ISSN-2966-0785 REVISTA ACADÊMICA DA LUSOFONIA

OS DESAFIOS DA IMPLEMENTAÇÃO DA LGPD NA ADMINISTRAÇÃO PÚBLICA BRASILEIRA

The Challenges Of Implementing The LGPD In Brazilian Public Administration

Gisele dos Santos Rosa Chiovetti
Acadêmico do Curso Superior de Tecnologia em Gestão Pública do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia. – IFRO/ Campus Jaru-RO.
E-mail:giseledossantosrosa@gmail.com

Érik Serafim da Silva
Doutorando em Desenvolvimento e Meio Ambiente–PRODEMA/UFPB
Mestre em Ciências Agrárias(Agroecologia) – UFPB
Especialista emTutoria e Educação a Distância-UFMS
Especialista em Gestão Pública – FOCUS
Especialista em Educação Financeira–UFPB
Graduado em Gestão Pública – IFRO
E-mail:erik.silva@professor.pb.gov.br

RESUMO

A crescente digitalização dos serviços públicos brasileiros ampliou a coleta, o armazenamento e o compartilhamento de dados pessoais, tornando necessária a adoção de mecanismos capazes de garantir a proteção dessas informações. Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) estabeleceu diretrizes para o tratamento de dados por instituições públicas e privadas, visando assegurar os direitos fundamentais à privacidade e à proteção de dados pessoais. Este estudo teve como objetivo analisar os principais desafios enfrentados pela administração pública brasileira na implementação da LGPD, identificando as dificuldades estruturais, tecnológicas, organizacionais e culturais relacionadas à sua aplicação, bem como discutir o papel da Autoridade Nacional de Proteção de Dados (ANPD) nesse processo. A pesquisa caracteriza-se como qualitativa, exploratória e descritiva, desenvolvida por meio de revisão bibliográfica e documental, com análise de conteúdo baseada na proposta metodológica de Bardin (2016). Os resultados evidenciaram que, apesar dos avanços normativos promovidos pela LGPD e do reconhecimento constitucional da proteção de dados pessoais por meio da Emenda Constitucional nº 115/2022, persistem desafios relacionados à infraestrutura tecnológica, à capacitação dos servidores, à governança de dados e à consolidação de uma cultura institucional voltada à privacidade. Conclui-se que a efetiva implementação da LGPD na administração pública requer investimentos contínuos em tecnologia, qualificação profissional e mecanismos de governança, contribuindo não apenas para o cumprimento da legislação, mas também para o fortalecimento da transparência, da segurança da informação e da confiança da sociedade nas instituições públicas.

Palavras-chave: Lei Geral de Proteção de Dados; Administração Pública; Proteção de Dados Pessoais; Governança de Dados; ANPD.

ISSN-2966-0785 REVISTA ACADÊMICA DA LUSOFONIA

ABSTRACT

The increasing digitalization of Brazilian public services has expanded the collection, storage, and sharing of personal data, making it necessary to adopt mechanisms capable of ensuring the protection of such information. In this context, the Brazilian General Data Protection Law (LGPD – Law No. 13,709/2018) established guidelines for the processing of personal data by both public and private institutions, aiming to safeguard the fundamental rights to privacy and personal data protection. This study aimed to analyze the main challenges faced by the Brazilian Public Administration in implementing the LGPD, identifying the structural, technological, organizational, and cultural difficulties related to its application, as well as discussing the role of the National Data Protection Authority (ANPD) in this process. The research is characterized as qualitative, exploratory, and descriptive, developed through bibliographic and documentary review, using content analysis based on Bardin's (2016) methodological framework. The findings revealed that, despite the regulatory advances promoted by the LGPD and the constitutional recognition of personal data protection through Constitutional Amendment No. 115/2022, significant challenges remain regarding technological infrastructure, staff training, data governance, and the consolidation of an institutional culture focused on privacy. It is concluded that the effective implementation of the LGPD in the public sector requires continuous investment in technology, professional qualification, and governance mechanisms, contributing not only to legal compliance but also to strengthening transparency, information security, and public trust in governmental institutions.

Keywords: General Data Protection Law (LGPD); Public Administration; Personal Data Protection; Data Governance; National Data Protection Authority (ANPD).

1. INTRODUÇÃO

A crescente digitalização das informações no setor público brasileiro trouxe avanços significativos para a gestão administrativa, especialmente no que se refere à eficiência, à transparência e à ampliação do acesso aos serviços públicos. Contudo, esse processo também intensificou os desafios relacionados à proteção dos dados pessoais dos cidadãos, tornando indispensável a criação de mecanismos legais capazes de garantir maior segurança e privacidade das informações (BASTOS, 2024). Nesse contexto, foi instituída a Lei Geral de Proteção de Dados Pessoais (LGPD), considerada um importante marco regulatório para a proteção de dados no Brasil (BRASIL, 2018).

A LGPD tem como finalidade estabelecer normas para a coleta, o armazenamento, o compartilhamento e o tratamento de dados pessoais por instituições públicas e privadas. Inspirada em legislações internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation – GDPR*), a lei busca assegurar direitos fundamentais relacionados à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural (DONEDA, 2021; BIONI, 2021). Segundo esses autores, a

proteção de dados pessoais tornou-se essencial para a consolidação dos direitos fundamentais na sociedade da informação.

Apesar da relevância da legislação, a administração pública brasileira enfrenta diversos desafios para sua implementação efetiva. Os órgãos públicos lidam diariamente com uma grande quantidade de dados sensíveis, incluindo informações de saúde, educação, segurança pública, tributação e assistência social. O uso inadequado dessas informações pode causar prejuízos significativos à população, comprometendo direitos individuais e a confiança nas instituições públicas (PINHEIRO, 2023).

Nesse cenário, Di Pietro (2021) destaca que a administração pública contemporânea deve buscar o equilíbrio entre os princípios da eficiência administrativa e da transparência, sem negligenciar a proteção da privacidade dos cidadãos. Entretanto, muitos órgãos ainda enfrentam limitações estruturais para atender às exigências previstas pela LGPD.

