

# REVISTA TÓPICOS

---

## PROTEÇÃO DE DADOS NO BRASIL E NA UNIÃO EUROPEIA: FUNDAMENTOS, REGULAMENTAÇÃO E REPERCUSSÕES NO CENÁRIO ORGANIZACIONAL

DOI: 10.5281/zenodo.14823003

Kevin Cristian Paulino Freires<sup>1</sup>

Micael Campos da Silva<sup>2</sup>

### RESUMO

Este trabalho aborda a temática da preservação de dados no Brasil e na União Europeia, com foco nas regulamentações da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral sobre a Proteção de Dados (GDPR), e suas repercussões no cenário organizacional. Desse modo, o estudo tem como objetivo analisar as instruções dessas legislações, comparando e analisando seus impactos nas práticas empresariais, com ênfase nos desafios enfrentados pelas organizações para garantir a conformidade e implementar políticas de privacidade e segurança da informação. Ademais, a pesquisa se caracteriza como uma investigação bibliográfica de natureza qualitativa, que busca fundamentar a análise por meio de fontes acadêmicas relacionados às normativas de preservação de dados dos indivíduos. Assim, salienta-se que o objetivo foi atingido com sucesso, evidenciando que as instituições têm se adaptado às exigências legais, implementando práticas de compliance e políticas mais robustas de

**REVISTA TÓPICOS - ISSN: 2965-6672**

# REVISTA TÓPICOS

---

defesa de dados. Logo, o trabalho contribui teoricamente ao oferecer uma visão comparativa entre a LGPD e o GDPR, destacando suas semelhanças e diferenças. Por fim, sugere-se a realização de estudos empíricos futuros para avaliar as práticas das empresas em diferentes setores e o impacto da conformidade nas relações com os consumidores e na competitividade no mercado global.

Palavras-chave: Defesa de dados Direitos digitais, Legislação comparada, Política de privacidade, Violação e Gestão de dados.

## ABSTRACT

This work addresses the issue of data preservation in Brazil and the European Union, focusing on the regulations of the General Data Protection Law (LGPD) and the General Data Protection Regulation (GDPR), and their repercussions on the organizational scenario. Therefore, the study aims to analyze the instructions of these laws, comparing and analyzing their impacts on business practices, with an emphasis on the challenges faced by organizations to ensure compliance and implement privacy and information security policies. Furthermore, the research is characterized as a bibliographic investigation of a qualitative nature, which seeks to support the analysis through academic sources related to the regulations for preserving individuals' data. Therefore, it should be noted that the objective was successfully achieved, showing that institutions have adapted to legal requirements, implementing compliance practices and more robust data defense policies. Therefore, the work contributes theoretically by offering a comparative view between the LGPD and the GDPR, highlighting their similarities and differences. Finally, it is suggested that future empirical

# REVISTA TÓPICOS

---

studies be carried out to evaluate companies' practices in different sectors and the impact of compliance on consumer relations and competitiveness in the global market.

Keywords: Data Defense, Digital rights, Comparative legislation, Privacy Policy, Breach and Data Management.

## 1 Introdução

A preservação de dados dos indivíduos é um tema que ganhou uma relevância significativa nas últimas décadas, em decorrência do avanço tecnológico e da crescente troca de informações no ambiente digital. O processamento, coleta, e armazenamento de dados particulares dos indivíduos tornou-se uma prática comum em organizações de diversos segmentos, o que levanta questões essenciais sobre a privacidade e a segurança das informações. A origem da defesa de dados remonta aos primeiros esforços de regulamentação na Europa, com o surgimento de legislações, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia. Desse jeito, esses marcos legais buscam estabelecer parâmetros claros para o tratamento de dados pessoais, equilibrando a defesa do indivíduo e a necessidade de inovação tecnológica nas organizações.

No Brasil, a LGPD foi sancionada em 2018 e entrou em vigor em 2020, com o objetivo de regulamentar o tratamento de dados individuais, trazendo um novo paradigma para a forma como as instituições lidam com as informações de seus consumidores. Dessa forma, a União Europeia, por sua vez, implementou o GDPR em 2018, o qual é considerado um dos

# REVISTA TÓPICOS

---

regulamentos mais rigorosos do mundo em termos de preservação de dados. Ou seja, o contexto dessas legislações reflete a preocupação com a segurança cibernética, a privacidade dos indivíduos e o uso ético dos dados no âmbito empresarial.

