



B1

ISSN: 2595-1661

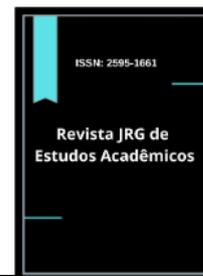
ARTIGO DE REVISÃO

Listas de conteúdos disponíveis em [Portal de Periódicos CAPES](#)

Revista JRG de Estudos Acadêmicos

Página da revista:

<https://revistajrg.com/index.php/jrg>



A proteção de dados na era digital: análise à luz da Constituição Federal Brasileira e da Lei Geral de Proteção de Dados

Data protection in the digital era: an analysis in light of the Brazilian Federal Constitution and the General Data Protection Law

DOI: 10.55892/jrg.v7i15.1537

ARK: 57118/JRG.v7i15.1537

Recebido: 28/10/2024 | Aceito: 04/11/2024 | Publicado *on-line*: 04/11/2024

Marcos Antonio Ferreira Cirqueira¹

<https://orcid.org/0000-0000-0000-0000>

<http://lattes.cnpq.br/0000000000000000>

Universidade Estadual do Tocantins, TO, Brasil

E-mail: kwartferreira@gmail.com

Paulo Beli Moura Stakoviak Júnior²

<https://orcid.org/0000-0002-2696-0152>

<http://lattes.cnpq.br/4177272982205028>

Universidade Estadual do Tocantins, TO, Brasil

E-mail: paulo.bs@unitins.br



Resumo

A evolução da tecnologia levou ao uso massivo da internet na “era digital” em que vivemos e diariamente somos bombardeados de informações de diferentes fontes. Concernente aos benefícios trazidos pela evolução digital, surgiram os desafios relacionados à proteção de dados pessoais tendo em vista que é muito difícil controlar, monitorar e gerenciar os dados na internet devido ao enorme volume que é gerado a todo momento. As informações pessoais são coletadas e exigidas a todo instante por diversas plataformas e serviços. Este presente trabalho visa abordar essa problemática da proteção de dados na era digital à luz da Constituição Federal Brasileira e da Lei Geral de Proteção de Dados Pessoais visto que o nosso ordenamento jurídico assegura o direito à intimidade e à proteção da vida privada. Os dados pessoais são sensíveis e por isso devem ser tratados com muita responsabilidade por todos envolvidos no tratamento destas informações. O estudo utilizou métodos qualitativos, com pesquisa bibliográfica em fontes jurídicas e análise em legislações pertinentes ao tema trabalhado.

Palavras chaves: Dados Pessoais. Constituição Federal. Lei Geral de Proteção de Dados Pessoais.

¹ Graduando em Direito pela Universidade Estadual do Tocantins

² Possui graduação em Direito pelo Centro Universitário Luterano de Palmas (2008) e mestrado em Constituição e Sociedade pelo Instituto Brasiliense de Direito Público (2015), Doutorando pela mesma instituição. Atualmente é professor da Universidade do Tocantins e coordenador do Curso de Direito do campus de Palmas. Tem experiência na área de Direito Imobiliário e de Direito Agrário.

Abstract

The evolution of technology has led to the massive use of the internet in the “digital age” in which we live and daily we are bombarded with information from different sources. Concerning the benefits brought by digital evolution, challenges related to the protection of personal data have arisen considering that it is very difficult to control, monitor and manage data on the internet due to the enormous volume that is generated at all times. Personal information is collected and required at all times by various platforms and services. This present work aims to address this issue of data protection in the digital era in light of the Brazilian Federal Constitution and the General Law for the Protection of Personal Data since our legal system guarantees the right to intimacy and the protection of private life. Personal data is sensitive and must therefore be treated with great responsibility by everyone involved in the processing of this information. The study used qualitative methods, with bibliographic research in legal sources and analysis of legislation relevant to the topic discussed.