Entre os principais obstáculos estão a insuficiência de investimentos em tecnologia da informação, a carência de servidores capacitados, a resistência organizacional às mudanças administrativas e a ausência de políticas internas de governança de dados. Conforme ressalta Pinheiro (2023), a cultura organizacional do setor público brasileiro ainda apresenta fragilidades no que diz respeito à gestão segura das informações, evidenciando a necessidade de modernização institucional e de adaptação dos processos administrativos.

Outro aspecto relevante refere-se à adequação dos procedimentos internos às exigências da LGPD. A implementação da legislação demanda a revisão de processos administrativos, o fortalecimento das políticas de segurança da informação e a criação de mecanismos eficazes de controle e fiscalização. Para Mendes (2020), a proteção de dados no setor público não depende apenas da existência de normas legais, mas também da capacidade administrativa do Estado para aplicá-las de forma eficiente e contínua.

Além disso, é necessário conciliar a proteção de dados pessoais com os princípios da transparência pública e do acesso à informação, garantidos pela Constituição Federal de 1988 e pela Lei de Acesso à Informação (LAI). Embora transparência e proteção de dados sejam princípios complementares, sua harmonização representa um dos principais desafios enfrentados pelos gestores públicos, uma vez que o dever de fornecer informações à sociedade deve coexistir com a obrigação de resguardar os dados pessoais dos cidadãos (DI PIETRO, 2021).

De acordo com Justen Filho (2018), a administração pública deve assegurar a publicidade dos atos administrativos sem comprometer os direitos individuais. Dessa forma,

observa-se que a implementação da LGPD ultrapassa questões meramente tecnológicas, envolvendo também aspectos jurídicos, administrativos, culturais e organizacionais. Trata-se de um processo que exige planejamento estratégico, capacitação contínua dos servidores e fortalecimento das políticas de governança digital. Nesse sentido, a adequação à legislação representa não apenas uma obrigação legal, mas também uma oportunidade de aprimorar a gestão pública, fortalecer a confiança da população nas instituições estatais e promover maior responsabilidade no tratamento dos dados pessoais.

A relevância do tema está associada não apenas à necessidade de cumprimento das exigências legais, mas também ao fortalecimento de uma cultura organizacional pautada na ética, na transparência e na responsabilidade no tratamento das informações. Diante desse contexto, surge a seguinte problemática de pesquisa: quais são os principais desafios enfrentados pela administração pública brasileira na implementação da LGPD e de que forma esses desafios impactam a gestão pública e os direitos dos cidadãos?

Para responder a essa questão, este trabalho tem como objetivo geral analisar os principais desafios da implementação da LGPD na administração pública brasileira, identificando as dificuldades enfrentadas pelos órgãos públicos e discutindo seus impactos na gestão pública contemporânea. Como objetivos específicos, busca-se: compreender o arcabouço legal da LGPD e sua aplicabilidade ao setor público; identificar os principais obstáculos estruturais, tecnológicos e culturais para a adequação dos órgãos públicos à legislação; e analisar a atuação da Autoridade Nacional de Proteção de Dados (ANPD) no acompanhamento e na fiscalização do cumprimento da LGPD no âmbito da administração pública.

2 REFERÊNCIAL TEÓRICO

2.1 PROTEÇÃO DE DADOS PESSOAIS: FUNDAMENTOS CONCEITUAIS E HISTÓRICOS

A proteção de dados pessoais passou a ganhar destaque a partir da segunda metade do século XX, sendo reconhecida como um elemento fundamental para a tutela dos direitos da personalidade na sociedade da informação. O avanço das tecnologias digitais e a crescente capacidade de coletar, armazenar e processar informações sobre os indivíduos criaram um cenário propício à violação da privacidade em larga escala, exigindo respostas normativas por parte dos Estados (BIONI, 2021; DONEDA, 2021).

Segundo Bioni (2021), a proteção de dados pessoais representa uma evolução do direito à privacidade, adaptada às características da era digital, marcada pela circulação acelerada de informações e pelo frequente desconhecimento dos titulares acerca da utilização de seus dados. Nesse sentido, o autor demonstra a transição do conceito clássico de privacidade, entendido como o direito de ser deixado em paz, conforme formulado por Warren e Brandeis (1890), para a concepção contemporânea de autodeterminação informativa, segundo a qual o indivíduo deve possuir controle sobre o fluxo e a utilização de suas informações pessoais.

No cenário internacional, a consolidação da proteção de dados teve como marco inicial a Convenção 108 do Conselho da Europa, de 1981, considerada o primeiro instrumento juridicamente vinculante voltado especificamente para a proteção de dados pessoais (DONEDA, 2021). Posteriormente, a Diretiva 95/46/CE da União Europeia estabeleceu parâmetros de proteção que influenciaram diversas legislações ao redor do mundo (BIONI, 2021). Esse processo atingiu seu ponto mais significativo com a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation – GDPR*), em maio de 2018, que se tornou referência internacional na regulamentação da privacidade e da proteção de dados pessoais (BIONI, 2021).

No Brasil, a proteção de dados pessoais desenvolveu-se de forma fragmentada durante muitos anos, sem a existência de uma legislação específica que disciplinasse a matéria de maneira integrada. Normas como o Código de Defesa do Consumidor, a Lei do Habeas Data, a Lei do Cadastro Positivo e a Lei de Acesso à Informação tratavam de aspectos relacionados ao tema, porém sem estabelecer um regime jurídico unificado. Essa lacuna foi superada com a promulgação da Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), que inaugurou uma nova fase na proteção da privacidade e dos dados pessoais no ordenamento jurídico brasileiro (PINHEIRO, 2023).

De acordo com Doneda (2021), a proteção de dados no ambiente organizacional não deve ser compreendida apenas como uma obrigação legal, mas também como uma expressão da responsabilidade institucional. No âmbito da contabilidade e do Departamento Pessoal, essa preocupação assume especial relevância em razão do tratamento contínuo de informações sensíveis, como dados bancários, fiscais, trabalhistas e de saúde dos colaboradores.

Nesse contexto, a adequação à LGPD exige a adoção de medidas de segurança da informação, o mapeamento dos fluxos de tratamento de dados e a observância dos princípios da finalidade, necessidade e segurança previstos na legislação. A ausência dessas práticas pode resultar em sanções administrativas, responsabilização civil e outras penalidades aplicáveis.

