FACULDADE ARI DE SÁ
CURSO DE DIREITO

ALEF SARAIVA DA CUNHA

A EVOLUÇÃO LEGISLATIVA NA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA

FORTALEZA
2023

ALEF SARAIVA DA CUNHA

A EVOLUÇÃO LEGISLATIVA NA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA

Projeto de Pesquisa apresentado ao Curso de Direito da Faculdade Ari de Sá, como requisito parcial da disciplina de Trabalho de Conclusão de Curso I.

Orientador: Prof. Me. Eugênio Ximenes

FORTALEZA

2023

Dados Internacionais de Catalogação na Publicação
Faculdade Ari de Sá
Gerada automaticamente mediante os dados fornecidos pelo(a) autor(a)

D111a da Cunha, Alef Saraiva .

A EVOLUÇÃO LEGISLATIVA NA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA / Alef Saraiva da Cunha. – 2023.

34 f.

Trabalho de Conclusão de Curso – Faculdade Ari de Sá, Curso de Direito, Fortaleza, 2023.

Orientação: Prof. Me. Eugênio Ximenes.

1. Proteção de dados. 2. Privacidade. 3. Lei Geral de Proteção de Dados. 4. Regulamento Geral de Proteção de Dados. 5. Direitos Digitais. I. Título.

CDD 340

ALEF SARAIVA DA CUNHA

A EVOLUÇÃO LEGISLATIVA NA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Direito da Faculdade Ari de Sá.

Orientador: Prof. Me. Eugênio Ximenes

Aprovada em: ___/___/___

BANCA EXAMINADORA

_____
Prof. Me. Eugênio Ximenes
Faculdade Ari de Sá

_____
Prof. Me./Dr. Marlene Pinheiro
Faculdade Ari de Sá

_____
Prof. Me. Roberta Brandão

Dedico este trabalho à minha amada família,
cuja compreensão e apoio foram fundamentais
nos momentos em que estive ausente.

AGRADECIMENTOS

Agradeço primeiramente a Deus, cuja mão esteve presente em cada etapa deste percurso. Como disse o salmista no versículo 118 da Bíblia Sagrada, “Foi o SENHOR que fez isto, e é coisa maravilhosa aos nossos olhos.” Sua orientação e bênçãos foram fundamentais.

À minha família, o alicerce inabalável que sustentou meus sonhos. Ao meu pai, Reginaldo, e minha mãe, Elane, cujo amor e apoio foram meu suporte incondicional. Aos meus irmãos, Gabriel e Lucas, por serem fonte de inspiração e encorajamento em todos os momentos.

E a minha querida noiva e agora esposa, Bianca, cujo amor, compreensão e paciência foram a âncora que me ajudou a atravessar tempos desafiadores. Sua presença foi minha motivação para alcançar cada objetivo.

Obrigado a todos por fazerem parte desta jornada e por serem os pilares que tornaram possível a realização deste trabalho.

As coisas têm muitos jeitos de ser,
Depende de o jeito da gente ver...
O comprido pode ser curto.
E o pouco pode ser muito.
O quente pode ser frio,
E o que parece um mar,
Também pode ser um rio.
(Jandira Mansur, 2015)

RESUMO

O estudo analisa a evolução legislativa na proteção de dados pessoais no Brasil e na União Europeia, destacando a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre a Proteção de Dados (RGPD ou GDPR), respectivamente. A proteção de dados tem emergido como tema central no debate sobre privacidade e direitos na era digital. O objetivo geral desse trabalho foi realizar análise comparativa entre as legislações de proteção de dados no Brasil e na UE, visando compreender convergências e divergências no desenvolvimento e implementação das normativas. A metodologia utilizada foi uma pesquisa bibliográfica com abordagem qualitativa e objetivo descritivo. Foram analisadas 15 referências teóricas publicadas nos últimos 5 anos, predominantemente artigos científicos. A busca focou nas bases Scielo, DOAJ e BDTD. Utilizou-se análise temática em 3 eixos: fundamentos das leis, comparação entre diplomas legais e aspectos críticos na aplicação. Os resultados observados, tanto LGPD quanto GDPR avançaram na garantia de privacidade e autodeterminação informacional, embora persistam assimetrias importante entre os contextos brasileiro e europeu. O estudo revela que as leis compartilham princípios, mas divergem em rigor das sanções administrativas e no grau de institucionalização dos órgãos de proteção de dados. Conclui-se que a efetividade da LGPD ainda requer aprofundamento. Novos estudos poderiam investigar desafios e impactos da lei brasileira, além da interconexão entre ordenamentos jurídicos nesta área essencial do direito digital.

Palavras-chave: Proteção de dados. Privacidade. Lei Geral de Proteção de Dados. Regulamento Geral sobre a Proteção de Dados. Direitos digitais.

ABSTRACT

The study analyzes legislative developments in the protection of personal data in Brazil and the European Union, highlighting the General Data Protection Law (LGPD) and the General Data Protection Regulation (GDPR or GDPR), respectively. Data protection has emerged as a central topic in the debate on privacy and rights in the digital age. The general objective of this work was to carry out a comparative analysis between data protection legislation in Brazil and the EU, aiming to understand convergences and divergences in the development and implementation of regulations. The methodology used was a bibliographical research with a qualitative approach and descriptive objective. 15 theoretical references published in the last 5 years were analyzed, predominantly scientific articles. The search focused on the Scielo, DOAJ and BDTD databases. Thematic analysis was used in 3 axes: foundations of laws, comparison between legal diplomas and critical aspects in application. The results observed, both LGPD and GDPR made progress in guaranteeing privacy and informational self-determination, although important asymmetries persist between the Brazilian and European contexts. The study reveals that the laws share principles, but differ in the severity of administrative sanctions and the degree of institutionalization of data protection bodies. It is concluded that the effectiveness of the LGPD still requires further investigation. New studies could investigate challenges and impacts of Brazilian law, in addition to the interconnection between legal systems in this essential area of digital law.

Keywords: Data protection. Privacy. General Data Protection Law. General Data Protection Regulation. Digital rights.

SUMÁRIO

1 INTRODUÇÃO

A proteção de dados pessoais é uma questão cada vez mais importante no mundo contemporâneo, à medida que a tecnologia avança e a coleta, armazenamento e uso de informações pessoais se tornam cada vez mais comuns em todos os setores da sociedade. A proteção de dados pessoais no Brasil passou por um importante processo de evolução legislativa nos últimos anos. Esse movimento foi principalmente impulsionado pelo crescimento da economia digital e a crescente preocupação com a privacidade e a segurança dos dados pessoais.

Desta forma, a proteção de dados pessoais tem emergido como um tema central nas discussões sobre privacidade e direitos digitais, tanto no Brasil quanto na União Europeia. A evolução legislativa nesta área reflete uma crescente preocupação com a segurança da informação e a privacidade dos indivíduos em um mundo cada vez mais conectado. No cenário europeu, a introdução do Regulamento Geral sobre a Proteção de Dados (GDPR) marcou um ponto de inflexão na abordagem regulatória, estabelecendo um padrão global e influenciando legislações ao redor do mundo (KUNER, 2014). O GDPR é reconhecido por sua abrangência e rigor, impondo obrigações significativas às organizações e conferindo direitos extensos aos titulares dos dados (SCHWARTZ; PEIFER, 2017).