Keywords: *Personal Data. Federal Constitution. General Personal Data Protection Law.*

1. Introdução

Atualmente, estamos presenciando a revolução tecnológica ou era digital, caracterizada pelo uso massivo da tecnologia digital. Muitos recursos e ferramentas passaram a funcionar no ambiente digital e conseqüentemente as pessoas precisaram se adaptar para não se tornarem obsoletas. A onipresença da tecnologia digital criou um ecossistema onde os dados são coletados, as informações pessoais são exigidas para determinadas ações e, desse modo, a privacidade e a intimidade das pessoas acabam sendo afetadas.

Neste cenário, veio à tona a questão da proteção de dados e da privacidade. A Constituição Federal Brasileira tem a privacidade consagrada como um direito fundamental e anos depois, em 2018, surgiu a Lei Geral de Proteção de Dados Pessoais com o objetivo de regulamentar a privacidade e a proteção de dados no país. Conforme vivemos cada vez mais em uma sociedade digital, a preocupação com a segurança dos dados pessoais se tornou iminente.

Este trabalho tem como objetivo realizar uma análise minuciosa sobre a proteção de dados à luz da Constituição Federal e da Lei Geral de Proteção de Dados Pessoais buscando compreender como esses dispositivos são essenciais para a segurança dos dados pessoais, como esses instrumentos legais são aplicados na prática e os desafios que os mesmos enfrentam em um cenário digital em constante evolução. Esta pesquisa busca contribuir com o conhecimento dos cidadãos acerca de um tema pouco difundido, mostrando que o mundo digital também é regido por leis que visam resguardar a segurança dos usuários.

O presente trabalho é desenvolvido sob a perspectiva qualitativa, visto que o mesmo se propõe a fazer uma análise profunda da proteção de dados pessoais na era digital, visando relacionar as questões legais com a privacidade pessoal, de modo que as pessoas tenham a compreensão que a segurança dos seus dados é resguardada por lei. As principais fontes de dados para esta pesquisa incluem: A Constituição Federal, a Lei Geral de Proteção de Dados e a revisão de artigos acadêmicos que abordam o tema, inclusive artigos do Jurista especialista em Proteção de Dados Danilo Doneda.

OBJETIVOS

Objetivo Geral

Analisar a proteção de dados pessoais na era digital sob a perspectiva da Constituição Federal Brasileira de 1988 e da Lei Geral de Proteção de Dados (LGPD), investigando como essas legislações contribuem para a garantia da privacidade e segurança de dados dos cidadãos e quais são os impactos de sua aplicação no contexto jurídico e social contemporâneo.

Objetivos Específicos

- a) Examinar a base constitucional da proteção de dados pessoais, desvendando a trajetória que levou o direito à privacidade à consagração na Emenda Constitucional 115/2022. Uma consolidação que elevou a proteção de dados ao status de direito fundamental.
- b) Descrever os alicerces da LGPD, destacando como cada princípio — finalidade, adequação, necessidade, entre outros — se integra para construir um arcabouço regulatório robusto que resguarda os direitos individuais com eficácia.
- c) Comparar minuciosamente a LGPD e o GDPR da União Europeia, destacando as semelhanças estruturais e as diferenças sutis ou marcantes nos enfoques regulatórios, refletindo em implicações práticas e legais.
- d) Analisar a aplicabilidade prática da LGPD. Desvendar casos reais de implementação, explorando os desafios enfrentados por empresas e instituições em suas tentativas de conformidade. Obstáculos que testam estratégias e adaptabilidade.
- e) Discutir as implicações sociais e jurídicas da proteção de dados em tempos digitais, onde o papel do Estado e das entidades privadas se entrelaça para manter a privacidade e garantir os direitos fundamentais. Um equilíbrio entre inovação e regulação.

JUSTIFICATIVA

A proteção de dados pessoais despontou como um tema vital em meio à avassaladora digitalização das relações humanas. No Brasil, a emergência desse debate foi propulsionada pela necessidade de equilibrar direitos fundamentais com os avanços tecnológicos acelerados. A Emenda Constitucional 115/2022 não é apenas um marco; é um divisor de águas que inscreve o direito à proteção de dados como direito fundamental. Um passo crucial para assegurar que, em um ambiente digital em contínua transformação, a privacidade não seja apenas um ideal, mas uma garantia inegociável.

