgãos de pesquisa, garantindo a anonimização dos dados sempre que possível, com o objetivo de obter informações vitais para o avanço e a segurança da saúde pública. Em segundo lugar, a alínea "f" do mesmo artigo permite a manipulação de dados sensíveis quando

essencial para a tutela da saúde, diretamente nos procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias.

Uma norma aplicável aos dois casos de tratamento de dados relativos à saúde encontra-se disciplinado no art. 11, § 4º da LGPD, que estabelece uma proibição explícita do uso compartilhado de dados pessoais sensíveis com o objetivo de obter vantagens econômicas.

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular; ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo (BRASIL, 2018)

A partir do dispositivo mencionado, percebe-se claramente que a norma estabelece a proibição do intercâmbio e da utilização conjunta de dados pessoais sensíveis relacionados à saúde por controladores com a finalidade de alcançar benefícios econômicos. Porém visando evitar confusões da interpretação da norma temos:

> Como pode haver confusão quando é feita a leitura dos parágrafos 3º e 4º do artigo 11 da LGPD, é importante destacar que o parágrafo 3º disciplina a possibilidade de comunicação ou uso compartilhado de dados pessoais sensíveis entre controladores com a finalidade de obtenção de lucro, asseverando que poderá haver vedação ou regulamentação pela Autoridade Nacional de Proteção de Dados (ANPD), ouvidos órgãos setoriais do poder público. Isso significa que a regra prevista no parágrafo em questão é a permissão da comunicação e do compartilhamento para fins de lucro, havendo a necessidade, porém, de consentimento do titular30. Em outras palavras, a norma prevista no parágrafo 3º permite a comunicação e o compartilhamento com a finalidade de lucro de qualquer dado pessoal sensível, desde que haja o consentimento do titular e que o dado sensível não seja relativo à saúde, na medida em que para este há vedação específica no parágrafo 4º do artigo 11 da LGPD. (BOTELHO, 2021)

A implementação da LGPD no setor de saúde requer um equilíbrio cuidadoso entre a proteção da privacidade e a necessidade de compartilhar informações para o atendimento médico e administração dos serviços. As instituições de saúde, portanto, devem adotar políticas e procedimentos rigorosos para garantir que o manuseio dos dados esteja em conformidade com a legislação que os direitos dos pacientes sejam respeitados e protegidos em todas as circunstâncias.

É crucial compreendermos como a violação dos dados pessoais sensíveis podem impactar os direitos à privacidade e potencializar riscos de discriminação. A exposição indevida de dados pessoais e sensíveis pode resultar em uma série de consequências negativas para os

indivíduos afetados, indo além do simples acesso não autorizado às suas informações. A violação pode levar a situações de estigma, constrangimento ou discriminação, especialmente em contextos delicados como o da pandemia de Covid-19.

Durante a pandemia, diversas formas de discriminação ganharam notoriedade, sendo uma das mais evidentes a xenofobia contra indivíduos de origem chinesa, conhecida como "sinofobia". Atribuições infundadas e preconceituosas, amplamente difundidas por algumas mídias e indivíduos, culparam erroneamente esses grupos pela propagação do vírus, acirrando a hostilidade e o preconceito. Tais atitudes não apenas são moralmente repreensíveis, como também violam princípios de respeito e dignidade humana. O vazamento de dados pessoais e de saúde durante a pandemia pode exacerbar essas situações, ao permitir a identificação ou associação de indivíduos a determinadas condições de saúde, nacionalidades ou outros atributos sensíveis. Isso não apenas viola a privacidade, mas também pode resultar em discriminação e estigmatização, afetando a vida social, o emprego, o acesso a serviços e a saúde mental dos indivíduos. (KHALIL, 2021)

O vazamento de informações pode servir como catalisador para a desinformação e alimentar ataques discriminatórios não apenas contra indivíduos de origem chinesa, mas contra todos aqueles afetados pelo vírus. Este cenário destaca os efeitos prejudiciais que tais vazamentos podem ter sobre a vida dos indivíduos cujos dados foram expostos, evidenciando a necessidade urgente de responsabilização das entidades envolvidas e de uma proteção mais eficaz dos dados pessoais, conforme estipulado pela LGPD.

Diante dos desafios impostos pelos vazamentos de dados, é imperativa uma análise aprofundada para compreender a interação entre as dimensões de fato, valor e norma. Como podemos fortalecer a segurança dos dados ao mesmo tempo em que garantimos a eficiência dos serviços de saúde? A solução engloba não somente estratégias técnicas, mas também a promoção de uma cultura de privacidade e responsabilidade, refletindo um comprometimento com princípios éticos e aderência às regulamentações. Ao investigar os vazamentos de dados no contexto da saúde pública sob a ótica da Teoria Tridimensional do Direito de Miguel Reale, ponderamos sobre os incidentes (fato), a relevância da privacidade e da proteção de dados (valor) e o alinhamento com a LGPD (norma). Estes elementos são interdependentes e juntos delineiam nossa interpretação e estratégias diante desses desafios.

No âmbito da saúde, a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece o princípio da não discriminação como um pilar central, reconhecendo a importância crítica de proteger dados sensíveis para evitar a estigmatização e preconceito baseados em histórico médico, dados genéticos, ou outras informações sensíveis. A disseminação inadequada de

informações pessoais não somente contraria a legislação, mas também pode submeter as vítimas a constrangimentos psicológicos e danos irreparáveis, indo contra tudo o que a LGPD visa proteger.

3.3 Estudo de Caso: O Incidente de Vazamento de Dados no Ministério da Saúde e Implicações da LGPD

No Brasil, sistemas de informação fazem parte da vigilância epidemiológica nacional e monitoram uma variedade de problemas de saúde. Os sistemas de informação na vigilância em saúde são projetados para permitir respostas rápidas em caso de epidemias ou mesmo eventos inesperados de propagação de agentes infecciosos. Por exemplo, durante a epidemia do vírus H1N1, o objetivo claro era aumentar o Sistema de Vigilância Epidemiológica para SRAG, também conhecido como SIVP-Gripe, para rastrear o aumento dos casos. Muitos mecanismos de monitoramento relacionados a emergências de saúde pública podem ser comprometidos se os dados armazenados nesses sistemas forem indisponíveis, claro que quanto mais utilizados esses sistemas mais dados eles tem e assim surge uma problemática de como deve ser resguardado os direitos dos titulares desse dados.