Paralelamente, o Brasil seguiu um caminho semelhante com a sanção da Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020. A LGPD representa um marco na legislação brasileira, introduzindo conceitos e mecanismos para assegurar a proteção de dados pessoais e estabelecendo penalidades para o seu descumprimento (DONEDA, 2020). O diálogo entre as legislações da UE e do Brasil revela não apenas convergências, mas também divergências que são reflexo de diferentes contextos sociais, econômicos e culturais (SANTOS, 2021).

A análise da evolução legislativa na proteção de dados, portanto, não se limita ao exame do conteúdo normativo, mas também engloba o entendimento das forças sociais, políticas e econômicas que moldam essa legislação. A presente pesquisa visa aprofundar o conhecimento sobre como essas legislações evoluíram, suas inter-relações e o impacto dessas normas na sociedade, no meio acadêmico e no ambiente profissional.

Na União Europeia, a evolução legislativa em proteção de dados teve início com a Diretiva de Proteção de Dados de 1995, que foi substituída pelo GDPR em 2016 (REDING, 2015). Esta transição refletiu a necessidade de atualizar a legislação para enfrentar os desafios

do avanço tecnológico. No Brasil, antes da LGPD, a proteção de dados pessoais era fragmentada em várias normas setoriais, sem um corpo legislativo unificado (Miranda, 2019). A criação da LGPD foi influenciada tanto pela necessidade interna de proteção como pela pressão externa para adequação a padrões internacionais, como o GDPR (LIMA, 2020).

Desta forma, a principal legislação nesse âmbito é a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018. A LGPD é uma lei abrangente que estabelece regras claras sobre o processamento de dados pessoais no Brasil, tanto por entidades privadas quanto públicas. A lei também define direitos para os titulares de dados, estabelece obrigações para os processadores de dados, e cria a Autoridade Nacional de Proteção de Dados (ANPD) para fiscalizar o cumprimento da lei.

A LGPD é considerada um marco na legislação brasileira sobre proteção de dados pessoais, pois é a primeira lei do país a fornecer um quadro legal abrangente para a proteção da privacidade e dos dados pessoais. Antes da LGPD, a proteção de dados pessoais era tratada de maneira fragmentada em várias leis e regulamentos, sem uma abordagem coerente e abrangente.

Sendo assim, a LGPD segue os princípios de outras leis semelhantes ao redor do mundo, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. A lei reflete um esforço global para estabelecer padrões de privacidade e proteção de dados que são adequados para a era digital.

É importante notar que a evolução legislativa na proteção de dados pessoais no Brasil ainda está em andamento. A LGPD está em plena vigência, mas muitos aspectos de sua implementação ainda estão sendo discutidos e definidos. Além disso, o Brasil ainda está trabalhando para garantir a conformidade com os padrões internacionais de proteção de dados e para estabelecer mecanismos eficazes de fiscalização e aplicação da lei.

A LGPD foi fruto de um longo processo de discussão e elaboração, que envolveu diversos atores sociais, incluindo parlamentares, especialistas em tecnologia e privacidade, organizações da sociedade civil e representantes do setor empresarial. Desde a sua aprovação, a lei tem sido objeto de intensos debates e análises, tanto sobre a sua adequação às necessidades do país quanto sobre os desafios e oportunidades para a sua implementação.

No entanto, a LGPD é uma lei recente e ainda não há consenso sobre a sua aplicação e eficácia na proteção dos dados pessoais. Além disso, os desafios para a implementação da lei são muitos, como a necessidade de adaptação das empresas e instituições aos novos requisitos, a definição de papéis e responsabilidades dos agentes

envolvidos no tratamento de dados e a criação de mecanismos efetivos de fiscalização e punição.

A LGPD representou uma evolução significativa ao estabelecer um marco legal abrangente para a proteção de dados no Brasil. Entretanto, no que concerne à aplicação concreta da lei, dois aspectos relevantes deverão ser mencionados merecendo maior detalhamento.

O primeiro ponto diz respeito à efetiva adequação de empresas e organizações do setor público e privado aos novos requisitos e obrigações instituídos pela LGPD. Conforme analisam Pinheiro e Sá (2021), a legislação introduce um extenso rol de princípios, diretrizes, responsabilidades e mecanismos de governança relativos ao tratamento de dados pessoais.

Portanto, a conformidade demande iniciativas amplas de mapeamento de dados, revisão de contratos, treinamento de colaboradores, reforço na segurança da informação e comunicação transparente junto a titulares sobre políticas de privacidade. Essas medidas exigem investimentos substanciais em políticas, processos e tecnologias pelas instituições.

O despreparo de grande parte das organizações tanto públicas quanto privadas frente às demandas da LGPD suscita questionamentos sobre a efetiva absorção das mudanças. Conforme pesquisa recente do Instituto DataPrivacy Brasil, menos de um terço das empresas percebem-se completamente adequadas à nova legislação mesmo após 3 anos de sua vigência.

O segundo aspecto diz respeito ao escopo das penalidades e à fiscalização do cumprimento da lei pela recém criada Autoridade Nacional de Proteção de Dados (ANPD). Embora sejam previstas sanções administrativas significativas, que incluem multas de até 2% do faturamento, a atuação da ANPD ainda é incipiente e focada principalmente em orientação e conscientização (MANCUSO; PEREIRA, 2022).

A maior parte das reclamações recebidas ainda não resultou em abertura de procedimentos sancionadores ou aplicação efetiva de punições. A concretização dos objetivos da LGPD parece demandar aprimoramento progressivo dos mecanismos de fiscalização e enforcement disponíveis no país (PINHEIRO; SÁ, 2021).

Portanto, os dois pontos levantados apontam para importantes desafios que ainda precisam ser enfrentados para que os princípios e diretrizes da Lei Geral de Proteção de Dados sejam de fato internalizados pela cultura organizacional brasileira e a plena garantia de direitos seja alcançada na prática.

Diante desse cenário surge a seguinte pergunta-problema dessa pesquisa: Como a legislação de proteção de dados pessoais evoluiu no Brasil e na União Europeia, e quais são as principais semelhanças e diferenças entre a LGPD e o GDPR?

Como hipótese central deste estudo é que, apesar de terem sido desenvolvidas em contextos distintos, tanto a LGPD quanto o GDPR compartilham princípios fundamentais de proteção de dados pessoais, mas diferem significativamente em aspectos relacionados à aplicabilidade, alcance e sanções.

Este trabalho justifica-se pela relevância da proteção de dados na atualidade, podendo contribuir para o entendimento de como normativas distintas podem convergir para a proteção de direitos fundamentais. No aspecto social, uma maior compreensão da legislação de proteção de dados pode capacitar indivíduos a resguardar sua privacidade. Academicamente, a pesquisa contribui para o debate jurídico sobre harmonização legislativa internacional. Profissionalmente, o estudo pode auxiliar empresas a se adequarem às regulamentações e a implementarem práticas de governança de dados mais eficazes, o que é essencial em um ambiente de negócios globalizado onde a confiança do consumidor é um ativo valioso. Ademais, a análise comparativa entre o GDPR e a LGPD pode fornecer insights para a elaboração e aprimoramento de políticas públicas e estratégias corporativas em proteção de dados.

A pesquisa contribuirá para a compreensão da evolução da legislação brasileira de proteção de dados pessoais, bem como das perspectivas dos parlamentares sobre a LGPD. Além disso, espera-se que os resultados da pesquisa possam contribuir para aprimorar a implementação da lei, identificando os principais desafios e oportunidades, e para o desenvolvimento de políticas públicas mais eficazes para a proteção de dados pessoais no país.