A LGPD, então, ergue-se como um bastião regulatório, definindo princípios que guiam o tratamento dos dados pessoais. No entanto, sua aplicação prática não se apresenta sem desafios. Ela levanta questões espinhosas sobre como empresas e instituições podem — e devem — alinhar-se a suas exigências sem comprometer o ritmo de suas operações. Comparada ao GDPR da União Europeia, a LGPD revela tanto convergências instrutivas quanto lacunas que instigam reflexões profundas sobre eficácia e adaptabilidade regulatória.

Este estudo justifica-se por sua busca em ir além do texto da lei, em esmiuçar a prática e dissecar as implicações sociais e jurídicas desse aparato normativo. O papel que o Estado e as entidades privadas desempenham na proteção da

privacidade e no resguardo dos direitos fundamentais redefine não só as responsabilidades atuais, mas antecipa os obstáculos futuros. São questões que clamam por atenção contínua, adaptabilidade e soluções que não hesitem em inovar.

REFERENCIAL TEÓRICO

O referencial teórico que sustenta esta pesquisa se estende por um terreno denso: a proteção de dados pessoais, das bases constitucionais aos desafios da legislação contemporânea. A Constituição Federal de 1988 oferece um alicerce sólido, firmando em seu artigo 5º, X, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas”. Essa garantia foi impulsionada pela Emenda Constitucional 115/2022, que transformou a proteção de dados em um direito fundamental. Um reconhecimento que reflete a urgência de proteger a privacidade em um ambiente digital que não cessa de se expandir e metamorfosear.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é um marco divisor na regulação do uso de dados no Brasil, inspirado pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Com o propósito de assegurar que o tratamento de dados respeite a liberdade, a privacidade e o pleno desenvolvimento da personalidade, a LGPD se firmou como um escudo dos direitos individuais. Para Danilo Doneda, jurista em destaque, “a LGPD transcende o papel de legislação; ela fomenta uma cultura de proteção e respeito ao usuário”.

A LGPD se estrutura em princípios como transparência e finalidade, moldando a coleta e o tratamento de dados para que respeitem o titular de forma inegociável. Ingo Wolfgang Sarlet, figura proeminente do direito, pontua: “A inclusão da proteção de dados como direito fundamental sinaliza a valorização da privacidade em uma era de hiperconectividade e digitalização desenfreada”.

Ao confrontar a LGPD com o GDPR, surgem paralelos e dissonâncias. Ambas as legislações compartilham o objetivo de resguardar a dignidade e a autonomia pessoal. No entanto, o GDPR é celebrado por suas penalidades rigorosas e uma fiscalização incisiva, enquanto a LGPD ainda enfrenta obstáculos práticos em sua execução e supervisão. Carlos Affonso Souza, do Instituto de Tecnologia e Sociedade (ITS-Rio), sublinha: “A adaptação da LGPD à realidade brasileira revela desafios inerentes de infraestrutura e uma cultura digital que requer atenção detalhada”.

A prática de aplicar a LGPD é desafiadora. Estudos recentes indicam que muitas empresas ainda encontram barreiras significativas na adaptação de suas políticas internas e nas medidas de segurança necessárias para cumprir a lei. A Associação Brasileira de Empresas de Software (ABES) aponta que cerca de 40% das empresas relatam dificuldades expressivas em alcançar a conformidade. Essa transição requer mais do que tecnologias; é uma reconfiguração cultural e treinamento intensivo de equipes.

Segundo as palavras de Ingo Wolfgang Sarlet, “direitos fundamentais são direitos do ser humano reconhecidos e positivados na esfera do direito constitucional positivo de determinado Estado”. Ou seja, os direitos fundamentais representam o conjunto de direitos individuais e coletivos positivados na Constituição Federal.

Em 10 de fevereiro de 2022 foi promulgada a Emenda Constitucional 115/2022 que elevou a condição de Direito fundamental a proteção de dados pessoais. Em razão disso, a proteção de dados se tornou cláusula pétrea da Constituição Federal, direito fundamental do cidadão brasileiro e consequentemente

trouxe uma maior segurança jurídica em relação ao tema. O direito à proteção de dados pessoais agora está previsto no artigo 5º, inciso LXXIX, da Constituição Federal.