Além disso, o autor ressalta que a legislação demanda uma postura proativa dos agentes responsáveis pelo tratamento dos dados, tornando os profissionais da contabilidade e do Departamento Pessoal atores fundamentais na proteção da privacidade e na garantia da conformidade legal das organizações.

A relevância constitucional do tema foi reforçada pela Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que incluiu expressamente a proteção de dados pessoais, inclusive nos meios digitais, no rol dos direitos e garantias fundamentais previstos no artigo 5º da Constituição Federal. A mesma emenda também atribuiu à União a competência privativa para legislar sobre a matéria. Conforme destacam Frazão, Tepedino e Oliva (2019, p. 42), essa constitucionalização "representa o reconhecimento de que a proteção de dados é condição indispensável para o livre desenvolvimento da personalidade e para o exercício pleno da cidadania no ambiente digital".

2.2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): ESTRUTURA E PRINCÍPIOS

A Lei Geral de Proteção de Dados (LGPD) é fundamentada em um conjunto de princípios que orientam todas as atividades relacionadas ao tratamento de dados pessoais, aplicáveis tanto às organizações privadas quanto aos órgãos da administração pública. O artigo 6º da legislação estabelece dez princípios fundamentais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Em conjunto, esses princípios constituem um sistema de diretrizes destinado a assegurar que o tratamento de dados ocorra de forma legítima, proporcional e em conformidade com os direitos dos titulares (BRASIL, 2018).

Entre esses princípios, destaca-se o da finalidade, segundo o qual os dados pessoais somente podem ser tratados para objetivos legítimos, específicos, explícitos e previamente informados ao titular, sendo vedado o uso posterior incompatível com as finalidades originalmente estabelecidas. Complementarmente, o princípio da necessidade determina que o tratamento deve se restringir ao mínimo de dados indispensáveis para o alcance dos objetivos pretendidos, correspondendo ao que a literatura especializada denomina de princípio da minimização de dados (BIONI, 2021).

Esses princípios exercem papel central na aplicação prática da LGPD, servindo como parâmetros para a interpretação e execução das atividades de tratamento de dados. Nesse sentido, Cots e Oliveira (2019, p. 57) destacam que:

> "Os princípios da LGPD não devem ser compreendidos como meras diretrizes programáticas, mas como normas jurídicas de eficácia plena, diretamente aplicáveis às operações de tratamento de dados. Sua inobservância configura violação legal passível de sanção administrativa pela Autoridade Nacional de Proteção de Dados, independentemente da ocorrência de dano concreto ao titular."

A Lei Geral de Proteção de Dados (LGPD) distingue duas categorias de dados pessoais, cada uma submetida a regimes jurídicos específicos. A primeira refere-se aos dados pessoais comuns, definidos como qualquer informação relacionada a uma pessoa natural identificada ou identificável (art. 5º, I). A segunda compreende os dados pessoais sensíveis, que incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde ou à vida sexual, além de dados genéticos e biométricos (art. 5º, II). Em razão do potencial discriminatório e dos riscos decorrentes de sua exposição, o tratamento dos dados sensíveis está sujeito a critérios mais rigorosos de proteção e controle (BRASIL, 2018).

Além de classificar os dados pessoais, a LGPD estabelece as bases legais que autorizam seu tratamento. No âmbito do setor público, destacam-se o cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II), a execução de políticas públicas previstas em leis e regulamentos (art. 7º, III) e a tutela da saúde em procedimentos realizados por profissionais da área ou por entidades sanitárias (art. 7º, VIII). Essas hipóteses permitem que os órgãos públicos realizem o tratamento de dados necessário ao desempenho de suas funções institucionais. Contudo, essa autorização não os exime da observância dos princípios, direitos e garantias previstos na legislação, devendo o tratamento ocorrer de forma transparente, segura e compatível com as finalidades estabelecidas pela LGPD (BRASIL, 2018).

2.3 A LGPD E A ADMINISTRAÇÃO PÚBLICA: ESPECIFICIDADES E OBRIGAÇÕES

A aplicação da Lei Geral de Proteção de Dados (LGPD) à administração pública apresenta características próprias que a diferenciam do regime adotado pelo setor privado. O Capítulo IV da legislação, dedicado ao tratamento de dados pessoais pelo poder público,

estabelece regras específicas que consideram as particularidades da atuação estatal, ao mesmo tempo em que impõem deveres relacionados à responsabilidade, à transparência e à proteção dos direitos dos cidadãos. Nesse sentido, o artigo 23 determina que o tratamento de dados pessoais por pessoas jurídicas de direito público deve ocorrer para o atendimento de finalidade pública, na persecução do interesse público e na execução das competências legais ou das atribuições dos serviços públicos (BRASIL, 2018).

A previsão legal demonstra que o tratamento de dados pelo Estado não possui caráter discricionário, mas está diretamente vinculado às funções institucionais atribuídas aos órgãos públicos. Dessa forma, a utilização das informações pessoais deve observar critérios de legalidade, necessidade e adequação, garantindo que os dados sejam empregados exclusivamente para o cumprimento das atividades administrativas e para a promoção do interesse coletivo.

Segundo Pinheiro (2023, p. 115), a aplicação da LGPD ao setor público apresenta desafios significativos, uma vez que "a administração pública opera em um ambiente de tensão permanente entre os princípios da publicidade e da transparência, que impõem a divulgação dos atos estatais, e os direitos de privacidade dos cidadãos cujos dados são tratados no exercício das funções governamentais". Tal realidade exige dos gestores públicos uma interpretação cuidadosa da legislação, capaz de harmonizar valores constitucionais igualmente relevantes, mas que, em determinadas situações, podem entrar em conflito.

Nesse contexto, a relação entre a LGPD e a Lei de Acesso à Informação (LAI – Lei nº 12.527/2011) constitui um dos temas mais complexos da gestão pública contemporânea. Enquanto a LAI busca ampliar a transparência e o acesso às informações produzidas pelo Estado, a LGPD estabelece limites para a divulgação de dados pessoais, exigindo que a administração pública encontre mecanismos que conciliem o direito à informação com a proteção da privacidade dos cidadãos (DI PIETRO, 2021).