O objetivo geral da pesquisa é realizar uma análise comparativa entre as legislações de proteção de dados pessoais no Brasil e na União Europeia através de uma revisão bibliográfica criteriosa, com o intuito de compreender as convergências e divergências no desenvolvimento legislativo e na implementação das normativas de privacidade e proteção de dados pessoais em ambas as jurisdições.

Os objetivos específicos da pesquisa são: a) Abordar definições conceituais e objetivos da Lei Geral de Proteção de Dados (LGPD). b) Analisar e comparar a evolução histórica da legislação de proteção de dados pessoais no Brasil e na União Europeia, destacando as transformações significativas desde a promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil e a evolução correspondente das leis e regulamentos na União Europeia. c) Investigar os princípios fundamentais de proteção de dados pessoais estabelecidos pela LGPD e pelo GDPR, examinando como cada legislação aborda direitos dos titulares, deveres dos controladores e processadores, além das bases legais para o tratamento

de dados pessoais.

O presente estudo consiste em uma pesquisa bibliográfica, com abordagem qualitativa e objetivo descritivo. Foi realizada por meio de levantamento, seleção e análise de referências teóricas já publicadas, predominantemente na forma de artigos científicos, mas também incluindo livros, teses e dissertações (FONSECA, 2002).

A busca foi conduzida nas seguintes bases de dados: Scientific Electronic Library Online (SciELO), Directory of Open Access Journals (DOAJ), Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), utilizando combinações de palavras-chave como "proteção de dados", "privacidade", "Lei Geral de Proteção de Dados", "General Data Protection Regulation".

Foram priorizados textos publicados nos últimos cinco anos, em Português, Inglês ou Espanhol. A amostra final foi composta por 15 referências, submetidas a fichamento para organização das informações-chave e posterior discussão integrada dos resultados à luz do referencial teórico levantado.

A análise foi realizada de forma temática, categorizando os dados em torno de três eixos centrais: (a) fundamentos e princípios das legislações, (b) comparação entre os diplomas legais brasileiro e europeu, (c) aspectos críticos e lacunas na aplicação das leis de proteção de dados.

2 REFERENCIAL TEÓRICO

2.1 Lei Geral de Proteção de Dados (LGPD): Definições Conceituais

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16º do Marco Civil da Internet.

A LGPD foi inspirada na General Data Protection Regulation (GDPR), que é a regulamentação europeia para proteção de dados pessoais. As duas leis têm objetivos similares, que é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A evolução da legislação revelou um desafio significativo nas regulamentações anteriores à Lei nº 13.709/2018, qual seja, a falta de clareza na terminologia empregada para designar assuntos relativos ao tratamento de dados pessoais, especialmente quando examinados por uma lente técnica.

Segundo Teixeira e Magro (2020), os principais fundamentos jurídicos para a proteção de dados são a Constituição Federal (1988), a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet e o Código de Defesa do Consumidor.

Os autores Teixeira e Magro (2020) destacam que a Constituição Federal de 1988 foi um marco na proteção de dados no Brasil, pois é o documento legal que instituiu e reforçou a importância da privacidade e da intimidade como direitos fundamentais dos cidadãos brasileiros. Esses princípios são basilares para o estabelecimento das leis subsequentes que visam a proteção de dados pessoais, sendo a LGPD uma delas, que ampliou e detalhou de forma mais específica os direitos dos titulares de dados e as obrigações das organizações que lidam com esses dados.

A Lei Geral de Proteção de Dados (LGPD), por sua vez, é uma lei bastante abrangente que regula o tratamento de dados pessoais no Brasil, independentemente de o tratamento ser feito por pessoa física ou jurídica, de direito público ou privado, e independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados. Além da LGPD, o Marco Civil da Internet também tem papel importante, pois estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, inclusive com relação ao tratamento de dados pessoais. O Código de Defesa do Consumidor, por sua vez, embora não trate especificamente de dados pessoais, também contribui para a proteção de dados ao estabelecer normas de proteção e defesa do consumidor, inclusive quanto a práticas comerciais, como a publicidade e a privacidade do consumidor (SANTOS, 2021).

Nas leis anteriores, termos como "tratamento de dados", "consentimento" e "dados sensíveis" eram frequentemente usados de maneira imprecisa ou ambígua, o que levava a interpretações variadas e potencialmente prejudiciais. Por exemplo, a falta de uma definição clara de "tratamento de dados" poderia levar a confusões sobre quais atividades exatamente estavam sujeitas à regulamentação. Da mesma forma, a ausência de uma definição rigorosa de "consentimento" poderia resultar em práticas questionáveis, como a obtenção de consentimento por meios enganosos ou coercitivos (SANTOS, 2021).

Com a Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD), houve uma maior clareza e precisão no uso desses termos. A LGPD fornece definições detalhadas e explícitas para uma ampla gama de conceitos relacionados à proteção de dados pessoais. Isso ajudou a evitar mal-entendidos e a garantir que todas as partes envolvidas - desde os titulares dos dados até os controladores e operadores de dados - entendam claramente suas obrigações e direitos. Isso também facilitou a implementação da lei, pois os reguladores e as empresas agora têm uma estrutura conceitual clara e detalhada.

Um exemplo de aplicação da LGPD no contexto brasileiro, foi o caso de uma startup de tecnologia com sede no Brasil coleta e armazena informações pessoais de seus usuários, como nome, e-mail, idade e gênero. Ao solicitar o cadastro na plataforma, os termos de uso da empresa requerem que o usuário concorde com diversas finalidades de tratamento de dados vagas e indefinidas (PINHEIRO, 2021).

Após um incidente de segurança que resultou no vazamento das informações de milhares de clientes, a Autoridade Nacional de Proteção de Dados (ANPD) iniciou um procedimento administrativo para investigar possíveis infrações da startup à Lei Geral de Proteção de Dados.

De acordo com Branco (2022) este caso ilustra a aplicação prática de importantes disposições e princípios da LGPD, em especial: consentimento, transparência, segurança e accountability. Primeiramente, o consentimento coletado pela startup não respeitou as exigências legais de ser livre, informado e inequívoco (art. 7o, LGPD). Os propósitos do tratamento precisam ser comunicados previamente ao titular de modo claro e acessível.

Além disso, houve falha no dever de transparência (art. 6o, VI), já que os termos de uso não detalharam as finalidades específicas para as quais cada tipo de dado seria empregado. Quanto à segurança, a startup descumpriu a obrigação legal de utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 46, caput) (PINHEIRO, 2021).

Por fim, o vazamento expõe ausência de um programa de governança em privacidade que permita a empresa demonstrar a adoção de medidas eficazes para atestar a observância e o cumprimento das normas de proteção de dados, conforme preconiza o accountability (art. 50, caput).

Esse caso sintetiza como falhas nos pilares do consentimento, transparência, segurança e responsabilização podem sujeitar organizações a sanções previstas na LGPD, que incluem desde uma advertência e determinação de exclusão dos dados até multa de 2% do faturamento, podendo chegar a R$ 50 milhões (PINHEIRO, 2021).

Segundo Pinheiro (2016), é fundamental estabelecer uma conceituação clara da terminologia técnica empregada no tratamento de dados pessoais para aumentar a segurança tanto do titular quanto do responsável pelo tratamento.

> Não obstante a falta de um marco legal específico, o Judiciário já se manifestou sobre a questão, adotando uma abordagem casuística sempre que houver questionamento quanto à utilização de dados de cidadãos brasileiros.