O exemplo recente do Hospital Albert Einstein serve como um exemplo premente da necessidade de rigorosas práticas de segurança desses dados. Em 2020, no enfrentamento da pandemia causada pela disseminação descontrolada do SARS-CoV-2, o coronavírus causador da COVID-19, o Hospital Albert Einstein, uma das principais instituições de saúde do Brasil, utilizou sistemas de dados massivos para gerenciar informações sobre pacientes afetados pelo vírus, incluindo detalhes sobre a gravidade da doença, histórico médico e outras condições preexistentes. E isso acontecia porque o Hospital Albert Einstein utilizava dois sistemas que montavam esse big data, ambos oriundos do governo federal brasileiro: o E-SUSVE, onde eram notificados os casos suspeitos e confirmados da COVID-19, além da complexidade que a doença tomara naquele organismo, e o Sivep-Gripe, software onde se registrava todas as internações por síndrome respiratória aguda grave.

A violação desses dados expõe os riscos inerentes ao armazenamento e processamento de informações médicas sensíveis, ressaltando a necessidade imperativa de segurança robusta e protocolos de proteção de dados para prevenir acessos não autorizados e garantir a confidencialidade e a integridade das informações dos pacientes. (PRIVACYTECH. 2020)

O incidente de vazamento de dados ocorrido no Hospital Albert Einstein em São Paulo, em maio de 2020, é um exemplo notório das vulnerabilidades que até mesmo instituições renomadas enfrentam no gerenciamento de informações sensíveis. As credenciais publicadas

permitiam o acesso a dados sensíveis de cerca de 16 milhões de pessoas, incluindo pacientes com diagnósticos suspeitos ou confirmados de Covid-19. As informações expostas incluíam CPF, endereço, telefone e detalhes sobre doenças pré-existentes. O incidente foi resultado de uma publicação de logins e senhas em uma plataforma aberta de compartilhamento de códigos, o GitHub, por um funcionário do hospital. As credenciais publicadas permitiam o acesso a dados sensíveis de cerca de 16 milhões de pessoas, incluindo pacientes com diagnósticos suspeitos ou confirmados de Covid-19. (G1, 2020)

A publicação das credenciais foi um erro humano cometido durante a realização de um teste na implementação de um modelo de dados, onde o funcionário esqueceu de remover o arquivo da página pública. O Hospital Albert Einstein tinha acesso a esses dados sensíveis como parte de um projeto em colaboração com o Ministério da Saúde do Brasil para monitoramento da pandemia de Covid-19.(G1, 2020)

A gravidade do incidente, teve sua gravidade acentuada quando o jornal "Estadão", de São Paulo, reportou sobre um link para o DataSUS que continha chaves de acesso ao sistema. Essa divulgação exacerbou a brecha de segurança já existente no hospital, demonstrando como a vulnerabilidade de um único ponto no sistema pode gerar amplas e graves consequências. (PRIVACYTECH. 2021)

Menos de um mês depois outro incidente ocorreu com os bancos de dados do Ministério da Saúde. O incidente relatado pela *Open Knowledge* Brasil envolvendo o sistema e-SUS Notifica ocorreu quando um arquivo com credenciais de acesso foi encontrado no código-fonte da plataforma, tornando-se acessível para quem pudesse localizá-lo. As credenciais davam acesso a um banco de dados contendo informações pessoais de cidadãos que haviam sido notificados de casos leves e moderados de Covid-19, suspeitos ou confirmados, por hospitais públicos e privados. Informações como identificação pessoal, tipo de teste realizado, sintomas, tratamento e condições pré-existentes estavam vulneráveis.

O incidente relacionado ao sistema e-SUS Notifica gerou amplas preocupações sobre as falhas de segurança e a adequação das políticas de gestão de informações e acesso a dados mantidos pelo Ministério da Saúde. De acordo com uma reportagem do G1, apesar das afirmações do Ministério da Saúde de que o sistema estava em conformidade com a Lei Geral de Proteção de Dados (LGPD), o episódio evidenciou a necessidade imperativa de melhorar a transparência e a eficácia das medidas de proteção de dados pessoais. (G1, 2020)

A correção do problema ocorreu dez dias após a notificação inicial à Controladoria-Geral da União, período durante o qual o Ministério da Saúde aparentemente não respondeu às solicitações da organização, que teve de realizar monitoramento diário para verificar a solução

da vulnerabilidade. Posteriormente, a Ouvidoria Geral da União encerrou o protocolo e o redirecionou automaticamente para a Ouvidoria do SUS. Em meio a esses desafios, a organização também solicitou uma auditoria para determinar a extensão do dano e verificar se houve acessos não autorizados ou downloads de dados, mas enfrentou dificuldades para acompanhar a solicitação. O Ministério da Saúde, em sua comunicação, mencionou que uma denúncia anônima havia sido recebida e assegurou que não houve invasão percebida no sistema pela sua equipe. (G1, 2020)

No contexto do vazamento de dados do sistema e-SUS Notifica, a *Open Knowledge Brasil*, valendo-se da Lei de Acesso à Informação (LAI), solicitou ao Ministério da Saúde informações detalhadas sobre os protocolos de segurança de dados pessoais adotados pelo sistema. Em resposta, o Ministério afirmou que o sistema estava em conformidade com a Lei Geral de Proteção de Dados (LGPD), mas não forneceu detalhes específicos sobre as medidas de segurança, alegando questões de segurança. (G1, 2020)

Esta resposta levanta questões sobre a observância do Artigo 6º, incisos VI e VII, da LGPD, que enfatizam a transparência e a prestação de contas no tratamento de dados pessoais. Esta abordagem parece entrar em conflito com o espírito da LGPD, particularmente em relação à necessidade de demonstrar claramente o cumprimento das normas de proteção e a eficácia das medidas de segurança implementadas, conforme delineado no Artigo 9º, da LGPD.