Um detalhe curioso, é que a Lei Geral de Proteção de Dados pessoais surgiu antes do direito à proteção de dados pessoais ser um direito fundamental positivado no texto constitucional, entretanto, o mesmo já estava implícito na Constituição Federal, visto que a mesma já tratava da liberdade de expressão, da inviolabilidade da intimidade, da vida privada da pessoa. O ponto central é que a sociedade tem se tornado cada vez mais digital e acabou surgindo a necessidade de deixar esse direito explícito.

Esse reconhecimento para o direito à proteção de dados pessoais como um direito fundamental representa, segundo as palavras de Carlos Alberto Molinaro e Gabrielle Bezerra S. Sarlet, “Um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes”.

Outro direito constitucional que tem relação com a proteção de dados é o direito à privacidade que está previsto no artigo 5º, X, da Constituição Federal de 1988 que trata sobre a inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa. É importante ressaltarmos a distinção entre direito à intimidade e direito à privacidade. O direito à privacidade refere-se a vida privada da pessoa no tocante as relações interpessoais. Já o direito à intimidade refere-se a algo muito mais intrínseco, muito mais íntimo como, por exemplo, a opção sexual da pessoa.

A Lei Geral de Proteção de Dados Pessoais tem como modelo o Regulamento Geral de Proteção de Dados, que foi concebido pela União Europeia e dispõe sobre a proteção de dados pessoais, inclusive nos meios digitais, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme exposto em seu artigo 1º, sendo promulgada em 2018 e entrado em vigor em 2020, foi considerada um marco na internet.

Antes de dar prosseguimento, é importante abordar sobre o Marco Civil da Internet e sobre a Lei Carolina Dieckmann, leis que antecederam a Lei Geral de Proteção de Dados Pessoais e já tratavam, de certa forma, sobre o tema. A Lei Carolina Dieckmann (Lei 12.737/2012) foi motivada após o vazamento de fotos íntimas da atriz Carolina Dieckmann na internet. Em 2012, esse tipo de conduta não era considerado crime e após esse acontecimento, os projetos de lei sobre esse tema voltaram à tona.

Em 2013 entrou em vigor a Lei Carolina Dieckmann e passou a criminalizar a conduta de invadir aparelhos eletrônicos com a intenção de roubar dados pessoais. Em 2014 surgiu o Marco Civil da Internet (Lei 12.965/14) com o objetivo de tornar a internet, que antes era um ambiente sem lei, em um ambiente onde o Estado é capaz de regulamentar os direitos e deveres. Em resumo, a lei colocava o usuário da internet como protagonista, visando proteger seus dados e sua privacidade, além de regular o que poderia ser disponibilizado ou retirado do mundo on-line.

O problema do Marco Civil da Internet é que o mesmo só prevê a proteção de dados no âmbito on-line, problema este resolvido pela Lei Geral de Proteção de Dados Pessoais.

A expressão “tratamento de dados pessoais” pode ser de difícil compreensão, por isso, abordaremos este conceito segundo a própria Lei Geral de Proteção de Dados Pessoais. Dados pessoais são as informações relacionadas a pessoa natural identificada ou identificável. A informação pode constar tanto em meio físico quanto em meio digital desde que se consiga identificar o detentor do

dado. A palavra “tratamento” na expressão acima citada se refere a toda e qualquer operação realizada com os dados pessoais como, por exemplo, a coleta, a produção, a transmissão, etc.

Os dez princípios em que a Lei Geral de Proteção de Dados Pessoais está pautada são: Finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não Discriminação e responsabilização.

O princípio da finalidade diz que os dados só podem ser coletados e trabalhados se for para propósitos legítimos, específicos, explícitos e informados ao titular dos dados. Não podendo esses dados serem utilizados posteriormente de maneira incompatível com a finalidade que foi exposta para o titular dos dados.