> No entanto, uma ambiguidade conceitual significativa surge quando se examina o assunto de uma perspectiva mais técnica. A implementação de uma determinada legislação contribuiria significativamente para garantir maior segurança tanto para o mercado quanto para a população. (PINHEIRO, 2016, p. 485).

O Artigo 5 da Lei Geral de Proteção de Dados Pessoais fornece um conjunto abrangente de conceituações e definições destinadas a melhorar a compreensão técnica e facilitar a implementação da lei. As definições, apresentadas nos itens I a XIX, servem para esclarecer os principais termos e conceitos relevantes à proteção de dados pessoais. A disposição estatutária da Lei 13.709/2018 está disposta no artigo 5º, conforme segue alguns dos incisos do I até o V: (BRASIL, 2018).

> Art. 5º Para os fins desta Lei, considera-se:
> I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - Dado pessoal sensível: 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 a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Segundo o argumento de Pinheiro (2018), é fundamental que a lei defina claramente os termos técnicos. A definição precisa da terminologia empregada no domínio dos dados pessoais é de suma importância, uma vez que se esforça para abordar as questões de conceituação e classificação que as informações coletadas encontraram. A LGPD fornece clareza e identificação em relação aos dados pessoais e todos os processos, técnicas ou procedimentos associados ao processamento de dados.

2.2 A evolução das leis e regulamentos de proteção de dados na União Europeia.

Krieger (2019) destaca, que a década de 1980 marca um período de ampla conscientização e ação política na União Europeia em relação à proteção de dados pessoais. Antes desta época, embora houvesse regulamentações pré-existentes, a abordagem era muito mais fragmentada e menos estruturada. Entretanto, a rápida evolução das tecnologias de informação e a expansão da economia digital começaram a levantar questões sérias sobre privacidade e proteção de dados.

Como resultado, os países membros da União Europeia passaram a reconhecer a necessidade de uma abordagem mais abrangente e unificada para lidar com os desafios emergentes na área de proteção de dados. Isso levou à criação de políticas mais robustas e à intensificação dos esforços para garantir que os direitos de privacidade dos cidadãos fossem adequadamente protegidos no novo ambiente digital.

A regulamentação da Convenção 108 está sob a alçada do Conselho Europeu, que estabeleceu a conexão inicial entre os dados pessoais e a transferência transnacional desimpedida de informações (KRIEGER, 2019).

A referida Convenção exerce influência significativa sobre a Diretiva Europeia sobre Dados Pessoais (95/96 CE). O modelo europeu é organizado por meio dessa diretriz, que, conforme observado por Doneda (2006), engloba uma disciplina abrangente e intrincada que é implementada nas leis internas de cada estado membro. Portanto, funciona como um meio de alcançar a consistência legislativa.

Um dos aspectos inovadores da diretiva diz respeito à imposição de obrigações aos controladores de dados que se envolvam em atividades de processamento de dados. Além disso, a diretiva estabelece princípios fundamentais que devem ser observados durante a coleta, processamento e utilização de dados. Além disso, forneça uma definição para práticas relacionadas à tecnologia (MALHEIRO, 2017).

O segundo artigo, especificamente em seu parágrafo oitavo, introduz a noção de consentimento, que é definido como "uma manifestação de vontade não coagida, explícita e informada do titular dos dados, indicando sua concordância com o tratamento de seus dados pessoais". Além disso, pode-se observar na alínea a do artigo 7º que o tratamento de dados está condicionado à obtenção de consentimento, exceto nas hipóteses de isenção, o que guarda semelhança com o disposto na LGPD.

Conforme análise de Bioni (2020), o marco regulatório em questão introduziu uma nova abordagem que o situa na quarta geração de leis de proteção de dados. Isso se deve à ênfase da Diretiva no titular dos dados e nos controladores de dados, o que ressalta seu caráter inovador.

Em relação às diretrizes, cada nação tem um prazo específico para realizar o processo de adaptação, comumente chamado de "transposição". "O descumprimento desse processo pode resultar em ação judicial contra o país em questão perante o Tribunal Europeu de Justiça" (DONEDA, 2006, p. 224).

No dia 27 de abril de 2016, foi aprovado o GDPR, também conhecido como Regulamento Geral de Proteção de Dados, que substituiu a Diretiva 95/46/CE. De acordo com

Malheiros (2017), embora tenha revogado a diretiva anterior, o GDPR manteve seus princípios.

O termo "consentimento" é um conceito recorrente no discurso jurídico, muitas vezes acompanhado de descritores qualificativos como "livre", "específico", "informado" e "inequívoco". Apesar da presença de hipóteses alternativas em que o consentimento pode ser dispensado, é evidente que o artigo 6º dá ênfase significativa à importância da obtenção do consentimento. Os adjectivos em causa encontram-se referenciados no ponto 32 das considerações e no ponto 11 do artigo 4.º.

2.2.1 Eslovénia (um “país digital”)

Neste tópico, examinaremos como a Eslovênia, conhecida por suas ambições de se tornar um "país digital", implementou as diretrizes de proteção de dados da União Europeia (UE), particularmente o Regulamento Geral sobre a Proteção de Dados (GDPR) e a Diretiva sobre a Proteção de Dados na Aplicação da Lei. Discutiremos as iniciativas de governo eletrônico da Eslovênia, a digitalização dos serviços públicos e como essas medidas se alinham com as normas de proteção de dados.

A Eslovênia, como Estado-membro da UE, está sujeita ao GDPR, que se tornou aplicável em 25 de maio de 2018. Este regulamento marca uma mudança significativa na proteção de dados pessoais, oferecendo uma abordagem mais unificada para a segurança da informação em toda a Europa. Exploraremos como as autoridades eslovenas adotaram as disposições do GDPR e as adaptaram às necessidades locais, garantindo que as empresas e instituições públicas cumprissem os novos requisitos legais (COMISSÃO EUROPEIA, 2021).

Desta forma, a Eslovênia tem traçado um caminho sólido para se estabelecer como um líder em governo eletrônico e digitalização de serviços públicos na União Europeia. A estratégia "Digital Slovenia 2030" é a resposta governamental para os desafios do desenvolvimento digital, com o objetivo de transformar integralmente o país até 2030. Essa estratégia abrangente inclui metas e indicadores mensuráveis que abarcam desde infraestrutura gigabit até a transformação digital da economia, serviços públicos digitais, caminho para a Sociedade Inteligente 5.0, cibersegurança, competências digitais e inclusão, além de elementos relacionados como ambientes habilitadores e a transição verde .(COMISSÃO EUROPEIA, 2021)

A avaliação da ONU, através do Índice de Desenvolvimento de Governo Eletrônico (EGDI), destaca o avanço significativo da Eslovênia neste campo, classificando-a

na 21ª posição entre 193 países. Este progresso é evidente em todas as componentes do índice, que incluem infraestrutura de telecomunicações, desenvolvimento de capital humano e melhoria na prestação de serviços (COMISSÃO EUROPEIA, 2022).

A melhoria no desempenho do país é particularmente notável no contexto dos Objetivos de Desenvolvimento Sustentável das Nações Unidas, onde as ferramentas digitais desempenham um papel crucial para enfrentar crises interligadas e acelerar a realização desses objetivos, garantindo que ninguém fique para trás na era digital (COMISSÃO EUROPEIA, 2016).