Adicionalmente, foi revelado que inúmeras pessoas, especificamente 8.714 indivíduos, tinham acesso para obter relatórios de casos suspeitos ou confirmados de Covid-19 pelo sistema. Essa quantidade foi considerada excessiva pela diretora da *Open Knowledge* Brasil, Fernanda Campagnucci, que argumentou que isso reflete não apenas uma falha de segurança, mas também uma abordagem equivocada na política de gestão da informação. Ela questionou a necessidade de tantas pessoas terem acesso a dados detalhados, apontando para uma possível falta de minimização de dados e de medidas adequadas para limitar o acesso apenas àqueles que necessitam da informação para desempenhar suas funções. (G1, 2020)

O referido princípio, contemplado no Artigo 6º, inciso III, da LGPD, levanta preocupações com a política de gestão da informação do Ministério, pois a ampla disponibilidade de acesso a dados detalhados pode não estar alinhada com as diretrizes da LGPD, que preconizam a limitação do tratamento dos dados ao mínimo necessário para atingir as finalidades legítimas, efetivas e específicas.

O caso também evidencia a complexidade inerente ao equilíbrio entre a segurança dos dados e a transparência nos sistemas de informação de saúde, especialmente sob as pressões de uma pandemia. A gestão e o compartilhamento de dados durante a crise da Covid-19 são

essenciais para a resposta de saúde pública, e este incidente ressalta a necessidade de revisões contínuas e melhorias nas políticas de segurança de dados.

Tais políticas devem estar em conformidade com as práticas recomendadas e os requisitos legais estabelecidos pela LGPD, assegurando que as medidas de proteção de dados pessoais sejam tanto eficazes quanto transparentes, conforme estipulado nos Artigos 46 a 50 da LGPD, que abordam a segurança dos dados. (BRASIL, 2018)

Apenas alguns meses depois, em dezembro de 2020, uma nova falha de segurança foi relatada pelo Ministério da Saúde, afetando cerca de 243 milhões de registros de brasileiros, incluindo dados de indivíduos já falecidos. Embora neste segundo incidente tenha sido alegado que não houve acesso a informações sensíveis, mas sim a vazamentos de bases cadastrais, a ocorrência ressalta a persistente fragilidade na proteção de dados, mesmo em entidades com recursos substanciais. (PRIVACYTECH, 2021)

Os tipos de dados expostos nesses vazamentos, embora possam não ser considerados extremamente sensíveis como informações de saúde detalhadas, ainda representam um risco significativo. Informações como CPF, nome completo, endereço e telefone são tipos de dados pessoais que, nas mãos de indivíduos mal-intencionados, podem se tornar instrumentos para a prática de fraudes e golpes, constituindo uma séria violação da privacidade dos indivíduos. Além disso, é importante reconhecer que o manejo inadequado de qualquer tipo de dado pessoal, mesmo aqueles não considerados extremamente sensíveis, pode resultar em discriminação e outros prejuízos significativos para as pessoas cujos dados foram expostos. Neste sentido:

> [...] seja porque dados pessoais, aparentemente não “sensíveis”, podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas” (RODOTÀ; 2008, p. 84 *apud* MULHOLLAND, 2018)

Os recentes incidentes de segurança de dados envolvendo o Ministério da Saúde evidenciam a importância crítica de uma governança de dados aprimorada e enfatizam a necessidade de protocolos de segurança rigorosos, conforme articulado nos artigos 46 a 50 da Lei Geral de Proteção de Dados (LGPD). Estes eventos não só destacam a necessidade vital de uma resposta rápida e transparente em caso de violações, como também reforçam a importância de implementar medidas corretivas imediatas. Estas ações são fundamentais para mitigar os danos e evitar a recorrência de tais eventos, alinhando-se com os princípios e obrigações delineados pela Lei Geral de Proteção de Dados (LGPD). (BRASIL, 2018)

No contexto descrito, os incidentes de segurança de dados no Ministério da Saúde evidenciam transgressões aos princípios estabelecidos no Artigo 6º da Lei Geral de Proteção de Dados (LGPD), que abordam a necessidade de livre acesso, garantia de integridade e qualidade dos dados, transparência e segurança. Essas violações não só comprometem a confiança do público e a segurança dos dados pessoais, mas também expõem as entidades responsáveis a responsabilidades legais e regulatórias significativas.

Diante das violações, a Autoridade Nacional de Proteção de Dados (ANPD), entidade incumbida de assegurar a observância da LGPD e proteger os direitos fundamentais de liberdade e privacidade, emitiu uma notificação ao Ministério da Saúde solicitando esclarecimentos acerca do incidente.Esta ação está em conformidade com as funções da Autoridade Nacional de Proteção de Dados (ANPD), que são responsáveis por monitorar e aplicar penalidades administrativas em caso de violação dos requisitos da Lei Geral de Proteção de Dados (LGPD). O Artigo 52 da referida lei descreve as sanções pertinentes. (BRASIL, 2018)

Além disso, a situação motivou investigações adicionais por parte da Polícia Federal e do Ministério Público Federal, que orientaram o Ministério da Saúde a elaborar e divulgar um Relatório de Impacto à Proteção de Dados Pessoais. Essa medida tem como objetivo avaliar a extensão dos danos e implementar ações corretivas, garantindo uma resposta adequada ao incidente e a adoção de práticas que previnam a ocorrência de novas violações.

O titular da pasta da Saúde informou que o ministério já havia fornecido cópias de segurança dos dados comprometidos logo após o incidente. Isso diminuiu significativamente o risco de perda de dados. No entanto, esse evento enfatiza a necessidade de criar uma política sólida de gestão de dados e implementar sistemas proativos e reativos eficazes para o manejo de incidentes de segurança, a fim de responder e prevenir a exposição de dados potenciais.

No mês de maio de 2022, o Ministério da Saúde informou sobre uma nova tentativa de invasão. Isso fez com que sistemas cruciais como Conecte SUS, e-SUS Notifica e SI-PNI ficassem inoperantes por alguns dias. Como medida preventiva para proteger as informações, o acesso a esses sistemas foi bloqueado, de acordo com o ministério.