Além disso, a transformação digital dos serviços públicos ampliou consideravelmente o volume de dados tratados pelos órgãos governamentais. Sistemas eletrônicos de saúde, educação, assistência social, segurança pública e arrecadação tributária passaram a concentrar grandes quantidades de informações pessoais, aumentando a necessidade de medidas eficazes de segurança da informação e de mecanismos de controle sobre o acesso e o compartilhamento desses dados. Nesse cenário, a conformidade com a LGPD tornou-se um requisito essencial para a modernização da administração pública e para o fortalecimento da confiança da população nas instituições estatais.

A LGPD também estabelece obrigações específicas para os agentes de tratamento de dados no setor público. Entre elas, destacam-se a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), sempre que as operações de tratamento apresentarem riscos aos direitos e às liberdades dos titulares (art. 38); a comunicação de incidentes de segurança à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados (art. 48); e a designação do Encarregado pelo Tratamento de Dados Pessoais, profissional responsável por atuar como canal de comunicação entre o controlador, os titulares e a ANPD (art. 41) (BRASIL, 2018; DI PIETRO, 2021). O cumprimento dessas obrigações é fundamental para a construção de uma governança de dados eficiente e responsável no âmbito da administração pública (BIONI, 2021).

Outro aspecto relevante refere-se à necessidade de capacitação contínua dos servidores públicos para o correto tratamento das informações pessoais. A efetividade da LGPD não depende apenas da existência de normas e procedimentos internos, mas também da conscientização dos agentes públicos sobre suas responsabilidades e sobre os riscos decorrentes do uso inadequado dos dados. Dessa forma, programas de treinamento e ações de educação institucional tornam-se instrumentos indispensáveis para a consolidação de uma cultura de proteção de dados no setor público.

Sobre o papel estratégico do Encarregado pelo Tratamento de Dados Pessoais, Mendes (2020, p. 89) afirma que essa função representa um avanço significativo na governança da privacidade. No contexto da administração pública, o Encarregado não apenas orienta o órgão quanto ao cumprimento das disposições da LGPD, mas também atua como garantidor dos direitos dos cidadãos cujos dados são tratados pelo Estado, contribuindo para o fortalecimento da transparência, da responsabilidade administrativa e da *accountability* governamental.

2.4 A LGPD NA ADMINISTRAÇÃO PÚBLICA: DESAFIOS, AVANÇOS E O PAPEL DA ANPD

A aplicação da Lei Geral de Proteção de Dados (LGPD) no setor público apresenta particularidades que a diferenciam do regime adotado pelas organizações privadas. Enquanto, no setor privado, o tratamento de dados pessoais frequentemente se fundamenta no consentimento do titular, na administração pública esse tratamento ocorre, em grande parte, para o cumprimento de obrigações legais ou para a execução de políticas públicas previstas em lei, conforme estabelecido pela própria LGPD (BRASIL, 2018). Ainda assim, os órgãos

públicos devem observar os princípios previstos na legislação, especialmente os da finalidade, necessidade, adequação e transparência, garantindo que os dados pessoais sejam utilizados de forma legítima e compatível com o interesse público.

Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha papel fundamental na implementação e fiscalização da LGPD. Criada pela Lei nº 13.709/2018, a ANPD é responsável por elaborar diretrizes, orientar os agentes de tratamento, fiscalizar o cumprimento da legislação e aplicar sanções em casos de descumprimento. Além disso, o órgão atua na promoção de ações educativas e na disseminação de boas práticas relacionadas à proteção de dados pessoais (ANPD, 2023).

Segundo Tepedino e Teffé (2023), a atuação da ANPD tem sido pautada, inicialmente, por uma abordagem orientativa e pedagógica. Nos primeiros anos de vigência da LGPD, o foco principal esteve voltado para a conscientização dos órgãos públicos e das instituições quanto às exigências da legislação, buscando promover a adequação gradual antes da aplicação de medidas sancionatórias mais rigorosas.

Apesar dos avanços observados desde a entrada em vigor da LGPD, muitos órgãos públicos brasileiros ainda enfrentam dificuldades para alcançar plena conformidade com a legislação. Estudo realizado pela Escola Nacional de Administração Pública (ENAP, 2024) identificou que diversos ministérios e autarquias federais ainda não concluíram o mapeamento dos dados pessoais sob sua responsabilidade, etapa considerada essencial para a implementação efetiva da política de proteção de dados. Entre os principais desafios identificados destacam-se a escassez de profissionais especializados, a insuficiência de investimentos em segurança da informação e a ausência de políticas internas de governança de dados.

Por outro lado, observa-se que diversos estados e municípios vêm adotando iniciativas voltadas ao fortalecimento da proteção de dados no âmbito da administração pública. Entre essas medidas estão a criação de programas de adequação à LGPD, a regulamentação de procedimentos internos e a formação de comitês de governança digital responsáveis por acompanhar e orientar as ações relacionadas ao tratamento de dados pessoais.

De acordo com Magalhães (2023), a cooperação entre os órgãos públicos e a ANPD é indispensável para garantir uma aplicação uniforme da LGPD em todo o território nacional. Essa articulação contribui para reduzir desigualdades entre os diferentes entes federativos e promover maior segurança jurídica na implementação da legislação.

Costa e Altoé (2025) destacam que a efetividade da proteção de dados depende da adoção de medidas concretas de governança, como o registro das operações de tratamento, a

definição clara de responsabilidades, a realização de treinamentos periódicos e o controle de acesso às informações. Os autores também ressaltam a necessidade de revisão de práticas administrativas inadequadas, como o armazenamento indiscriminado de documentos, o compartilhamento inseguro de informações e a ausência de políticas de retenção e descarte de dados. Tais condutas podem aumentar significativamente os riscos de incidentes de segurança e de responsabilização dos órgãos públicos.

Peiter *et al.* (2022) afirmam que a conformidade com a LGPD produz benefícios que vão além da prevenção de sanções legais. Em um contexto marcado pela crescente exigência por transparência, ética e responsabilidade na gestão pública, a demonstração de compromisso com a proteção dos dados pessoais fortalece a confiança da sociedade nas instituições governamentais. Dessa forma, a implementação da LGPD não deve ser compreendida apenas como uma obrigação normativa, mas como uma oportunidade de aperfeiçoar os processos administrativos, fortalecer a governança pública e promover uma cultura organizacional voltada à proteção dos direitos dos cidadãos.