Exemplificando, a entrada em vigor da LGPD no Brasil e do GDPR na União Europeia provocou mudanças significativas nas práticas empresariais, com as organizações precisando adaptar suas estruturas operacionais, processos internos e treinamentos de funcionários. Desse modo, o cumprimento das exigências dessas legislações exige que as instituições adotem medidas mais rigorosas para garantir a preservação de dados, como a implementação de políticas de privacidade, treinamentos regulares sobre segurança da informação e a criação de comissões de defesa de dados.

Diante disso, o problema da pesquisa reside na análise das repercussões dessas legislações no cenário organizacional, especialmente no que se refere aos desafios enfrentados pelas instituições para adequar-se às normas de preservação de dados, e como essas mudanças impactam a gestão estratégica da privacidade e segurança da informação nas organizações.

Ademais, esta pesquisa se justifica pela necessidade de compreender as implicações da LGPD e do GDPR no cenário organizacional, não apenas do ponto de vista legal, mas também em termos operacionais e estratégicos. Dessa maneira, a compreensão de como essas normas afetam as práticas empresariais é fundamental para que as instituições possam se adaptar de

# REVISTA TÓPICOS

---

maneira eficiente, garantindo a conformidade com as leis e preservando os dados dos indivíduos de seus clientes e colaboradores.

Ainda assim, a relevância da pesquisa está na contribuição que ela oferece para o entendimento das consequências jurídicas e operacionais da implementação das legislações de defesa de dados, especialmente em um momento em que as instituições estão enfrentando um ambiente regulatório cada vez mais complexo e exigente. À vista disso, este estudo proporciona esclarecimentos sobre como as organizações podem melhorar suas práticas de segurança da informação e estratégias de privacidade, tornando-se mais transparentes e confiáveis para os consumidores.

Diante do exposto, este trabalho objetiva analisar as instruções da LGPD e do GDPR, comparando suas semelhanças e diferenças, e analisar os desafios que as organizações enfrentam na criação dessas normas. Além disso, busca compreender as repercussões dessas regulamentações na gestão da privacidade e segurança da informação nas instituições, considerando a perspectiva de conformidade e as transformações operacionais que esses processos demandam.

Nesse sentido, o percurso metodológico adotado será uma pesquisa bibliográfica de natureza qualitativa, com a revisão e análise de artigos relacionados às legislações de defesa de dados e suas implicações no ambiente organizacional. E, também, a pesquisa buscará fundamentar-se em teorias jurídicas, tecnológicas e de gestão, para fornecer uma visão dos impactos das normas de preservação de dados.

# REVISTA TÓPICOS

---

Sendo assim, o percurso teórico se concentrará em teorias jurídicas relacionadas à preservação dos dados dos indivíduos, segurança da informação e privacidade, com ênfase nas diferenças e semelhanças entre a LGPD e o GDPR. Além disso, serão investigadas as abordagens de governança corporativa e compliance que auxiliam as organizações a se adequarem a essas legislações.

Com isso, a estrutura do trabalho está organizada da seguinte forma: no capítulo 1, será apresentada a introdução, contextualizando o tema e os objetivos da pesquisa. No capítulo 2, será discutido as diretrizes fundamentais da LGPD e do GDPR, analisando os desafios jurídicos e operacionais na preservação de dados. O capítulo 3 abordará os impactos organizacionais dessas leis, detalhando suas repercussões na gestão estratégica de privacidade e segurança da informação. Por fim, no capítulo 4, serão apresentadas as considerações finais, com reflexões sobre as implicações da pesquisa e sugestões para futuras investigações.

## 2 Diretrizes Fundamentais da LGPD e do GDPR: Desafios Jurídicos e Operacionais na Preservação de Dados no Ambiente Organizacional

A LGPD é uma regulamentação brasileira que visa defender os direitos essenciais de liberdade e privacidade, estabelecendo instruções claras para o tratamento de dados dos indivíduos mundialmente, em especial, no Brasil e União Europeia, bem como ela foi sancionada em 2018 e entrou em vigor em 2020, sendo inspirada, em grande parte, pela GDPR da União Europeia, que entrou em vigor em 2018 (Oliveira, 2023). Dessa forma, o GDPR é uma regulamentação europeia que estabelece normas rigorosas

# REVISTA TÓPICOS

---

sobre a recolha, processamento e armazenamento de dados pessoais, com o objetivo de reforçar a privacidade e a segurança dos dados dos cidadãos da União Europeia.