O segundo princípio é o da adequação e diz que o uso dos dados precisa ser compatível com as finalidades informadas ao titular. Ou seja, deve haver um nexo lógico. A coleta e o tratamento de dados deve ser condizente com o modelo de negócio da empresa que solicitou os dados, sob pena de punições e multa. Resumidamente, o pedido de dados solicitado deve fazer sentido e deve existir uma relação lógica entre o tratamento e a finalidade objetivada, o tratamento e a comunicação transmitida ao titular e entre a finalidade almejada e a comunicação transmitida ao titular.

O terceiro princípio é o princípio da necessidade e diz que os dados só podem ser solicitados se realmente for necessário. Ou seja, aqui é levado em conta o aspecto da responsabilidade das empresas com os dados. O objetivo e a finalidade devem ser colocados em pauta, pois quanto maior o número de dados coletados, mais difícil se torna o controle e tratamento destes dados. O princípio da necessidade aborda um aspecto de prender-se ao necessário e eliminar os excessos.

O quarto princípio é o livre acesso. As pessoas precisam ter acesso e saber quais dados delas foram coletados. Por exemplo, determinada empresa coletou os dados de uma pessoa, é necessário existir um ambiente aonde a pessoa possa acessar esses dados. Além disso, as pessoas precisam ser informadas de quanto tempo os seus dados serão utilizados para atingir a finalidade almejada pela empresa que os coletou.

O quinto princípio é a qualidade dos dados, o titular dos dados precisar ter o direito de completar, atualizar ou excluir dados, de modo que os dados do mesmo sempre tenham qualidade. Dependendo do contexto, o titular dos dados também pode pedir o anonimato dos seus dados, de maneira que não seja possível identificar o titular do mesmo. O titular dos dados também precisa ter acesso a qualquer momento aos termos de uso ou políticas de privacidade, o mesmo também pode, a qualquer momento, revogar a confirmação que ele deu aos termos de uso ou políticas de privacidade.

O sexto princípio é a transparência que expressa que o titular dos dados tem o direito de ser informado quais dados estão sendo coletados, ele também precisa ser informado caso ocorra algum risco de exposição desses dados. Quanto ao direito de ser informado, esse princípio nos ensina que as informações devem ser disponibilizadas de maneira clara, precisa e facilmente acessível. O princípio da transparência tem relação com a honestidade. As empresas precisam ser honestas com os titulares dos dados sobre questões pertinentes sobre o tratamento e o uso desses dados.

O sétimo princípio é o da segurança que diz que os dados pessoais devem ser tratados de uma forma que resguarde a segurança e a confidencialidade dos

mesmos. Inclusive esses dados não podem ser utilizados por pessoas não autorizadas. Nesse ponto crucial, são utilizadas técnicas e procedimentos de segurança e estes devem ser aprimorados de maneira constante visando resguardar um ambiente seguro e efetivo contra ameaças para os dados coletados.

O oitavo princípio é a prevenção que diz respeito as medidas de prevenção no tratamento dos dados pessoais. É o conjunto de princípios internos nos quais as pessoas ou empresas que estão coletando esses dados instituem de forma a garantir a segurança e a confidencialidade. Esse princípio acaba sendo uma complementação ao sétimo princípio, todavia o legislador resolveu destacá-lo em virtude da sua importância.

O nono princípio é o da não discriminação que basicamente trata sobre a forma com que os dados são utilizados. Ou seja, os dados não podem ser utilizados para discriminar o titular dos mesmos. Dados relacionados a orientação sexual, partidária, entre outros, são chamados de dados sensíveis e devem ser tratados com muito cuidado, visto que a discriminação configura crime e até mesmo o vazamento desses dados pode acarretar em prejuízos na vida do titular. Segundo a LGPD, este princípio diz respeito à “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”.

O décimo e último princípio é o da responsabilização e diz respeito a prestação de contas no qual quem coleta os dados deve prestar contas aos titulares e as autoridades com o objetivo de demonstrar a eficácia das medidas adotadas. É importante destacar que não basta somente a comprovação dos procedimentos adotados. Pelo contrário, é necessário demonstrar por meio que evidências a eficácia dos procedimentos adotados.