É essencial pensar sobre quem é responsável por esses problemas e falhas de segurança. O Artigo 52, em particular, enumera várias penalidades que a ANPD pode aplicar aos responsáveis pelo tratamento de dados em caso de violação. Esses castigos incluem advertências e restrições parciais ou totais para atividades relacionadas ao processamento de dados. Além disso, o primeiro parágrafo do mesmo artigo enfatiza que vários fatores serão levados em consideração na determinação das penalidades. Esses fatores incluem, entre outros,

a gravidade e a natureza da infração, a intenção do infrator, a situação financeira do responsável e os benefícios econômicos resultantes da infração. (BRASIL, 2018)

Cabe, neste ponto, lembrar que a LGPD prevê, em seu artigo 52, as seguintes sanções:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> VII - (VETADO);
> VIII - (VETADO);
> IX - (VETADO).
> X - (VETADO);
> XI - (VETADO);
> XII - (VETADO).
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
> § 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei n.º 8.112, de 11 de dezembro de 1990, na Lei n.º 8.429, de 2

> de junho de 1992, e na Lei n.º 12.527, de 18 de novembro de 2011. (BRASIL, 2018)

É importante destacar que o § 3º do Artigo 52 da LGPD estende a aplicação de várias dessas sanções a entidades e órgãos públicos, com a ressalva de que a pena pecuniária é excluída desse rol para órgãos públicos, evitando que o ônus financeiro recaia sobre o contribuinte. Essa disposição reflete a compreensão de que as penalidades devem ser apropriadas e justas, considerando a natureza do agente de tratamento de dados e as circunstâncias do caso. (BRASIL, 2018)

Essas normas e medidas são fundamentais para garantir que as entidades responsáveis pelo tratamento de dados pessoais adotem práticas que assegurem a proteção adequada dessas informações, particularmente em um contexto de gestão de saúde pública, onde a segurança e a privacidade dos dados são de extrema importância.

Há de se pontuar também que o artigo 12 da LGPD desempenha um papel crucial, delineando as obrigações específicas para controladores e operadores no contexto de violações de dados. Uma das estratégias destacadas para a proteção de dados pessoais é a anonimização, que transforma dados pessoais em não identificáveis, eliminando ou modificando os elementos que permitem a identificação do titular dos dados. A anonimização efetiva requer que os dados sejam irreversivelmente desvinculados de indivíduos específicos, garantindo que não possam ser reconectados a seus titulares por nenhum meio técnico razoavelmente disponível.(BRASIL, 2018)

Existem basicamente duas abordagens para a anonimização de dados pessoais. A primeira é a anonimização total, onde os dados são transformados de tal maneira que a reidentificação do titular dos dados é impossível ou impraticável, utilizando todos os meios técnicos disponíveis. A segunda, conhecida como pseudoanonimização, envolve a adição de uma camada adicional de informações que, embora torne o dado menos identificável, ainda permite a associação do dado pessoal ao seu titular sob certas condições. Ambas as estratégias têm seus lugares em um regime de proteção de dados, dependendo do contexto específico e dos riscos envolvidos. No entanto, é crucial que as entidades encarregadas de lidar com dados pessoais estejam equipadas com as ferramentas e o conhecimento necessários para implementar essas técnicas de forma eficaz e em conformidade com a LGPD. Isso inclui não só a compreensão técnica da anonimização e pseudoanonimização, mas também uma apreciação contínua das implicações legais e éticas associadas ao tratamento de dados sensíveis.(BRASIL, 2018)

Na Lei de Proteção de Dados brasileira, LGPD, o conceito de pseudonimização é delineado no § 4º do artigo 13. Essa técnica envolve o processamento de dados de forma que a identificação do indivíduo não seja direta ou indiretamente possível, exceto por meio do uso de informações adicionais que são mantidas separadamente pelo controlador dos dados em um ambiente seguro e controlado. Este método é especialmente relevante em contextos como estudos de saúde pública, onde pesquisadores necessitam acessar dados pessoais para avançar em seus estudos. A LGPD recomenda a pseudonimização, assim como a anonimização, como estratégias para preservar a segurança dos dados utilizados, assegurando ao mesmo tempo que todos os padrões éticos pertinentes à pesquisa e estudo sejam rigorosamente seguidos.

Há de se ressaltar que em casos como o do Hospital Albert Einstein, onde direitos fundamentais e constitucionais foram violados, a reparação aos dados causados é versada na LGPD em seu artigo 42, onde podemos abstrair que não somente o hospital pode ser responsabilizado mas o próprio Ministério da Saúde tem responsabilidade solidária no caso, sendo aplicáveis sanções administrativas, assim como reparação aos danos causados. Nesse sentido, Caitlin Mulholland traz a seguinte análise:

> Consideradas as posições opostas levantadas pelos autores citados, afirma-se que a Lei Geral de Proteção de Dados, em seu artigo 42, adota a teoria que impõe a obrigação de indenizar independentemente da análise da culpa dos agentes de tratamento de dados, isto é, a responsabilidade civil é objetiva. Fundamenta esta conclusão o fato de que a atividade desenvolvida pelo agente de tratamento é evidentemente uma atividade que impõe riscos aos direitos dos titulares de dados. Estes riscos, por sua vez, são intrínsecos, inerentes à própria atividade. Significa dizer que os danos resultantes da atividade habitualmente empenhada pelo agente de tratamento de dados, uma vez concretizados, são quantitativamente elevados - pois atingem um número indeterminado de pessoas - e qualitativamente graves - pois violam direitos que possuem natureza personalíssima, reconhecidos pela doutrina como direitos que merecem a estatura jurídica de direitos fundamentais. (MULHOLLAND, 2021)

Além das medidas jurídicas e tecnológicas, um componente crucial na prevenção de vazamentos de dados é a educação. Informar profissionais da saúde e pacientes sobre seus direitos e responsabilidades, bem como sobre práticas seguras de gestão de dados, é fundamental para construir um sistema de saúde resiliente e confiável. A complexidade dos desafios de proteção de dados na saúde exige uma abordagem colaborativa. Incluir um apelo para ação que convide legisladores, profissionais de saúde, tecnólogos, pacientes e a sociedade civil a trabalharem juntos pode reforçar a ideia de que a proteção efetiva dos dados é uma responsabilidade compartilhada.