Assim, a aplicabilidade da LGPD na administração pública ultrapassa o simples cumprimento da legislação, representando um processo contínuo de transformação institucional que envolve mudanças culturais, capacitação dos servidores, modernização tecnológica e fortalecimento das práticas de governança e transparência.

2.5 IMPLEMENTAÇÃO DA LGPD NA ADMINISTRAÇÃO PÚBLICA

A implementação da Lei Geral de Proteção de Dados (LGPD) na administração pública exige mais do que o simples cumprimento de exigências legais. Trata-se de um processo contínuo que demanda mudanças na cultura organizacional, na forma de gestão das informações e nos procedimentos adotados pelos órgãos públicos. Para que a adequação à legislação seja efetiva, é necessário integrar ações de planejamento, capacitação de servidores, investimentos em tecnologia e mecanismos permanentes de monitoramento e avaliação (PINHEIRO, 2023).

Uma das etapas iniciais desse processo consiste no mapeamento dos dados pessoais tratados pela instituição. Esse procedimento permite identificar quais informações são coletadas, onde estão armazenadas, quem possui acesso a elas e quais são as finalidades de sua utilização. De acordo com Bioni (2021), o conhecimento detalhado do fluxo dos dados é fundamental para a identificação de riscos e para a definição de medidas adequadas de proteção e controle.

Outro aspecto relevante refere-se à elaboração de políticas internas voltadas à proteção de dados e à segurança da informação. Essas políticas devem estabelecer diretrizes claras sobre coleta, armazenamento, compartilhamento, acesso e descarte de dados pessoais, além de definir responsabilidades para servidores e gestores envolvidos no tratamento dessas informações. A existência de regras bem estruturadas contribui para a redução de falhas operacionais e fortalece a segurança dos processos administrativos (MENDES, 2020; MINGHELLI, 2024).

A capacitação dos servidores públicos também desempenha papel essencial no processo de adequação à LGPD. Em muitos órgãos, os profissionais responsáveis pelo tratamento de dados não possuem formação específica na área, o que torna indispensável a realização de treinamentos e ações de conscientização. Conforme destaca Mendes (2020), a disseminação de boas práticas relacionadas à privacidade e à segurança da informação é um dos fatores mais importantes para o sucesso da implementação da legislação, contribuindo para a construção de uma cultura institucional comprometida com a proteção dos dados pessoais.

Além das medidas organizacionais, os órgãos públicos precisam investir em recursos tecnológicos capazes de fortalecer a segurança das informações. Ferramentas como controle de acesso, autenticação de usuários, criptografia, cópias de segurança e monitoramento contínuo dos sistemas representam mecanismos importantes para prevenir incidentes de segurança e acessos não autorizados. A adoção dessas soluções reduz vulnerabilidades e amplia a capacidade de resposta das instituições diante de possíveis riscos (PINHEIRO, 2023).

Outro elemento fundamental nesse processo é a atuação do Encarregado pelo Tratamento de Dados Pessoais, também conhecido como *Data Protection Officer (DPO)*. Esse profissional é responsável por orientar a instituição quanto ao cumprimento da LGPD, atuar como canal de comunicação entre os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), além de acompanhar a implementação das medidas de conformidade adotadas pelo órgão. Sua atuação contribui para o fortalecimento da governança de dados e para a efetividade das ações de proteção da privacidade no setor público (BRASIL, 2018; PINHEIRO, 2023).

Também merece destaque a necessidade de integrar a proteção de dados aos processos de gestão pública. A adequação à LGPD não deve ser tratada como uma atividade isolada ou restrita aos setores de tecnologia da informação, mas como uma responsabilidade compartilhada por toda a instituição. Nesse sentido, a participação da alta administração é indispensável para garantir recursos, definir prioridades e promover uma cultura organizacional voltada à proteção dos direitos dos cidadãos.

Por fim, a adequação à LGPD deve ser compreendida como um processo permanente de aperfeiçoamento institucional. A realização de auditorias, avaliações periódicas de riscos e revisões constantes dos procedimentos internos permite que os órgãos públicos acompanhem as mudanças tecnológicas e regulatórias, mantendo elevados padrões de proteção de dados. Dessa forma, a implementação da LGPD contribui não apenas para o cumprimento da legislação, mas também para o fortalecimento da transparência, da eficiência administrativa e da confiança da sociedade nos serviços públicos oferecidos pelo Estado (ANPD, 2023; PINHEIRO, 2023).

2.6 A CONVERGÊNCIA ENTRE O ARCABOUÇO LEGAL E A VULNERABILIDADE COMPORTAMENTAL NA GOVERNANÇA DE DADOS

A construção de um ambiente digital seguro exige das organizações uma postura que vai além do simples cumprimento das obrigações legais. Mais do que atender às exigências normativas, é necessário compreender como a legislação se aplica às atividades cotidianas e de que forma pode ser incorporada à cultura organizacional. Nesse contexto, Melo (2026) destaca que a Lei Geral de Proteção de Dados (LGPD) foi fortemente inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), compartilhando princípios fundamentais, como a definição de bases legais para o tratamento de dados e a garantia de direitos aos titulares das informações.

Apesar das semelhanças entre os dois modelos regulatórios, o autor observa que a realidade brasileira ainda enfrenta desafios significativos para alcançar níveis mais elevados de maturidade em proteção de dados. Entre esses obstáculos estão a consolidação da atuação da Autoridade Nacional de Proteção de Dados (ANPD), a necessidade de fortalecimento das práticas de governança e a resistência de muitas organizações em incorporar rotinas efetivas de conformidade. Em comparação com o cenário europeu, onde a cultura de proteção de dados se encontra mais consolidada, o Brasil ainda passa por um processo gradual de adaptação e amadurecimento institucional (MELO, 2026).

Essa distância entre a previsão legal e sua efetiva aplicação torna-se ainda mais evidente quando analisada sob a perspectiva da gestão organizacional. Ferreira (2026) argumenta que investimentos em tecnologias avançadas e em instrumentos jurídicos bem estruturados não são suficientes para garantir a proteção das informações. Segundo o autor, o comportamento

humano continua sendo um dos principais fatores de vulnerabilidade nos sistemas de segurança da informação.