Em termos de índices específicos, a Eslovênia mostra um desempenho notável no Índice de Serviços Online (OSI), onde ocupa a 22ª posição, no Índice de Capital Humano (HCI), alcançando a 12ª posição, e no Índice de Infraestrutura de Telecomunicações (TII), onde é classificada na 40ª posição. Além disso, o país tem melhorado no Índice de Participação Eletrônica (EPI), situando-se na 25ª posição, o que reflete a eficácia com que o governo esloveno utiliza serviços online para informar, consultar e decidir conjuntamente com seus cidadãos (COMISSÃO EUROPEIA, 2016).

Esses índices são componentes do EGDI, que é uma média ponderada de três índices normalizados, incluindo o OSI, que se baseia em dados coletados pela UNDESA e avalia as apresentações online nacionais de todos os Estados membros da ONU. O EPI, em particular, se concentra no uso de serviços online pelos governos para troca de informações, consultas e tomada de decisão (COMISSÃO EUROPEIA, 2016).

Os esforços da Eslovênia para integrar a digitalização com políticas de proteção de dados são fundamentais para assegurar que a inovação não comprometa a privacidade dos cidadãos. Embora os detalhes específicos de como a Eslovênia alinha sua digitalização com as políticas de proteção de dados não sejam explicitamente mencionados nas fontes consultadas, é razoável inferir que a adesão aos padrões da UE em matéria de proteção de dados, como o GDPR, desempenha um papel significativo nessa integração (SLOVENIA, 2030).

A transição digital que a Eslovênia está buscando, portanto, não é apenas uma transformação tecnológica, mas também um realinhamento cultural e estrutural que abrange todos os aspectos da sociedade e do governo. O sucesso contínuo da Eslovênia nesse empreendimento dependerá de sua capacidade de manter a inovação tecnológica em equilíbrio com a proteção rigorosa dos dados e a privacidade dos cidadãos. (GOVERNMENT OF THE REPUBLIC OF SLOVENIA, 2022).

É importante notar que a digitalização e as iniciativas de governo eletrônico abrangem uma variedade de serviços públicos, desde a saúde até a educação e a administração

fiscal. A Eslovênia tem investido em plataformas digitais que permitem aos cidadãos e às empresas interagir com o governo de maneira mais eficiente, reduzindo o tempo e os custos associados à burocracia. (GOVERNMENT OF THE REPUBLIC OF SLOVENIA, 2022).

No entanto, para garantir que as informações detalhadas sobre a implementação específica dessas iniciativas e sua relação com as políticas de proteção de dados sejam precisas e completas, seria necessário acessar mais recursos e realizar uma análise mais profunda. Isso envolveria, por exemplo, a revisão de relatórios governamentais, estudos de impacto sobre a privacidade e análises de especialistas em proteção de dados e cibersegurança.

A eficácia com que a Eslovênia gerencia a digitalização dos serviços públicos enquanto protege os dados pessoais dos cidadãos é um indicador crítico de sua capacidade de navegar no equilíbrio entre a inovação tecnológica e os direitos à privacidade. Isso não apenas melhora a prestação de serviços públicos, mas também reforça a confiança do público nas instituições digitais.

2.3 General Data Protection Regulation - GDPR

O Regulamento Geral de Proteção de Dados (General Data Protection Regulation - GDPR) é uma lei da União Europeia que entrou em vigor em 25 de maio de 2018. Ele foi projetado para harmonizar as leis de privacidade de dados em toda a Europa, proteger e fortalecer a privacidade e os direitos dos cidadãos da UE sobre seus dados pessoais e remodelar a maneira como as organizações em toda a região abordam a privacidade de dados (MALHEIRO, 2017).

O GDPR substituiu a Diretiva de Proteção de Dados de 1995, que estabeleceu o primeiro conjunto de leis de privacidade de dados na UE. O novo regulamento é um passo significativo na evolução da proteção de dados, expandindo os direitos dos indivíduos e colocando obrigações mais pesadas sobre as organizações (EUROPEIA, 2020).

De acordo com Europeia (2020) relata um exemplo de aplicação do regulamento de uma empresa que tem uma filial na União Europeia oferece serviços de viagens para clientes localizados nos países Bálticos e, para isso, precisa lidar com informações pessoais de indivíduos. Em relação a um exemplo de não aplicação do regulamento: Uma pessoa utiliza sua lista de contatos privada para enviar convites por e-mail para uma festa que está organizando (atividade doméstica excluída do regulamento).

De acordo com Europeia (2020) entre as muitas disposições do GDPR, algumas das mais notáveis incluem:

1) **Consentimento**: As organizações precisam obter o consentimento explícito para processar os dados das pessoas e as pessoas têm o direito de saber exatamente que dados pessoais uma organização tem e o que está fazendo com eles.
2) **Direito ao acesso e à portabilidade dos dados**: As pessoas têm o direito de acessar seus dados pessoais, corrigi-los, excluí-los ou transferi-los para outra empresa.
3) **Direito ao esquecimento**: Também conhecido como direito à exclusão, significa que as pessoas podem solicitar que suas informações sejam apagadas.
4) **Notificação de violação de dados**: As organizações devem informar as autoridades reguladoras e os indivíduos afetados em caso de violação de dados.
5) **Penalidades**: As organizações podem ser multadas em até 20 milhões de euros ou 4% de sua receita global anual por violações ao GDPR, o que for maior.

O GDPR tem um alcance global, pois se aplica a todas as empresas que processam os dados pessoais dos residentes da UE, independentemente de onde estejam localizadas. Assim, muitas organizações fora da UE também foram obrigadas a se conformar com o GDPR.

2.4 Comparativo com outros países

Segundo Silva (2021), a aplicação da Lei Geral de Proteção de Dados no contexto brasileiro difere em aspectos importantes das abordagens adotadas por países como os Estados Unidos no que concerne à privacidade e proteção de dados pessoais.

Enquanto o Brasil finalmente consolidou uma legislação geral sobre o tema em 2018, os EUA nunca desenvolveram uma lei federal ampla equivalente. A regulação americana é multifacetada, envolvendo uma combinação de leis federais, estaduais e själv-regulatory frameworks específicos de determinados setores (SAFARI, 2020).

Essa característica híbrida e fragmentada do sistema regulatório americano gera incertezas para empresas e cidadãos. Além disso, o foco tem sido historicamente maior em

aspectos ligados à segurança nacional e combate à fraude do que na garantia de direitos dos indivíduos (SILVA, 2021).

Já o modelo inaugurado pela LGPD está alinhado à tradição europeia de leis omnibus sobre privacidade, conferindo controle dos dados ao próprio titular, fornecendo transparência sobre como os dados são usados e limitando o compartilhamento de informações confidenciais (RAAB, 2018).

A disparidade entre as abordagens regulatórias do Brasil e Estados Unidos no campo da proteção de dados reflete distintas culturas políticas e prioridades nacionais (RAAB, 2018).

Enquanto a Lei Geral de Proteção de Dados personifica uma concepção de privacidade como direito civil fundamental, o modelo estadunidense se ancora primordialmente na defesa de interesses governamentais e comerciais (SAFARI, 2020).

Essa assimetria tem raízes históricas no individualismo característico da sociedade americana, bem como na ênfase em valores como livre iniciativa, propriedade privada e liberdade de expressão (SILVA, 2021).

A fragmentação das leis de privacidade nos EUA é reflexo do sistema federativo, da menor ingerência estatal sobre o mercado e da autorregulação setorial. Já a tradição europeia consolidou uma noção mais coletiva e universal de direitos relacionados à proteção de dados pessoais e da vida privada.