CONCLUSÃO

O trabalho realizado buscou entender e analisar a Lei Geral de Proteção de Dados (LGPD) do Brasil, visando aprimorar a compreensão sobre sua aplicabilidade e eficácia, especialmente em incidentes de vazamento de dados sensíveis como o ocorrido com o sistema e-SUS Notifica. A monografia foi orientada pela Teoria Tridimensional do Direito de Miguel Reale, utilizando uma abordagem que integra normas, fatos e valores para uma análise do cenário jurídico digital, empregando uma metodologia analítico-dedutiva complementada pelo pensamento hermenêutico para interpretação legal e cultural, assim como pesquisa documental, bibliográfica e estudo de caso.

A aplicação da Teoria Tridimensional do Direito ao desafio dos vazamentos de dados na saúde pública nos permite ver além dos incidentes isolados para entender o quadro completo de como os fatos, valores e normas interagem e moldam o futuro do atendimento médico. Este estudo, envolto na relevância da Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro, especialmente durante a crise pandêmica, reflete sobre a emergente necessidade de uma abordagem robusta e eficaz na proteção de dados pessoais sensíveis, particularmente aqueles relacionados à saúde.

Dentro deste contexto, a presente pesquisa se propôs a responder ao seguinte problema: Como as normas legais, particularmente a Lei Geral de Proteção de Dados, estão se adequando aos desafios tecnológicos e sociais emergentes no contexto da proteção de dados sensíveis em tempos de crise?

A aplicabilidade e a eficácia da LGPD foram exploradas através de uma investigação detalhada em três capítulos, cada um abordando uma faceta distinta da lei e sua interação com o tecido social e tecnológico contemporâneo. Ao longo deste trabalho, emergiu uma visão crítica da LGPD: apesar de seus avanços promissores, evidenciou-se que a lei requer adaptações contínuas e uma implementação mais robusta, especialmente em setores críticos como o da saúde.

Em um primeiro momento, a pesquisa se debruçou sobre as origens e o desenvolvimento da Lei Geral de Proteção de Dados (LGPD) no Brasil, estabelecendo um contexto fundamental para compreender como a lei surgiu e evoluiu dentro do ambiente global de direitos digitais e privacidade de dados. O estudo das origens e evolução da LGPD revelou a trajetória do Brasil em um complexo cenário internacional, marcado por influências de iniciativas globais e requisitos de conformidade, sublinhando a importância de reconhecer o histórico e as influências externas que formaram a LGPD. Além disso, o estudo procurou situar o Brasil no

contexto da Sociedade da Informação, buscando entender como a privacidade é percebida e gerida neste novo ambiente. Observou-se que a infraestrutura de rede criada pelas modernas tecnologias de informação transformou fundamentalmente a sociedade. Com a popularização da internet e a adesão quase universal às tecnologias conectadas, as fronteiras entre os mundos online e offline se tornam cada vez mais difusas, com vidas cotidianas sendo compartilhadas com milhões na rede. Esse fenômeno levanta debates sobre a possível erosão da privacidade na sociedade contemporânea.

Contudo, enquanto as pessoas compartilham aspectos de suas vidas na esfera pública, ainda persiste um domínio privado que muitos desejam proteger de intrusões externas. Há argumentos válidos para a defesa da privacidade hoje em dia, onde sua violação mais comum não vem da invasão física de domicílios ou da interceptação de correspondências, mas do acúmulo e uso indiscriminado de informações pessoais em transações abstratas.

As pessoas expõem suas vidas online, mas ainda assim fazem escolhas sobre o que compartilham, mantendo certas informações dentro de uma esfera privada. Esta seleção consciente destaca que, apesar da vasta exposição na internet, existe uma parte da vida individual que permanece resguardada, indicando uma área que continua não pública e protegida.

Em um segundo momento se discutiu o imperativo jurídico e social da proteção de dados pessoais na era digital, aprofundando na essência da LGPD e seu papel no cenário jurídico e social brasileiro, este capítulo discutiu a importância crítica da proteção de dados na era digital, explorando a aliança entre a LGPD, os princípios constitucionais e éticos, e a responsabilidade dos agentes de tratamento. Os debates sobre privacidade e ética foram especialmente iluminados, destacando a responsabilidade social e legal emergente em um mundo digitalizado.

Adicionalmente, foi realizada uma análise substancial dos aspectos relacionados à proteção de dados e privacidade, examinando como a legislação brasileira salvaguarda a privacidade e os dados pessoais. A privacidade é protegida como um direito fundamental no sistema jurídico brasileiro, conforme estabelecido no artigo 5º, inciso X, da Constituição Federal. Além disso, é reconhecida como um direito da personalidade, conforme delineado no artigo 21 do Código Civil. Este artigo não apenas eleva a privacidade a um direito autônomo, mas também oferece uma proteção preventiva, isto é, visa "impedir" atos que ameacem a vida privada de um indivíduo. A implementação de uma tutela inibitória do direito à privacidade é justificada pela irreversibilidade de sua violação; uma vez que o privado se torna público, não é possível reverter a situação.

A LGPD estabelece distinções claras entre as condições que permitem o tratamento de dados pessoais e dados sensíveis. As condições legais para o tratamento de dados sensíveis, especificadas no artigo 11 da lei, são mais restritivas em comparação às condições para dados pessoais não sensíveis. Essa diferenciação é crucial para entender como a legislação busca proteger informações mais delicadas e privadas dos indivíduos.

O estudo avançou com conceitos de proteção à privacidade e proteção de dados pessoais, articulando a diferença entre interromper e controlar o fluxo de informações. A proteção de dados, relacionada ao controle informacional, é uma proteção procedimental que permite o fluxo informacional, mas este deve ser regulado para promover responsabilidades públicas significativas para os agentes que tratam dados pessoais.