Mesmo diante de recursos tecnológicos sofisticados, como sistemas de criptografia, autenticação multifator e *firewalls*, incidentes podem ocorrer em razão de falhas humanas. Situações como o compartilhamento indevido de informações, o uso inadequado de senhas ou a abertura de mensagens fraudulentas demonstram que a segurança da informação depende diretamente do nível de conscientização dos colaboradores. Nesse sentido, ataques de engenharia social, especialmente os golpes de *phishing*, continuam figurando entre as principais causas de vazamentos e comprometimento de dados (FERREIRA, 2026).

Outro aspecto relevante refere-se à necessidade de promover uma cultura organizacional voltada à proteção de dados. A conformidade com a LGPD não pode ser tratada como uma responsabilidade exclusiva dos setores jurídicos ou de tecnologia da informação. Pelo contrário, a proteção de dados deve envolver todos os níveis da organização, desde a alta administração até os colaboradores que lidam diretamente com informações pessoais em suas atividades diárias. A criação dessa cultura depende de ações permanentes de conscientização, treinamentos periódicos e do fortalecimento das práticas de governança corporativa.

Além disso, a adoção de programas de educação digital contribui para reduzir riscos operacionais e fortalecer a capacidade de resposta das organizações diante de incidentes de segurança. Quando os colaboradores compreendem a importância da proteção de dados e conhecem os procedimentos adequados para o tratamento das informações, tornam-se agentes ativos na prevenção de falhas e na promoção da conformidade legal.

As reflexões de Melo (2026) e Ferreira (2026) convergem para um ponto essencial: a efetividade da LGPD depende não apenas da existência de normas e tecnologias, mas também da transformação dos comportamentos organizacionais. A maturidade desejada para o sistema brasileiro de proteção de dados somente será alcançada quando as instituições reconhecerem que a segurança da informação é uma responsabilidade compartilhada e contínua.

Sob a perspectiva jurídica, um incidente causado por erro humano não afasta a responsabilidade da organização perante a legislação. Ao contrário, falhas decorrentes da ausência de treinamento, supervisão ou controle adequado podem resultar em sanções administrativas, danos reputacionais e responsabilização perante os órgãos competentes. Dessa forma, a proteção de dados deve ser entendida como um processo estratégico que integra aspectos tecnológicos, jurídicos e humanos.

Em síntese, para que o modelo de proteção de dados inspirado no GDPR alcance resultados efetivos no contexto brasileiro, é fundamental que as organizações deixem de encarar a LGPD como uma mera obrigação burocrática. A consolidação de uma cultura de privacidade, aliada à capacitação contínua dos colaboradores e ao fortalecimento das práticas de governança, representa um dos caminhos mais eficazes para garantir a segurança das informações e a proteção dos direitos dos titulares de dados na era digital.

3 METODOLOGIA

O presente estudo caracteriza-se como uma pesquisa de abordagem qualitativa, de natureza exploratória e descritiva, desenvolvida por meio de revisão bibliográfica e análise documental. A escolha da abordagem qualitativa justifica-se pela necessidade de compreender os aspectos jurídicos, administrativos e institucionais relacionados à implementação da Lei Geral de Proteção de Dados (LGPD) no âmbito da Administração Pública. Segundo Minayo (2016), a pesquisa qualitativa possibilita a análise de fenômenos complexos a partir de seus significados, contextos e relações sociais, contribuindo para uma compreensão mais aprofundada da realidade estudada.

A pesquisa bibliográfica foi realizada mediante consulta às bases de dados *Scientific Electronic Library Online (SciELO)*, *Google Acadêmico* e Portal de Periódicos da CAPES. Para a busca dos materiais, foram utilizados os descritores “LGPD”, “proteção de dados pessoais”, “administração pública”, “governança de dados” e “Autoridade Nacional de Proteção de Dados (ANPD)”, empregados de forma isolada e combinada. O levantamento contemplou artigos científicos, livros, dissertações, teses e demais publicações acadêmicas relacionadas ao tema.

Como critério temporal, foram selecionadas obras publicadas entre os anos de 2018 e 2026, período correspondente à promulgação e consolidação da Lei Geral de Proteção de Dados no Brasil. Foi dada prioridade às produções mais recentes, especialmente aquelas publicadas a partir de 2023, em razão das atualizações normativas, dos avanços institucionais e da ampliação dos estudos voltados à aplicação da LGPD no setor público.

A análise documental concentrou-se na legislação e nos atos normativos relacionados à proteção de dados pessoais no ordenamento jurídico brasileiro. Foram examinados, principalmente, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), a Emenda Constitucional nº 115/2022, que reconheceu a proteção de dados pessoais como direito

fundamental, bem como regulamentos, guias e orientações emitidos pela Autoridade Nacional de Proteção de Dados (ANPD).

Para a interpretação dos dados, utilizou-se a técnica de análise de conteúdo proposta por Bardin (2016), desenvolvida em três etapas: pré-análise, exploração do material e tratamento dos resultados. Inicialmente, realizou-se a leitura exploratória das fontes selecionadas, seguida da organização e categorização das informações consideradas relevantes para o estudo. Posteriormente, os dados foram analisados de forma crítica e sistemática, possibilitando a identificação dos principais desafios, avanços e perspectivas relacionados à implementação da LGPD na Administração Pública brasileira.

A partir desse procedimento metodológico, foi possível reunir e interpretar contribuições teóricas e normativas sobre a proteção de dados pessoais no setor público, fornecendo subsídios para a análise e discussão dos resultados apresentados ao longo deste trabalho.

4 RESULTADOS E DISCUSSÃO

A análise da literatura permitiu identificar que a implementação da Lei Geral de Proteção de Dados (LGPD) na administração pública brasileira ainda se encontra em processo de consolidação. Embora a legislação esteja em vigor desde 2020, os estudos analisados demonstram que grande parte dos órgãos públicos enfrenta dificuldades para adequar suas estruturas, procedimentos e práticas administrativas às exigências previstas na norma (PINHEIRO, 2023).

Entre os desafios mais recorrentes apontados pelos autores, destacam-se as limitações estruturais e tecnológicas presentes em diversas instituições públicas. Muitos órgãos ainda utilizam sistemas informatizados desenvolvidos antes da vigência da LGPD, sem mecanismos adequados de controle, rastreabilidade e proteção das informações pessoais. Além disso, a fragmentação dos bancos de dados e a falta de integração entre sistemas dificultam a gestão eficiente das informações e aumentam a exposição a riscos de vazamentos e incidentes de segurança (TEPEDINO; TEFFÉ, 2023).