Dessa maneira, ambas as legislações surgiram em um contexto global de crescente preocupação com a privacidade e segurança de dados, especialmente devido aos avanços tecnológicos e ao aumento da coleta de informações de cada pessoa pelas instituições, principalmente em contexto empresarial, no qual a globalização e o comércio digital implicaram a necessidade de uma regulamentação robusta que garanta que as instituições, especialmente as multinacionais, respeitem a privacidade das pessoas, impondo-lhes responsabilidades significativas no tratamento de dados (Oliveira, 2023). A partir dessa ótica, salienta-se que a LGPD surgiu para adequar o Brasil e a União Europeia às exigências de um mercado global cada vez mais focado em dados, alinhando-se ao GDPR e facilitando as relações comerciais entre as duas regiões.

Exemplo de semelhança se encontra em ambas as legislações, que excluem que as instituições obtenham consentimento explícito dos titulares de dados antes de processá-los (Oliveira, 2023). Uma empresa que obtém dados de clientes para fins publicitários deve garantir que esse consentimento seja claro e documentado, seja no Brasil, seja na União Europeia, ou em qualquer outra parte do mundo (Oliveira, 2023). Um exemplo de diferença seria que o GDPR impõe multas de até 4% do faturamento anual global de uma empresa em caso de descumprimento, enquanto a LGPD estabelece

# REVISTA TÓPICOS

---

um limite de 2% da receita bruta anual, com um teto de R\$ 50 milhões por infração (Oliveira, 2023).

Nessa perspectiva, os direitos dos titulares de dados são um conjunto de prerrogativas concedidas aos indivíduos para garantir o controle sobre suas informações. Esses direitos são essenciais para que os cidadãos possam exercer a sua autonomia e garantir que os seus dados sejam tratados de forma ética e segura. No GDPR, esses direitos incluem o direito à retificação, à portabilidade, ao desligamento (direito ao esquecimento) e à limitação do processamento, entre outros (Oliveira, 2023). Dessa forma, a LGPD, por sua vez, também assegura direitos semelhantes, com algumas diferenças nas condições de aplicação, mas ambos visam a preservação da intimidade e ao empoderamento do indivíduo (Oliveira, 2023).

Ademais, a implementação desses direitos nas organizações exige um esforço significativo para que as instituições desenvolvam mecanismos claros e eficientes para atender às transmissões dos titulares de dados, o que inclui a criação de canais específicos e prazos para resposta, no qual a não aplicação pode acarretar avaliações e prejudicar a imagem da instituição, além de gerar perdas financeiras consideráveis (Oliveira, 2023). Ou seja, o reconhecimento desses direitos é essencial para garantir a confiança do consumidor, e as instituições devem garantir que seus sistemas e práticas estejam alinhados às regulamentações vigentes, o que representa um desafio no que diz respeito à transformação digital e à adaptação das empresas à nova realidade.

# REVISTA TÓPICOS

---

À exemplo disso, um cliente pode solicitar a exclusão de seus dados pessoais de uma base de dados de uma instituição, seja sob o GDPR ou LGPD, e a organização deve atender a essa solicitação dentro de um prazo estipulado (Lopes, 2023). Ademais, se um titular de dados solicitar a portabilidade de suas informações para outra entidade jurídica, a organização deve garantir que o processo seja feito de forma segura e ágil, respeitando o direito previsto em ambas as legislações (Lopes, 2023).

Assim sendo, as medidas de conformidade referem-se às ações que as organizações devem adotar para garantir que estejam em conformidade com as regulamentações de defesa de dados, como a LGPD e o GDPR, no qual isso inclui a criação de políticas internas, auditorias regulares e treinamento de pessoal. Dessa forma, a governança corporativa, por sua vez, diz respeito à estrutura organizacional que garante que essas medidas sejam cumpridas, com uma supervisão constante sobre a forma como os dados são tratados e protegidos dentro de uma organização jurídica, bem como o conceito de conformidade e governança surge da necessidade de as organizações demonstrarem responsabilidade no processamento de dados dos indivíduos (Lopes, 2023).

Com isso, a implementação das medidas de conformidade e governança exige que as empresas reestruturem seus processos internos, o que pode ser um grande desafio, principalmente em instituições de grande porte ou com operações internacionais. Dessa forma, a conformidade com a LGPD e o GDPR exige a adoção de tecnologias específicas, como ferramentas de segurança da informação e a contratação de profissionais especializados,

# REVISTA TÓPICOS

---

como o Encarregado de Proteção de Dados (DPO) (Lopes, 2023). Além disso, a falta de conformidade pode gerar impactos negativos, como multas e danos à concessão, o que torna a governança um aspecto crucial para qualquer organização.