Um dos principais pontos de destaque da Lei Geral de Proteção de Dados Pessoais é ter o usuário como protagonista. Em resumo, no momento da coleta dos dados pessoais do usuário este deve consentir com a coleta, ao passo que quem estiver coletando os dados deve informar ao usuário qual será a finalidade do uso dos dados do mesmo. Se isso não for feito, a conduta poderá incorrer em penalidade como, por exemplo, uma multa. O usuário, também, sempre deve ter a possibilidade de suspender o uso dos seus dados quando julgar necessário. Pode se ter como exemplo as redes sociais. O usuário sempre terá a possibilidade de excluir a sua conta e os seus dados gerados até o momento da exclusão.

O papel do Estado e das entidades privadas na proteção da privacidade não pode ser subestimado. Entidades privadas devem adotar políticas de compliance rigorosas e salvaguardas de segurança para proteger os dados dos usuários, enquanto cabe ao Estado fiscalizar e assegurar a aplicação justa das normas. Gabriela S. Sarlet, especialista em direito digital, enfatiza: “A responsabilidade compartilhada é a chave para um sistema de proteção eficiente, equilibrando o avanço tecnológico com os direitos fundamentais dos indivíduos”.

Portanto, o referencial teórico traçado vai além de uma simples análise normativa. Ele explora as implicações práticas e sociais da proteção de dados, mostrando que uma abordagem que inclua tanto a base normativa quanto os desafios de sua implementação prática é essencial em um mundo digital em constante transformação.

METODOLOGIA

Esta pesquisa envereda pelo caminho da abordagem qualitativa, um caminho que se propõe a mergulhar nas entrelinhas da proteção de dados pessoais no Brasil, sob o olhar atento da prática e da teoria legal. Não se trata apenas de entender o que está na letra da lei, mas de captar como essa letra vive, respira e se transforma no dia a dia jurídico e social. É essa profundidade que motiva a escolha pelo método qualitativo: explorar além da superfície, desvendar nuances, ouvir ecos entre os artigos e as realidades que eles tentam alcançar.

Método de Pesquisa: A metodologia aqui é rigorosa, quase artesanal. Uma análise documental que se debruça sobre fontes primárias — a Constituição Federal de 1988 e a Lei nº 13.709/2018 (LGPD) são pilares inegociáveis. A Emenda Constitucional 115/2022 é outro alicerce, dando contornos robustos a essa fundação. A revisão bibliográfica, por sua vez, amplia o campo, trazendo à luz vozes de especialistas em direito digital, artigos acadêmicos e relatórios de instituições respeitadas. Um trabalho que costura tradição e inovação em busca de clareza.

Crítérios de Seleção de Fontes: A escolha das fontes é uma tarefa meticulosa. Relevância e credibilidade são os filtros que norteiam esse processo. Cada documento, seja um estudo de caso ou uma análise comparativa com legislações como o GDPR europeu, é selecionado por sua capacidade de iluminar as complexidades do tema. Esse garimpo visa trazer à tona não apenas informações, mas insights que dialoguem com as realidades sociais, econômicas e jurídicas da proteção de dados.

Procedimentos de Coleta de Dados: Coletar dados foi um exercício de imersão. A análise de textos legais se entrelaça com leituras de artigos e publicações especializadas, uma tentativa de compor um mosaico rico e detalhado. Os estudos de caso complementam essa investigação, oferecendo exemplos palpáveis de como a LGPD se manifesta em práticas corporativas e institucionais. A realidade ganha forma, e a teoria se reflete nela, num jogo de espelhos revelador.

Procedimentos de Análise: A análise foi desenhada como um processo interpretativo. Cada dado coletado é categorizado, confrontado, despido de superficialidade para que padrões, semelhanças e dissensos possam emergir. O resultado? Um panorama que funde teoria e prática, uma narrativa que evidencia não apenas os avanços, mas os obstáculos que a implementação da LGPD enfrenta em um cenário digital pulsante e desafiante.