Outro aspecto amplamente discutido na literatura refere-se à capacitação dos servidores públicos. A implementação da LGPD exige conhecimentos relacionados à proteção de dados, segurança da informação, gestão de riscos e governança digital. No entanto, os estudos indicam que muitos profissionais ainda não receberam treinamento suficiente para desempenhar suas

funções em conformidade com as novas exigências legais. Essa realidade evidencia que a adequação à legislação depende não apenas de investimentos em tecnologia, mas também da qualificação contínua dos agentes públicos responsáveis pelo tratamento dos dados (MENDES, 2020).

Os resultados também demonstram que a principal barreira à implementação da LGPD não está restrita aos aspectos técnicos ou jurídicos, mas envolve mudanças culturais dentro das organizações públicas. Durante décadas, a gestão de dados esteve associada principalmente à eficiência administrativa e à prestação de serviços, sem que a proteção da privacidade ocupasse posição central nas decisões institucionais. Nesse contexto, a LGPD introduziu uma nova lógica de atuação, exigindo que os órgãos públicos incorporem a proteção de dados como elemento permanente de suas atividades. Conforme destaca Bioni (2021), a criação de uma cultura de proteção de dados constitui um dos maiores desafios para a efetivação da legislação no Brasil.

A pesquisa também revelou a existência de um descompasso entre o reconhecimento da importância da LGPD e sua aplicação prática no cotidiano da administração pública. Ribeiro e Moreira (2021) observam que, embora gestores e servidores demonstrem compreender a relevância da proteção de dados pessoais, essa percepção nem sempre se traduz em ações concretas de adequação. Em muitos casos, a implementação ocorre de forma parcial, limitada por restrições orçamentárias, ausência de planejamento estratégico e dificuldades na definição de responsabilidades internas.

No que se refere à atuação institucional, verificou-se que a Autoridade Nacional de Proteção de Dados (ANPD) tem desempenhado papel fundamental no processo de implementação da LGPD. A publicação de guias orientativos, notas técnicas, regulamentos e recomendações tem contribuído para reduzir inseguranças jurídicas e oferecer parâmetros para a atuação dos órgãos públicos. Esse trabalho tem sido particularmente relevante para instituições que ainda se encontram em estágios iniciais de adequação, fornecendo orientações práticas para o desenvolvimento de programas de governança em privacidade e proteção de dados (ANPD, 2023).

Apesar das dificuldades identificadas, os resultados também evidenciam avanços importantes. Diversos órgãos públicos já iniciaram processos de mapeamento de dados pessoais, elaboração de inventários de tratamento, criação de políticas internas de proteção de dados e designação de encarregados pelo tratamento de dados pessoais. Embora essas iniciativas ocorram em ritmos distintos entre os diferentes entes federativos, elas demonstram

que a temática vem conquistando espaço crescente na agenda da gestão pública brasileira (MAGALHÃES, 2023).

Outro resultado relevante refere-se à necessidade de fortalecimento das práticas de governança de dados. Conforme destacam Pimenta e Medeiros (2025), setores tradicionalmente vistos como operacionais devem assumir papel estratégico na proteção das informações institucionais. A gestão adequada dos dados pessoais exige integração entre diferentes áreas administrativas, definição clara de responsabilidades e adoção de mecanismos permanentes de controle, monitoramento e avaliação.

Os estudos analisados também indicam que a adequação à LGPD não deve ser compreendida como um objetivo a ser alcançado em curto prazo, mas como um processo contínuo de aperfeiçoamento institucional. Nesse sentido, Dorigo (2024) e Doneda (2021) ressaltam que a implementação da legislação deve considerar as particularidades de cada organização, priorizando inicialmente os setores e processos que apresentam maior risco para os titulares dos dados. Essa abordagem gradual tende a produzir resultados mais consistentes e compatíveis com a realidade dos órgãos públicos.

Diante dos resultados obtidos, observa-se que a efetivação da LGPD na administração pública depende da articulação entre diferentes fatores, incluindo investimentos em infraestrutura tecnológica, capacitação dos servidores, fortalecimento da governança de dados e comprometimento da alta gestão. Mais do que uma obrigação legal, a proteção de dados pessoais representa um instrumento de qualificação da gestão pública, contribuindo para a ampliação da transparência, da segurança da informação e da confiança da sociedade nas instituições estatais. Dessa forma, os desafios identificados não devem ser interpretados apenas como obstáculos, mas também como oportunidades para a modernização administrativa e para o fortalecimento dos direitos fundamentais dos cidadãos na sociedade digital.

7. CONCLUSÃO

O presente estudo teve como objetivo analisar os principais desafios da implementação da Lei Geral de Proteção de Dados (LGPD) na administração pública brasileira, identificando as dificuldades enfrentadas pelos órgãos públicos e discutindo seus impactos na gestão pública contemporânea. A partir da revisão bibliográfica e documental realizada, constatou-se que a adequação à LGPD constitui um processo complexo, que ultrapassa a mera observância das

disposições legais e envolve mudanças estruturais, tecnológicas, administrativas e culturais no âmbito das instituições públicas.

Os resultados evidenciaram que, embora a legislação represente um importante avanço na proteção dos direitos fundamentais relacionados à privacidade e à autodeterminação informativa, sua efetiva implementação ainda encontra obstáculos significativos. Entre os principais desafios identificados destacam-se a utilização de sistemas tecnológicos obsoletos, a insuficiência de investimentos em segurança da informação, a escassez de profissionais qualificados, a ausência de políticas consolidadas de governança de dados e as dificuldades de integração entre os diversos setores da administração pública. Tais fatores demonstram que a conformidade com a LGPD exige esforços contínuos de modernização institucional e fortalecimento da capacidade administrativa do Estado.

Outro aspecto relevante observado ao longo da pesquisa refere-se à necessidade de transformação da cultura organizacional dos órgãos públicos. A proteção de dados pessoais não pode ser tratada apenas como uma exigência jurídica ou uma atribuição exclusiva dos setores de tecnologia da informação. Pelo contrário, trata-se de uma responsabilidade compartilhada que deve envolver gestores, servidores e demais agentes públicos, demandando ações permanentes de capacitação, conscientização e desenvolvimento de boas práticas voltadas à privacidade e à segurança da informação.