Em vista disso, a nomeação de um Data Protection Officer (DPO) para supervisionar as políticas de privacidade e garantir o cumprimento das normas é uma prática comum tanto no Brasil quanto na União Europeia (Lopes, 2023). Ainda assim, estabelecimentos como o Google e o Facebook precisam revisar suas políticas de conformidade com o GDPR e implementar novos processos de governança após serem multados por especificamente, destacando a importância da conformidade contínua (Lopes, 2023).

## 3 Impactos Organizacionais das Leis de Proteção de Dados: Repercussões da LGPD e do GDPR na Gestão Estratégica de Privacidade e Segurança da Informação

A transformação da cultura organizacional em relação à privacidade e segurança dos dados dos indivíduos envolve uma mudança nos valores, atitudes e comportamentos dentro da organização, com o objetivo de tornar a proteção de dados uma prioridade. Essa mudança tem como origem o reconhecimento de que a privacidade é um direito essencial e deve ser incorporado às operações diárias das empresas, especialmente com a criação de legislações como o GDPR e a LGPD, que impõem regras rigorosas para o processamento de dados particulares das pessoas (Dias, 2025).

# REVISTA TÓPICOS

---

Dessa forma, essa transformação exige não apenas mudanças nos processos internos, mas também um esforço de conscientização e treinamento para todos os colaboradores, no qual a cultura organizacional precisa abraçar a ideia de que a preservação de dados não é apenas uma questão legal, mas uma responsabilidade ética, o que afeta diretamente a confiança do consumidor e a imagem da organização (Dias, 2025). Nessa perspectiva, o desafio é integrar essas novas práticas de forma eficiente no cotidiano das operações e no comportamento dos funcionários.

Em vista disso, instituições como a Microsoft realizaram campanhas internas de treinamento e conscientização para garantir que seus colaboradores adotassem práticas de segurança de dados no dia a dia (Dias, 2025). Ademais, organizações que implementam processos de defesa dos dados dos indivíduos desde a fase de concepção de produtos (privacy by design) demonstram uma mudança cultural significativa em relação à privacidade, alinhada com as exigências do GDPR (Dias, 2025).

Outrossim, a gestão de riscos e auditorias internas envolve a identificação, avaliação e mitigação de riscos associados ao processamento dos dados das pessoas, garantindo que as entidades jurídicas cumpram as obrigações legais e minimizem os impactos de possíveis falhas de segurança (Dias, 2025). Dessa forma, a origem desses processos remonta aos exercícios de governança corporativa, que visam garantir a integridade dos dados e a transparência das operações, no qual a implementação da LGPD e do GDPR intensificou a necessidade de processos de auditoria mais rigorosos para monitorar a conformidade.

# REVISTA TÓPICOS

---

Ainda assim, a gestão de risco tornou-se um componente essencial na estratégia organizacional, principalmente em entidades jurídicas que lidam com grandes volumes de dados. Dessa forma, a auditoria interna é crucial para identificar e corrigir falhas no tratamento de dados antes que resultem em deliberações legais ou danos à comentários. Nesse sentido, o aumento da exigência de transparência e prestação de contas, tanto no Brasil quanto na União Europeia, exige que as empresas adotem uma abordagem mais proativa na identificação e mitigação de riscos (Dias, 2025).

À exemplo disso, muitas empresas agora realizam auditorias regulares para verificar se estão em conformidade com as exigências da LGPD e do GDPR, a fim de evitar multas (Rocha, 2025). Além do mais, instituições como a Amazon e a Apple desenvolveram relatórios internos de conformidade, que são frequentemente auditados para garantir que estejam cumprindo as regulamentações de proteção aos dados pessoais dos indivíduos (Rocha, 2025).

À vista disso, a conciliação entre defesa dos dados e inovação tecnológica envolve a busca por soluções que permitam o uso de tecnologias avançadas sem comprometer a segurança e privacidade dos dados pessoais. Dessa forma, a origem desse conceito está no desafio de equilibrar os avanços tecnológicos, como a inteligência artificial e a análise de grandes volumes de dados (big data), com as obrigações legais de proteção de dados impostos pela LGPD e pelo GDPR (Rocha, 2025).

Sendo assim, o crescimento da digitalização e da utilização de tecnologias disruptivas, como o machine learning e a análise preditiva, colocadas as

# REVISTA TÓPICOS

---

organizações frente a um dilema: como adotar essas tecnologias sem violar os direitos dos indivíduos e comprometer a segurança dos dados? (Rocha, 2025). Desse modo, a legislação de proteção de dados impõe restrições, mas também abre espaço para inovação, desde que as empresas adotem práticas específicas de proteção e governança.