Contudo, alguns autores questionam se o rigor do modelo representado pela GDPR e replicado pela LGPD não acarreta também em ônus excessivo para a inovação e a livre circulação de dados. As implicações práticas de restrições amplas sobre o uso de informações pessoais ainda carecem de investigação aprofundada (ANDRADE, 2020).

De toda forma, as especificidades de implementação das leis de proteção de dados em diferentes países servem como laboratórios globais para experimentações regulatorias diante de problemas comuns gerados pela economia digital. A recíproca influência e até hibridização parcial de modelos são possíveis no futuro (ANDRADE, 2020).

O Brasil tem a oportunidade de conciliar o resguardo de direitos individuais com políticas que fomentem a prosperidade, num equilíbrio sensível entre valores públicos e privados. A efetividade da LGPD dependerá da calibragem adequada desse balanceamento de interesses (ANDRADE, 2020).

Portanto, embora vários princípios e conceitos da legislação brasileira sejam oriundos de referenciais globais, sua aplicação prática reflete uma ênfase distinta dos marcos regulatórios em vigor nos EUA no que se refere à proteção da privacidade e dos direitos

fundamentais dos cidadãos.

2.5 A proteção de dados no Brasil vs. Europa

Inicialmente, é importante destacar que neste texto será realizada uma análise comparativa entre o cenário brasileiro e o europeu em relação à proteção de dados, considerando que este último é considerado um dos mais avançados globalmente e que a lei brasileira foi inspirada na GDPR.

Em maio de 2016, a União Europeia iniciou sua jornada em prol da proteção de dados em seu território. Apesar do lapso temporal entre as ações europeias e brasileiras, não é apenas uma questão de adequação, mas sim de estruturação das empresas e países, apoiando-se no Comitê Europeu de Proteção de Dados e nas Autoridades locais (DONEDA, 2020).

O continente europeu já se encontra em um estágio bastante avançado em relação à proteção de dados, com a uniformização de diretrizes, produção de modelos documentais, diretrizes de implementação e diversos materiais instrutivos. Além disso, grandes empresas atuam na Europa e o poder aquisitivo favorece a conformidade com a lei (DONEDA, 2020).

A proteção de dados é uma questão crítica na era digital. À medida que cada vez mais nossas vidas se movem on-line, é importante ter leis rígidas para proteger nossos dados pessoais. O Brasil e a União Europeia (UE) promulgaram leis abrangentes de proteção de dados, a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR), respectivamente. Essas leis compartilham muitas semelhanças, mas também existem algumas diferenças importantes (BRANCO; FORTES, 2022).

A LGPD e a GDPR têm os seguintes objetivos:

1) Proteger a privacidade dos indivíduos;
2) Dar aos indivíduos controle sobre seus dados pessoais;
3) Exigir que as empresas sejam transparentes sobre como coletam e usam dados pessoais;
4) Exigir que as empresas e organizações implementem fortes medidas de segurança para proteger dados pessoais.

Ambas as leis também dão aos indivíduos o direito de acessar seus dados pessoais, o direito de ter seus dados apagados e o direito de se opor ao processamento de seus dados.

A LGPD e a GDPR diferem em alguns aspectos importantes. Uma das diferenças mais significativas é o escopo das leis. A LGPD se aplica a todas as empresas que processam dados pessoais de pessoas físicas localizadas no Brasil, independentemente de onde a empresa esteja localizada. O GDPR se aplica a todas as empresas que processam dados pessoais de indivíduos localizados na UE, mas somente se a empresa oferecer bens ou serviços a indivíduos na UE ou monitorar o comportamento de indivíduos na UE.

Outra diferença importante são as penalidades em caso de descumprimento. A LGPD permite multas de até 2% da receita anual de uma empresa no Brasil, ou até R$ 50 milhões (aproximadamente € 8 milhões), o que for maior. O GDPR permite multas de até 4% do faturamento global anual de uma empresa, ou € 20 milhões, o que for maior (MIRANDA, 2019).

A LGPD e a GDPR são leis abrangentes de proteção de dados que compartilham muitas semelhanças. No entanto, também existem algumas diferenças importantes entre as leis, como o escopo das leis e as penalidades por descumprimento. As empresas que operam no Brasil e na UE devem estar cientes das diferenças entre as leis e tomar medidas para cumprir ambas as leis. (MIRANDA, 2019).

Em relação a proteção de Dados no Brasil, a Lei Geral de Proteção de Dados (LGPD) do Brasil é uma lei abrangente que regula o processamento de dados pessoais por entidades públicas e privadas. A LGPD foi promulgada em 2018 e entrou em vigor em 2020.

A LGPD é aplicada pela Autoridade Nacional de Proteção de Dados (ANPD). A ANPD tem poderes para investigar e punir violações à LGPD. As multas por infrações à LGPD podem chegar a 2% da receita anual da controladora no Brasil, ou até R$ 50 milhões (aproximadamente € 8 milhões). (PINHEIRO, 2021).

Em relação a proteção de dados na União Europeia, **o** Regulamento Geral de Proteção de Dados (GDPR) é uma lei abrangente que regula o processamento de dados pessoais por entidades públicas e privadas na União Europeia (UE). O GDPR foi promulgado em 2016 e entrou em vigor em 2018.

2.5.1 A LGPD do Brasil e a GDPR da EU

A LGPD e a GDPR são leis abrangentes que regulam o processamento de dados pessoais. No entanto, existem algumas diferenças fundamentais entre as duas leis.

Uma diferença fundamental é o escopo das leis. A LGPD se aplica a todo processamento de dados pessoais por entidades públicas e privadas no Brasil. O GDPR, por

outro lado, aplica-se apenas ao processamento de dados pessoais por controladores e processadores localizados na UE, ou por controladores e processadores fora da UE que oferecem bens ou serviços a indivíduos na UE ou que monitoram o comportamento de indivíduos na EU. (DONEDA, 2020).

Outra diferença fundamental são os direitos que os indivíduos têm de acordo com as leis. A LGPD concede aos indivíduos uma série de direitos, incluindo o direito de acessar seus dados pessoais, solicitar que seus dados pessoais sejam corrigidos, atualizados ou excluídos, opor-se ao processamento de seus dados pessoais, restringir o processamento de seus dados pessoais, portar sua dados pessoais para outro controlador e registrar uma reclamação junto a uma autoridade supervisora. O GDPR dá aos indivíduos direitos semelhantes, mas também dá aos indivíduos o direito de serem esquecidos, que é o direito de ter seus dados pessoais apagados em determinadas circunstâncias (BRANCO; FORTES, 2022).

Finalmente, as penalidades por violações das leis são diferentes. A LGPD permite multas de até 2% da receita anual da controladora no Brasil, ou até R$ 50 milhões (aproximadamente € 8 milhões). O GDPR permite multas de até 4% do faturamento anual global do controlador, ou € 20 milhões, o que for maior.