Finalmente, o terceiro capítulo foi dedicado a explorar a natureza e as categorias de dados pessoais e sensíveis, focando na análise da complexidade inerente aos dados pessoais, com um destaque especial para os dados sensíveis no âmbito da LGPD. Este segmento elucidou as consequências éticas, legais e sociais envolvidas na administração de dados, com uma atenção particular voltada para o domínio da saúde pública. Dados pessoais são definidos como qualquer informação que se refira a um indivíduo identificado ou identificável, constituindo um aspecto fundamental da personalidade humana e, como tal, requerendo classificação e proteção cuidadosa. Foi observado que os dados pessoais se diversificam em várias categorias, dentre as quais os dados sensíveis se destacam devido aos riscos associados ao seu armazenamento, tratamento e circulação, particularmente em relação a práticas discriminatórias. Tais riscos justificam a necessidade de uma proteção mais rigorosa e limitações específicas no tratamento desses dados. Dados de saúde são tipicamente considerados sensíveis devido ao seu conteúdo profundamente pessoal e aos riscos significativos envolvidos em seu manejo; sua distribuição indiscriminada pode resultar em danos sérios aos indivíduos, demandando assim uma vigilância e cuidado intensificados.

Conclui-se que o valor intrínseco dos dados de saúde deriva do quão sensíveis às informações são e das possíveis aplicações práticas desses dados. Considerando a lucratividade do setor de saúde, assim como a vasta quantidade de dados de saúde dos pacientes disponíveis para determinados agentes, sem transparência clara sobre como esses dados são utilizados, emerge a preocupação de que existe um mercado de troca de informações, frequentemente desvantajoso para o titular dos dados.

O caso do e-SUS Notifica foi utilizado como um exemplo específico para ilustrar as vulnerabilidades e as necessidades urgentes na proteção de dados sensíveis, servindo como uma

representação em menor escala das amplas implicações e desafios enfrentados na proteção de tais dados.

Ao revisitar cada um desses componentes, restou evidente que, apesar dos avanços legislativos e das promessas de segurança e privacidade, a LGPD está em um processo contínuo de evolução e adaptação. As falhas e vulnerabilidades identificadas, particularmente no estudo de caso do e-SUS Notifica, demonstram a lacuna existente entre a legislação e a prática efetiva, revelando um panorama de desafios e oportunidades.

Além disso durante este estudo emergiu um aspecto crítico ao discutir vazamentos de dados que é o erro humano. Apesar das robustas estruturas legais e tecnológicas, o fator humano permanece como um elo significativo e vulnerável. Erros de configuração, negligência na proteção de dados e falhas no entendimento e na aplicação das normas de segurança são apenas alguns exemplos de como as ações ou omissões humanas podem levar a consequências drásticas. A discussão sobre o erro humano nos leva a questionar: Como a LGPD responde a esses desafios intrinsecamente humanos e qual é o papel da legislação na mitigação desses riscos?

A LGPD, em seu núcleo, não apenas impõe obrigações e padrões técnicos para a proteção de dados, mas também enfoca na conscientização, formação e capacitação dos indivíduos que interagem com dados pessoais. A lei reconhece que a segurança dos dados é uma responsabilidade compartilhada, estendendo-se desde os mais altos níveis de governança corporativa até o indivíduo que opera sistemas no seu dia a dia. Por isso, além de sanções e diretrizes, a LGPD promove uma cultura de proteção de dados que visa reduzir os riscos associados ao erro humano através da educação, conscientização e treinamentos regulares.

Portanto, cabe enfatizar que o sucesso da LGPD e de leis similares depende não apenas de sólidos quadros legais e tecnológicos, mas também de uma transformação cultural e comportamental contínua. É vital que as organizações e os indivíduos estejam constantemente engajados na aprendizagem, no treinamento e na conscientização sobre a importância e as práticas de segurança de dados.

Diante dos resultados obtidos reforçam a hipótese inicial de que, apesar das promessas de segurança e privacidade trazidas pela LGPD, há um caminho considerável a ser percorrido na implementação efetiva de suas diretrizes, especialmente em setores críticos como o da saúde. A LGPD é um marco significativo na trajetória jurídica brasileira, mas seu sucesso depende de implementações efetivas, acompanhamento contínuo e adaptações ágeis frente às inovações tecnológicas e às mudanças sociais. Além disso, sugere-se uma investigação contínua sobre as

intersecções entre tecnologias emergentes, privacidade e legislação, bem como a promoção de uma cultura de proteção de dados mais robusta e consciente em todos os níveis da sociedade.

Isso responde ao problema de pesquisa, demonstrando que a LGPD é um avanço significativo na legislação brasileira, mas ainda requer ajustes contínuos para enfrentar eficazmente os desafios emergentes na proteção de dados pessoais. Diante dos achados, torna-se imperativo não só aprimorar as estratégias de segurança e privacidade mas também promover uma cultura de proteção de dados mais sólida e consciente, envolvendo todos os atores do ecossistema de saúde. Isso inclui desde a formação e sensibilização de profissionais até a adoção de políticas públicas e práticas corporativas que reflitam os valores éticos e legais da sociedade.

A metodologia empregada permitiu uma análise detalhada e abrangente, proporcionando uma compreensão profunda e multifacetada dos fenômenos investigados, destacando a importância da constante adaptação e evolução das normativas para garantir a proteção eficaz dos dados pessoais sensíveis e a privacidade dos indivíduos em um mundo digitalizado.

Os direcionamentos futuros devem incluir a continuação da pesquisa e do monitoramento das práticas de proteção de dados, a avaliação de novas tecnologias e metodologias para a segurança da informação e a promoção de um diálogo mais amplo e inclusivo sobre privacidade e proteção de dados no Brasil. Este trabalho espera contribuir para esse debate, fornecendo um ponto de partida sólido para futuras investigações e ações na busca por um equilíbrio entre inovação, privacidade e proteção de dados na era digital. No entanto, reconhece-se que a complexidade do tema e o constante avanço tecnológico demandam uma vigilância contínua e possíveis ajustes nos instrumentos de coleta de dados e nas abordagens de análise.