Como por exemplo, empresas de tecnologia, como o Facebook e o Twitter, enfrentam desafios para equilibrar a inovação em seus produtos e serviços com a proteção dos dados dos usuários, especialmente no uso de dados pessoais para segmentação de anúncios (Rocha, 2025). E, também, startups de tecnologia podem implementar “privacy by design”, um conceito que integra a privacidade e a segurança dos dados diretamente no desenvolvimento de novos produtos e serviços, em conformidade com as normas legais (Rocha, 2025).

## 4 Considerações Finais

O objetivo geral deste trabalho foi analisar as instruções da LGPD e do GDPR, compreendendo suas implicações no cenário organizacional, especialmente no que se refere aos desafios enfrentados pelas instituições para se adequarem a essas normativas e às transformações operacionais geradas por elas. Dessa forma, este objetivo foi melhorado de maneira satisfatória, pois foi possível analisar as principais normas dessas legislações, evidenciando suas semelhanças, diferenças e os impactos práticos na gestão de dados dentro das organizações.

# REVISTA TÓPICOS

---

Desse modo, os principais resultados deste estudo incluem a compreensão dos desafios enfrentados pelas instituições para atender às exigências da LGPD e do GDPR, além das repercussões dessas regulamentações na gestão estratégica de privacidade e segurança da informação. Ademais, a pesquisa evidenciou que, embora as legislações apresentem alguns desafios, as organizações têm buscado se adaptar por meio da implementação de processos de compliance, políticas de privacidade robustas e uma maior conscientização sobre a importância da proteção de dados.

Nesse viés, a contribuição teórica deste trabalho reside na análise comparativa entre as legislações da preservação de dados brasileiras e europeias, oferecendo uma visão mais clara das implicações dessas normas para as organizações, especialmente no contexto brasileiro. Além do mais, o estudo contribui para a literatura ao abordar a adaptação organizacional em resposta a essas regulamentações, analisando como as empresas podem integrar a conformidade com a proteção de dados na sua estratégia de gestão da informação e segurança cibernética.

Assim sendo, não há limitações significativas em relação aos métodos adotados para a realização deste estudo. Nessa perspectiva, a pesquisa foi conduzida de maneira abrangente, utilizando fontes bibliográficas que permitiram uma reflexão sobre os impactos das regulamentações. Assim, os métodos qualitativos, com base em pesquisa bibliográfica, foram adequados para fornecer os resultados obtidos, sem que tenham restrições

# REVISTA TÓPICOS

---

metodológicas surgidas que comprometessem a análise e interpretação dos dados.

Para trabalhos futuros, sugere-se a realização de estudos empíricos que avaliam como as organizações de diferentes setores estão implementando as medidas previstas pela LGPD e o GDPR. Assim, a comparação entre instituições que já se adequaram a essas regulamentações e aquelas que ainda estão sem processo de adaptação pode trazer esclarecimentos sobre os desafios práticos enfrentados no dia a dia. Além disso, seria interessante explorar como essas normas impactam a confiança do consumidor e a competitividade das empresas no mercado global, um aspecto ainda pouco explorado em estudos anteriores.

## REFERÊNCIAS BIBLIOGRÁFICAS

Dias, J. H. Além dos Códigos: Inteligência Artificial, humanismo e habilidades essenciais para o advogado contemporâneo. São Paulo: Editora Dialética. 2025.

Lopes, B. P. Os efeitos da institucionalização de arquivos de escritoras no Brasil: análise de usos e usuários a partir da produção científica. 2023. 224 f., il. Tese (Doutorado em Ciência da Informação) — Universidade de Brasília, Brasília. 2023.

Oliveira, Y. M. de. Novas tecnologias de defesa cibernética na proteção da propriedade intelectual sob uma visão jurídica. 2023. 70 f. Dissertação

# REVISTA TÓPICOS

---

(Mestrado Profissional em Propriedade Intelectual e Transferência de Tecnologia para a Inovação) — Universidade de Brasília, Brasília. 2023.

Rocha, H. R. da. Regulação da inteligência artificial generativa e racismo algorítmico no reconhecimento facial. São Paulo: Editora Dialética. 2025.

<sup>1</sup> Docente de Deficiência Intelectual e TEA na SEDU. Doutorando em Ciências da Educação pela Facultad Interamericana de Ciencias Sociales.

E-mail: [freireskeven43@gmail.com](mailto:freireskeven43@gmail.com).

<sup>2</sup> Coordenador pedagógico da prefeitura municipal de Picos-PI. Mestre em Tecnologias Emergentes da Educação pela Must University. E-mail:

[micaelcamposdasilva@gmail.com](mailto:micaelcamposdasilva@gmail.com).