Quadro 1 - Comparação entre a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral de Proteção de Dados (GDPR)

LEIS	PRINCÍPIOS	DIREITOS	OBRIGAÇÕES
LGPD	• Legalidade, justiça e transparência • Limitação de finalidade • Minimização de dados • Precisão • Limitação de armazenamento • Integridade e confidencialidade • Responsabilidade	• Acessar seus dados pessoais • Solicitar que seus dados pessoais sejam corrigidos, atualizados ou excluídos • Opor-se ao tratamento dos seus dados pessoais • Restringir o tratamento dos seus dados pessoais • Transferir seus dados pessoais para outro controlador	• Obtenha o consentimento dos indivíduos antes de processar seus dados pessoais • Implementar medidas de segurança adequadas para proteger os dados pessoais • Fornece aos indivíduos informações sobre o processamento de seus dados pessoais • Responder a solicitações

			individuais de acesso, correção, exclusão, objeção, restrição ou portabilidade de seus dados pessoais
GDPR	• Legalidade, justiça e transparência • Limitação de finalidade • Minimização de dados • Precisão • Limitação de armazenamento • Integridade e confidencialidade • Responsabilidade	• Acessar seus dados pessoais • Solicitar que seus dados pessoais sejam corrigidos, atualizados ou excluídos • Opor-se ao tratamento dos seus dados pessoais • Restringir o tratamento dos seus dados pessoais • Transferir seus dados pessoais para outro controlador • Apresentar uma reclamação a uma autoridade supervisora	• Obtenha o consentimento dos indivíduos antes de processar seus dados pessoais • Implementar medidas de segurança adequadas para proteger os dados pessoais • Fornece aos indivíduos informações sobre o processamento de seus dados pessoais • Responder a solicitações individuais de acesso, correção, exclusão, objeção, restrição ou portabilidade de seus dados pessoais

Fonte: OneTrust DataGuidance (2022).

O quadro que fornece uma comparação entre a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. A tabela está estruturada para ilustrar a semelhança entre os dois marcos regulatórios em termos de princípios, direitos dos titulares de dados e obrigações dos controladores de dados.

Princípios: Ambas as leis compartilham princípios idênticos. Eles exigem que o tratamento de dados seja realizado de maneira legal, justa e transparente, com limitação de finalidade (os dados só podem ser coletados para finalidades específicas, explícitas e legítimas), minimização de dados (apenas os dados necessários devem ser coletados), precisão (os dados devem ser precisos e, se necessário, atualizados), limitação de armazenamento (os

dados não podem ser mantidos por mais tempo do que o necessário), integridade e confidencialidade (os dados devem ser tratados de forma a garantir sua segurança, incluindo proteção contra tratamento não autorizado ou ilegal), e responsabilidade (o controlador é responsável por demonstrar conformidade com os princípios).

Direitos: Os direitos dos titulares de dados também são muito semelhantes sob ambas as leis. Os titulares de dados têm o direito de acessar seus dados pessoais, solicitar que seus dados pessoais sejam corrigidos, atualizados ou excluídos, opor-se ao tratamento dos seus dados pessoais, restringir o tratamento dos seus dados pessoais e transferir seus dados pessoais para outro controlador. A única diferença notável aqui é que o GDPR também dá ao titular dos dados o direito de apresentar uma reclamação a uma autoridade supervisora.

Obrigações: As obrigações dos controladores de dados são as mesmas em ambas as leis. Eles devem obter o consentimento dos indivíduos antes de processar seus dados pessoais, implementar medidas de segurança adequadas para proteger os dados pessoais, fornecer aos indivíduos informações sobre o processamento de seus dados pessoais e responder a solicitações individuais de acesso, correção, exclusão, objeção, restrição ou portabilidade de seus dados pessoais.

Figura 1 - DPO (GDPR) vs Encarregado (LGPD)

Fonte: Guia Prático do Encarregado pelo Tratamento de Dados – DPO – LGPD. (2020).

Em geral, o quadro ilustra que a LGPD e o GDPR são muito semelhantes em sua estrutura e requisitos, embora existam algumas diferenças nos detalhes de como essas leis são aplicadas e cumpridas.

A proteção de dados é uma questão crítica na era digital. A LGPD e a GDPR são leis abrangentes que ajudam a proteger a privacidade dos indivíduos e dão aos indivíduos controle sobre seus dados pessoais. As empresas que operam no Brasil e na UE devem estar cientes das leis e tomar medidas para cumpri-las (LEAL; SOUZA, 2020).

O Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e a Lei Geral de Proteção de Dados (LGPD) do Brasil determinam o papel dos profissionais de proteção de dados. O GDPR exige um Data Protection Officer (DPO) para organizações públicas e privadas que processam dados pessoais em grande escala. O DPO tem autonomia para cumprir suas obrigações sem interferência, deve relatar à alta administração e manter confidencialidade. A LGPD também exige um Encarregado responsável, com funções similares ao DPO, incluindo a aceitação de reclamações, orientação e conformidade com a lei. Embora a posição do Encarregado na empresa não seja clara pela LGPD, é possível que a Autoridade Nacional de Proteção de Dados (ANPD) estabeleça regras futuras. Em ambos os casos, esses profissionais são fundamentais para a proteção de dados pessoais (LEAL; SOUZA, 2020).

CONSIDERAÇÕES FINAIS

A análise desenvolvida permite concluir que tanto a Lei Geral de Proteção de Dados quanto o Regulamento Geral de Proteção de Dados instituíram avanços importantes na garantia dos direitos à privacidade e à autodeterminação informativa. Ambos os diplomas estão ancorados em um rol de princípios e diretrizes que visam limitar a coleta e o uso de dados pessoais por organizações públicas e privadas.

No entanto, o estudo também revelou que existem diferenças importantes entre as abordagens adotadas pelo Brasil e pela União Europeia, o que reflete distintas culturas regulatórias, trajetórias políticas e contextos socioeconômicos. Enquanto o GDPR constitui regulamentação diretamente aplicável e de observância obrigatória em todos os países-membros, a LGPD ainda carece de normatização infralegal e enfrenta percalços de implementação.

Além disso, o rigor das sanções administrativas e o grau de consolidação das respectivas autoridades de proteção de dados são fatores que potencialmente influenciam no cumprimento efetivo das normas de privacidade. A União Europeia conta com tradição mais longeva e instituições supranacionais responsáveis por zelar uniformidade na aplicação do

GDPR.

A análise desenvolvida ao longo deste trabalho permitiu elucidar uma série de aspectos centrais sobre a evolução das legislações de proteção de dados pessoais no Brasil e na União Europeia.

Observou-se que tanto a Lei Geral de Proteção de Dados quanto o Regulamento Geral sobre a Proteção de Dados representaram um grande avanço em relação aos marcos normativos anteriores em seus respectivos contextos. A LGPD finalmente forneceu uma estrutura legal abrangente e unificada para a privacidade no Brasil, enquanto o GDPR elevou os requisitos de compliance e as sanções pelo descumprimento na UE.

Ambas as normativas compartilham princípios e fundamentos essenciais, como os direitos dos titulares sobre seus dados, a transparência sobre as operações de tratamento, as bases legais que autorizam o processamento de informações pessoais e a atribuição de responsabilidades aos agentes de tratamento. Isso reflete um consenso internacional mínimo sobre o que significa efetivamente "proteger" dados na era digital.

No entanto, diferenças importantes entre os contextos brasileiro e europeu implicam em variações significativas na aplicabilidade e *enforcement* das respectivas leis de proteção de dados. O rigor das sanções e a consolidação institucional das autoridades regulatórias parecem ser fatores críticos.

Enquanto a União Europeia já conta com mais de duas décadas de amadurecimento nesse campo do direito digital, o desenvolvimento infralegal, a capacitação de empresas e entes públicos e a atuação da ANPD ainda suscitam dúvidas sobre o cumprimento pleno dos objetivos da LGPD no cenário nacional.

Portanto, novas investigações se fazem necessárias para avaliar os desafios concretos e as perspectivas associadas à efetiva implementação da Lei Geral de Proteção de Dados no Brasil. São questões especialmente prementes em face da aceleração da transformação digital impulsionada pela pandemia de Covid-19.