REFERÊNCIAS

BIONI, Bruno. **Dados “anônimos” como antítese de dados pessoais: o filtro da razoabilidade**. Disponível em: http://genjuridico.com.br/2019/10/11/dados-anonimos-antitese-dados-pessoais/. Acesso em: 15 nov. 2023.

BOTELHO, Marcos César; CAMARGO, Elimei Paleari do Amaral. **A aplicação da Lei Geral de Proteção de Dados na saúde**. Revista de Direito Sanitário, 2021.

BRASIL. **Código de Defesa do Consumidor**. Decreto Presidencial nº 2.181, de 20 de março de 1997, Brasília–DF, 1997.

BRASIL. **Constituição da República Federativa do Brasil** de 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 set. 2023.

BRASIL. **Lei Geral De Proteção De Dados Pessoais (LGPD),** Lei nº 13.709, De 14 De Agosto De 2018**.** Brasília–DF: Presidência Da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14020.htm. Acesso em: 12 dez. 2022.

BRASIL. **Marco Civil da Internet**. Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 ago. 2022.

BRASIL. **Tribunal Superior do Trabalho. Súmula nº 443**. Disponível em: https://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_401_450.html. Acesso em: 28 dez. 2023.

CASTELLS, Manuel. **A sociedade em rede.** 9. ed. São Paulo: Paz e Terra, 2006. v. 1.

CASTELLS, M. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Tradução Maria Luiza X. de A. Borges. Revisão técnica Paulo Vaz. Rio de Janeiro: Editora Jorge Zahar, 2003.

CONFESSORE, N. **Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.** New York Times, 4 abr. 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 23 jan. 2023.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada. 2. ed**. São Paulo: Editora Revista dos Tribunais, 2019. p. 71.

COSTA, F. P. et al. "**O futuro da proteção de dados na saúde digital"**. Revista de Tecnologia da Informação e Comunicação, 2022.

DINIZ, D. et al. "**Desafios da privacidade de dados no Brasil"**. Revista de Saúde Pública, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Revista dos Tribunais, 2020.

Entrevista de Spiros Simitis, concedida à Revista Forschung Frankfurt: Das Wissenschaftsmagazin der Goethe-Universität, vol. 1/2015, disponível em <www.forschung-frankfurt.uni-frankfurt.de>. Acesso em: 28 dez. 2023.

G1. **Senhas do Ministério da Saúde para sistema de notificação de Covid-19 também ficaram expostas em junho, diz ONG**. G1 Economia Tecnologia, 27 nov. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/11/27/senhas-do-ministerio-da-saude-para-sistema-de-notificacao-de-covid-19-tambem-ficaram-expostas-em-junho-diz-ong.ghtml. Acesso em: 28 dez. 2023.

G1. **Vazamento de senhas do Ministério da Saúde expõe informações de pessoas que fizeram testes de Covid-19, diz jornal.** G1 Bem Estar Coronavírus, 26 nov. 2020. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/11/26/vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml. Acesso em: 28 dez. 2023.

GARCIA, Bruna Pinotti. **Ética na Internet: os conflitos entre particulares no ciberespaço face às dimensões da liberdade e os princípios éticos como base de solução.** 2010. 150 f. Trabalho de Curso (Bacharelado em Direito) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2010.

GARCIA, Lara Rocha; FERNANDES, Edson Aguilera; GONÇALVES, Rafael Augusto Moreno; BARRETO, Marcos Ribeiro Pereira. **Lei Geral de Proteção de Dados (LGPD): Guia de Implantação**. Editora Edgard Blücher Ltda., 2020.

GOLDSCHMIDT, Ronaldo; PASSOS, Emmanuel; BEZERRA, Eduardo. **Data mining: conceitos, técnicas, algoritmos, orientações e aplicações**. 2. ed. Rio de Janeiro: Elsevier, 2015. p. 3.

GREENWALD, G. **NSA collecting phone records of millions of Verizon customers daily.** The Guardian, 6 jun. 2023. Disponível em: <URL>. Acesso em: 28 dez. 2023. (Nota: O URL precisa ser especificado)

HERÓDOTO. História. Brasília: Ed. Da Universidade de Brasília, 1985.

HUGHES, C. **It's Time to Break Up Facebook**. New York Times, 9 maio 2019. Disponível em: https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html?searchresultposition=1. Acesso em: 23 jan. 2023.

INFOGRIPE. **Resumo do Boletim InfoGripe - Semana Epidemiológica 48 de 2021**. Disponível em: https://bit.ly/infogripe-resumo-482021. Acesso em: 28 dez. 2023.

JESUS, D. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

JESUS, D. E. de. **Direito penal. 25.ed.** São Paulo: Saraiva, 2014.

KHALIL, O. A. K.; DA SILVA KHALIL, S.; CAETANO JUNIOR, E. **Xenofobia: um velho sintoma de um novo Coronavírus.** Revista Thema, Pelotas, v. 20, p. 132–142, 2021. DOI: 10.15536/thema.V20.Especial.2021.132-142.1855. Disponível em: https://periodicos.ifsul.edu.br/index.php/thema/article/view/1855. Acesso em: 02 out. 2023.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**. Tese de mestrado da Faculdade de Direito da Universidade Federal de Juiz de Fora. Juiz de Fora, 2019. Disponível em: https://repositorio.ufjf.br/jspui/bitstream/ufjf/11438/1/mariareginadetonicavalcantirigolonkorkmaz.pdf. Acesso em: 02 dez. 2023.

LEMOS, O. **Marco Civil como símbolo do desejo por inovação no Brasil**. In: LEITE, G.; LEMOS, R. (Eds.). Marco Civil da Internet. São Paulo: Atlas, 2014.

LÈVY, Pierre. **Cibercultura**. Tradução: Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

LIMA, C.R.P. D. **Comentários à Lei Geral de Proteção de Dados.** São Paulo: Almedina, 2020.

Marsden, C. **Regulating the global information society**. Londres e Nova Iorque: Routlegdge, 2000.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva Educação, 2014. (Série IDP: linha de pesquisa acadêmica).

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. 2008. 158 f. Dissertação (Mestrado) – Curso de Direito. Universidade de Brasília, Brasília, 2008.