Limitações da Pesquisa: Toda pesquisa tem suas margens. Esta não é exceção. Restrita à análise documental e ao exame de estudos de caso já existentes, a investigação pode não capturar todas as facetas da aplicação da LGPD em nichos específicos. Ainda assim, a abordagem qualitativa confere uma amplitude e uma profundidade que revelam as camadas essenciais do tema, mostrando-se suficientemente robusta para uma compreensão abrangente.

Justificativa da Metodologia: Escolher o qualitativo é optar por um mergulho mais profundo. É ter a coragem de explorar complexidades e encarar os desafios da proteção de dados com um olhar crítico. Mais que decifrar o texto da lei, é decodificar suas implicações sociais e práticas. Em um mundo onde o digital não apenas avança, mas redefine, essa análise se faz não apenas relevante, mas urgente.

CONCLUSÃO

A conclusão desta pesquisa destaca algo crucial: entender a proteção de dados pessoais exige olhar por diferentes lentes — legal, prática e social. No Brasil, onde a tecnologia avança a passos largos e quase atropela, a LGPD não é só uma lei. É um alerta da necessidade de adaptação.

Este estudo mostrou que a junção da Constituição de 1988 com a Emenda Constitucional 115/2022 elevou a proteção de dados a um novo patamar, tornando a privacidade um bastião da dignidade humana. Mas a criação de regulamentação não é, por si só, suficiente, se não vier acompanhada de uma estrutura de fiscalização que torne efetivas as determinações previstas em lei.

Não é simples. A implementação acompanha muitos desafios. Empresas ainda penam para ajustar suas rotinas e se alinhar à LGPD. Falta preparo, falta estrutura, falta recurso. É uma jornada que requer investimentos em tecnologia, no treinamento para qualificar os funcionários e na contratação de especialistas no assunto.

O Estado, por sua vez, não pode ficar só assistindo de longe. Precisa ser protagonista, fiscalizar, orientar, garantir que a proteção de dados saia do papel e vire parte do dia a dia. Isso se coaduna com a necessidade da implementação de políticas públicas que visem a implementação de mecanismos que proporcionem uma maior segurança para os dados do titular, ao passo que campanhas de conscientização devem ser implantadas para informar as pessoas sobre os direitos que possuem a cerca desta temática.

A comparação com o GDPR europeu trouxe à tona algumas lições importantes. Ambas as leis visam proteger a dignidade e a liberdade das pessoas, mas, quando chega na hora de agir, as diferenças aparecem. Cada país tem suas próprias bagagens culturais e econômicas, e isso reflete em como as leis ganham força e efetividade. A LGPD, mesmo vindo de fonte europeia, precisa traçar seu próprio caminho, respeitando as peculiaridades do Brasil.

Proteger dados vai além de palavras frias em um documento. É como proteger um tesouro que, ao mesmo tempo, é a uma grande vulnerabilidade. E nesse equilíbrio, empresas, cidadãos e o Estado tentam estar em harmonia, buscando inovar sem perder a segurança, crescer sem deixar a ética para trás. Esta pesquisa mostrou que, sim, o Brasil tem avançado. Mas a estrada para a maturidade em proteção de dados ainda é longa, sinuosa e cheia de desafios.

Em resumo, o debate sobre a proteção de dados não pode parar. Precisa se alimentar de novas tecnologias, de práticas que façam sentido e tragam mais eficiência. O futuro pede mais do que normas escritas; ele exige um compromisso constante com a educação, a clareza e a responsabilidade de todos os envolvidos. Só assim, a privacidade e a proteção de dados vão deixar de ser só um direito escrito e se tornar parte viva de uma sociedade que se pretende moderna, justa e, acima de tudo, humana.

REFERÊNCIAS

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 02/11/2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 02/11/2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02/11/2024

DONEDA, Danilo. **Proteção de dados pessoais**: fundamentos e princípios. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/anexos/29536-29552-1-PB.pdf>. Acesso em: 02/11/2024.

SARLET, Ingo Wolfgang. **Direitos fundamentais na Constituição Federal de 1988**. Rio de Janeiro.

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra S. **A evolução do direito à proteção de dados pessoais e seu impacto na dignidade humana**.

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 30/10/2024.