Além disso, a crescente interconexão entre diferentes ordenamentos jurídicos em matéria de privacidade e governança de dados pessoais constitui fenômeno pouco explorado pela literatura especializada até o momento. São temas que tendem a assumir papel cada vez mais estratégico.

A análise comparativa entre as legislações do Brasil e da União Europeia cumpriu seu propósito de lançar luz sobre convergências e assimetrias entre dois dos principais modelos regulatórios em vigência globalmente. Contribui assim para o aprofundamento do entendimento de como salvaguardar direitos fundamentais diante dos desafios do mundo

hiperconectado do presente e do futuro.

Diante do exposto, novos estudos poderiam investigar os desafios, impactos e perspectivas associadas à concretização dos objetivos da LGPD, tanto do ponto de vista da administração pública quanto das corporações e dos cidadãos. A efetividade das estruturas de governança do tratamento de dados no Brasil também carece de investigação aprofundada. Ademais, a interconexão entre diferentes ordenamentos jurídicos nesta seara crucial do direito digital constitui fenômeno de importância crescente a ser elucidado.

REFERÊNCIAS

ANDRADE, Pedro. **Privacidade e proteção de dados**: a perspectiva do desenvolvimento. In: LEITE, George Salomão; LEMOS, Ronaldo (org.). Marco Civil da Internet. São Paulo: Atlas, 2020.

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

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 18 maio. 2020.

BRANCO, Gina Vidal Marcílio; FORTES, Vinícius Borges. **Privacidade e Proteção de Dados Pessoais.** São Paulo: Thomson Reuters Brasil, 2022.

CERVO, A. L. BERVIAN, P. A. **Metodologia científica**. 5.ed. São Paulo: Prentice Hall, 2002.

COMISSÃO EUROPEIA. **Proteção de dados na UE.** (2021) [online] Disponível em: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt. .Acesso em: 07 nov. 2023.

COMISSÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados (RGPD).** (2022) [online] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679 .Acesso em: 07 nov. 2023.

COMISSÃO EUROPEIA. **Diretiva sobre a Proteção de Dados na Aplicação da Lei**. (2016) [online] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680 .Acesso em: 07 nov. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. ed. Rio de Janeiro: Renovar, 2006.

DONEDA, D. **A Lei Geral de Proteção de Dados.** São Paulo: Saraiva Educação, 2020.

ERCOLE, F. F., MELO, L. S., ALCOFORADO, C. L. G. C. Revisão integrativa versus revisão sistemática. **Revista Mineira de Enfermagem**. 9-11. (2020).

EUROPEIA, Comissão. **Para que serve o regulamento geral sobre a proteção de dados (RGPD)?** Europa: 2020. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pt#resposta>. Acesso em: 23 mai. 2023.

GALVÃO, C.M.; SAWADA, N.O.; TREVIZAN, M.A. Revisão sistemática: recurso que proporciona a incorporação das evidências na prática da enfermagem. **Revista Latino-Americana de Enfermagem,** Ribeirão Preto (SP), v.12, n.3, p.549-556, jun. 2004.

GOVERNMENT OF THE REPUBLIC OF SLOVENIA. UN: **Slovenia has made progress in the field of E-Government.** (2022) [online] Disponível em: https://www.gov.si/en/news/2022-10-03-un-slovenia-has-made-progress-in-the-field-of-e-government/. Acesso em: 07 nov. 2023.

GUSTAVO. **Guia Prático do Encarregado pelo Tratamento de Dados – DPO – LGPD**. [*S. l.: s. n.*], 2020. Disponível em: https://www.pdcati.com.br/encarregado-pelo-tratamento-de-dados-dpo-lgpd/. Acesso em: 7 nov. 2023.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do brasil (lei nº 13.709/18).** Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, 2019. Data da publicação: 05 dez. 2019. Disponível em: Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 20 mai. 2023.

KUNER, Christopher. **The European Union and the Search for an International Data Protection Framework** (December 6, 2014). Groningen Journal of International Law, volume 2 number 2, pp. 55-71, 2014, University of Cambridge Faculty of Law Research Paper No. 48/2015, Available at SSRN: https://ssrn.com/abstract=2495273 or http://dx.doi.org/10.2139/ssrn.2495273.

LIMA, C. L. **Proteção de Dados Pessoais**: A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2020.

LEAL, Mônia Clarissa Hennig; SOUZA, Carlos Affonso. **Casos de direito digital e proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020.

MIRANDA, J. **Manual de Proteção de Dados Pessoais**. Lisboa: Universidade de Lisboa, 2019.

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

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet:** uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016. Trabalho de Conclusão de Curso (graduação) – Universidade de Brasília, Faculdade de Direito, 2017. Data da publicação: 8 jan. 2018. Disponível em: bdm.unb.br/handle/10483/18883. Acesso em: 10 mai. 2023.

MANCUSO, Vinícius; PEREIRA, Maria Fernanda. **Desafios da ANPD revelam limites na**

implementação da LGPD. Jota, 27 jul. 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/desafios-da-anpd-revelam-limites-na-implementacao-da-lgpd-27072022. Acesso em: 10 dez. 2023.

ONETRUST DATAGUIDANCE; Baptista Luz Advogados. **Comparando as leis de privacidade:** GDPR v. LGPD. Disponível em: https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-lgpd-0. Acesso em: 07 niv. 2023.

PINHEIRO, Patricia Peck. **Direito digital**. 6. Ed. São Paulo: Saraiva, 2016. E-book. Acesso restrito via Minha Biblioteca.

PINHEIRO, Patricia Peck; SÁ, André. **Desvendando a Lei Geral de Proteção de Dados**: tudo o que você precisa saber a respeito da LGPD. Rio de Janeiro: GZ Editora, 2021.

REDDING, V. **The Long Road to the General Data Protection Regulation**. Brussels: EU Commission, 2015.

RAAB, C. **Information privacy**: networks of regulation at the subglobal level. Global Justice: Theory Practice Rhetoric, v.11, n.2, p. 76-98, 2018.

SLOVENIA, **Republic of. Digital Slovenia** (2030). [online] Disponível em: https://nio.gov.si/nio/asset/strategija+digitalna+slovenija+2030?lang=en. Acesso em: 07 nov. 2023.

SAFARI, H. A comparative review of data protection legislation in the United States and European Union. **Journal of Contemporary Issues in Business and Government**, v.26, n.1, p 44-58, 2020.

SILVA, F. M. **Lei Geral de Proteção de Dados**: a experiência jurídica brasileira e o direito comparado. Civilistica.com, Rio de Janeiro, v. 10, n. 1, p. 1-25, 2021.

SILVA, Edna Lúcia da.; MENEZES, Estera Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. Florianópolis: UFSC/ PPGEP/LED, 2000, 118 P.

SANTOS, C. R. P. **Proteção de Dados Pessoais**: Um Diálogo entre o Brasil e a União Europeia. Brasília: Câmara dos Deputados, 2021.

SCHWARTZ, P. M.; PEIFER, R. **Transatlantic Data Protection. Oxford**: Oxford University Press, 2017.

SMITS, J. M. **The Mind and Method of the Legal Academic**. Cheltenham: Edward Elgar, 2014.

TEIXEIRA, Tarcisio; MAGRO, Américo Ribeiro. **Proteção de dados**: fundamentos jurídicos. Salvador: JusPODIVM, 2020.