MENKE, Fabiano. **Spiros Simitis e a primeira lei de proteção de dados do mundo**.Disponivel em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo. Acesso em: 20 jan. 2023.

MULHOLLAND, Caitlin. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018).** Revista Jur. Puc. Rio, 2021. Disponível em: https://www.jur.puc-rio.br/wpcontent/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 28 dez. 2023.

MULHOLLAND, C. **Dados pessoais sensíveis e a tutela de Direitos Fundamentais. Uma análise à luz da Lei geral de Proteção de Dados (Lei 13.709/18).** R. Dir. Gar. Fund., Vitória, 2018, v. 19, n. 3.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 03 dez. 2023.

OLIVEIRA, S. R. et al. **Consentimento informado e proteção de dados em saúde**. Revista Bioética, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 28 dez. 2023.

PAESANI, Liliana Minardi. **Direito e internet: liberdade de informação, privacidade e responsabilidade civil.** 6. ed. São Paulo: Atlas. 2013.

PECK, Patrícia. **Direito digital**. São Paulo, 2002.

PECK, Patrícia. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD).** São Paulo: Editora Saraiva, 2023.

PECK, Patrícia. **Direito Digital**. São Paulo, 2021.

PESTANA, Marcio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais).** Disponível em: https://www.conjur.com.br/dl/ar/artigo-marcio-pestana-lgpd.pdf. Acesso em: 07 set. 2023.

PRIVACYTECH. **Mais de 200 milhões de brasileiros têm dados pessoais expostos em nova falha de segurança do Ministério da Saúde**. PrivacyTech. Disponível em: https://privacytech.com.br/destaque/mais-de-200-milhoes-de-brasileiros-tem-dados-pessoais-expostos-em-nova-falha-de-seguranca-do-ministerio-da-saude.,381645.jhtml. Acesso em: 27 dez. 2023.

PRIVACYTECH. **Vazamento no Ministério da Saúde expõe dados de 16 milhões de pacientes de COVID-19. PrivacyTech, 2020.** Disponível em: https://privacytech.com.br/destaque/vazamento-no-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid.,381009.jhtml. Acesso em: 27 dez. 2023.

REALE, Miguel. **O Direito como Experiência. 2.ª ed.** São Paulo: Saraiva, 1992.

REALE, Miguel. **Introdução à Filosofia. 3.ª ed.** São Paulo: Saraiva, 1994.

REALE, Miguel. **Filosofia do Direito. 19.ª ed.** São Paulo: Saraiva, 1999.

REALE, Miguel. **Teoria Tridimensional do Direito. 5.ª ed.** São Paulo: Saraiva, 2010.

ROCHA, Thauane Prieto; PIVETO, Lucas Colombera Vaiano. **Um diálogo sobre a relevância da proteção de dados pessoais e sensíveis nos estabelecimentos de saúde.** Disponível em: https://aberto.univem.edu.br/bitstream/handle/11077/2122/TC%20-%20Thauane%20Prieto%20Rocha.pdf?sequence=1&isAllowed=y. Acesso em: 26 dez. 2023.

RODOTÀ, Stefano. **A vida privada na sociedade da vigilância: a privacidade hoje**. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTOS, A. R. "**Regulação internacional de proteção de dados em saúde".** Direito e Saúde, 2021.

SCHAEFER, Fernanda. **Proteção de dados de saúde na sociedade de informação: a busca pelo equilíbrio entre privacidade e interesse social.** Curitiba: Juruá, 2010.

SCHREIBER, Anderson. **Privacidade na pandemia: por que adiar a LGPD é um erro?** Jota, 22 abr. de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/privacidade-na-pandemia-por-que-adiar-a-lgpd-e-um-erro-22042020>. Acesso em: 22 dez. 2023.

SILVA, L. M. et al. **"Governança de dados em saúde: Um caminho necessário"**. Cadernos de Saúde Pública, 2020.

SIMITIS, S. **Rechtliche Anwendungsmöglichkeiten kybernetischer Systeme**. Mohr: Tübingen, 1966.

SOUZA, Ana Paula Loureiro de Souza. **Modelos e fontes do Direito em Miguel Reale**. In: Miguel Reale e o pensamento luso-brasileiro; Atas do IX Colóquio Tobias Barreto. Lisboa: Instituto de Filosofia Luso-Brasileiro, 2010.

TEFFÉ, Chiara Spadaccini. **A saúde na sociedade da vigilância como proteger os dados sensíveis?** Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/324485/a-saude-na-sociedade-da-vigilancia--como-proteger-os-dados-sensíveis>. Acesso em: 06 dez. 2023.

UNIÃO EUROPEIA. **Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas)**. Jornal Oficial das Comunidades Europeias. n.º L 201/37-47, 31 de julho de 2002. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_pt.pdf>. Acesso em: 27 nov. 2023.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Jornal Oficial da União Europeia, n.º L 281, 31-50, 23 de novembro de 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 28 nov. 2023.

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, nº. 119/1-88, 05 de maio de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 30 nov. 2023.

VAINZOF, Rony. **Capítulo 1 – Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). LGPD: Lei Geral de Proteção de Dados Comentada.** 2 ed. São Paulo: Thomson Reuters - Revista dos Tribunais, 2020, p. 20–177.

VENTURA, Míriam; COELI, Cláudia Medina. **Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança.** [*S. l.*], 2018. Disponível em: https://doi.org/10.1590/0102-311x00106818. Acesso em 27 de dez. 2023.

VILLELA, D. A. M., & Gomes, M. F. D. C. **O impacto da disponibilidade de dados e informação oportuna para a vigilância epidemiológica**. Cadernos de Saúde Pública, 38, e00115122. 2022. Disponível em: <https://www.scielosp.org/article/csp/2022.v38n7/e00115122/>. Acesso em: 28 dez. 2023.

MELTWATER. **We Are Social & Meltwater. Digital 2023 Global Overview Report.** Disponível em: <https://datareportal.com/reports/digital-2023-global-overview-report>. Acesso em: 21 nov. 2023.

YIN, R. K. **Estudo de caso: planejamento e métodos**. Sage, 2014.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder.** Tradução de George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2020.