Verificou-se, ainda, a importância da atuação da Autoridade Nacional de Proteção de Dados (ANPD) no processo de implementação da legislação. Por meio da elaboração de orientações, regulamentos e instrumentos de apoio à adequação, a Autoridade tem contribuído para a consolidação de uma cultura de proteção de dados no setor público. Contudo, os resultados também demonstram que persistem diferenças significativas entre os níveis federal, estadual e municipal quanto ao grau de maturidade das iniciativas de conformidade, evidenciando a necessidade de maior articulação institucional e cooperação entre os entes federativos.

A pesquisa permitiu concluir que a efetivação da LGPD na administração pública depende da adoção de uma abordagem integrada, capaz de reunir investimentos em infraestrutura tecnológica, fortalecimento da governança de dados, qualificação dos servidores e comprometimento da alta gestão. Nesse sentido, a proteção de dados deve ser compreendida como elemento estratégico para a modernização administrativa e para o aprimoramento da prestação dos serviços públicos.

Por fim, conclui-se que a LGPD representa uma oportunidade de fortalecimento da relação entre Estado e sociedade, ao promover maior segurança jurídica, transparência e respeito aos direitos dos cidadãos no ambiente digital. Mais do que atender a uma obrigação normativa, sua implementação contribui para o desenvolvimento de uma administração pública mais eficiente, responsável e alinhada aos princípios democráticos que orientam a atuação estatal. Dessa forma, a consolidação da cultura de proteção de dados no setor público configura-se como um dos desafios centrais da gestão pública contemporânea, exigindo esforços contínuos para garantir a efetividade dos direitos fundamentais na era da informação.

Como sugestão para pesquisas futuras, recomenda-se a realização de estudos empíricos em órgãos públicos de diferentes esferas administrativas, a fim de avaliar o estágio de adequação à LGPD e identificar boas práticas capazes de subsidiar a formulação de estratégias mais eficazes para a proteção de dados pessoais no setor público brasileiro.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Portal institucional.** Brasília, 2026. Disponível em: https://www.gov.br/anpd. Acesso em: 05 mai. 2026.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2016.

BASTOS, E. B. **A Lei geral de proteção de dados pessoais nas relações de trabalho especialmente na fase pré-contratual.** Revista do Tribunal Superior do Trabalho, v. 90, n. 2, 2024. Disponível em: https://revista.tst.jus.br/rtst/article/view/69. Acesso em: 20 jun. 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 08 mai. 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir os direitos de proteção de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 01 de mai. 2026.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Lei de Acesso à Informação. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 05 mai. 2026.

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: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 de mai. 2026.

COSTA, M. P.; ALTOÉ, S. M. L. **Conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD):** uma análise dos determinantes junto aos profissionais de contabilidade. Revista Catarinense da Ciência Contábil, v. 24, n. 5 e3552, 2025. Disponível em: https://doi.org/10.16930/2237-766220253552. Acesso em: 19 jun. 2026.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: Thomson Reuters Brasil, 2019.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo.** 34. ed., rev., atual. e ampl. Rio de Janeiro: Forense, 2021.

DONEDA, D. **Da privacidade à proteção de dados pessoais.** 3. ed. São Paulo: Revista dosTribunais, Thomson Reuters Brasil, 2021. 368 p.

DORIGO, E. **Os impactos da Lei Geral de Proteção de Dados nas rotinas do Departamento Pessoal de empresas de pequeno porte.** 2024. Dissertação (Mestrado em Administração) –Universidade de Caxias do Sul, Guaporé/RS, 2024.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (ENAP). Portal institucional. Brasília, 2026. Disponível em: https://www.enap.gov.br. Acesso em: 05 mai. 2026.

FERREIRA, Antonio Coutinho. **O fator humano na segurança da informação sob a ótica da LGPD. Revista Ibero-Americana de Humanidades**, Ciências e Educação, São Paulo, v. 12, n. 5, p. 1-13, mai. 2026.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato**. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

JUSTEN FILHO, Marçal. **Curso de direito administrativo.** 13. ed. São Paulo: Thomson Reuters Brasil, 2018.

MAGALHÃES, Brunno Roberto Araujo Lins; DE ANDRADE MATTIETTO, Leonardo. **Políticas Públicas E O Direito A Proteção De Dados: Uma Análise Da** ADI Nº 6561/TO. **Revista de Direito da Administração Pública**, v. 1, n. 03, 2023.

MELO, Gabriel Penna Firme de. **Proteção de dados pessoais na era digital: um estudo comparativo entre a LGPD brasileira e o GDPR europeu.** Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 12, n. 4, p. 1-24, abr. 2026.

MENDES, L. S., & FONSECA, G. C. S. da. (2020). Proteção de Dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, *6*(2), 507–533. https://doi.org/10.21783/rei.v6i2.521 Acesso em: 01 mai. de 2026.

MINAYO, Maria Cecília de Souza. DESLANDES, Suely Ferreira; GOMES, Romeu. **Pesquisa social: teoria, método e criatividade**, v. 25, 2016.

MINGHELLI, M. **Lei Geral de Proteção de Dados e a elaboração do Relatório de Impacto à Proteção de Dados Pessoais.** Revista em questão, v. 30, n. 49, 2024. Disponível em: https://www.scielo.br/j/emquestao/a/FyFnttTbBfXvcfnFMNGMcVs/?format=html&lang=pt Acesso em: 20 jun. 2026.

PEITER, E. E. *et al*. **Lei Geral de Proteção de Dados:** roteiro para implantação e adequação em escritórios de contabilidade. In: Congresso USP de Iniciação Científica em Contabilidade, São Paulo, v. 22, n. 07, 2022. Disponível em: https://congressousp.fipecafi.org/anais/22uspinternational/ArtigosDownload/3631.pdf Acesso em: 18 jun. 2026.

PIMENTA, D.; MEDEIROS, J. **Contribuição da Lei Geral de Proteção de Dados (LGPD) na construção da confiança do cliente em escritórios de contabilidade.** Revista de Administração e Contabilidade da UNIFAT, v. 17, n. 1, 2025. Disponível em: https://reacfat.com.br/reac/article/view/422 Acesso em: 20 jun. 2026.

ISSN-2966-0785 REVISTA ACADÊMICA DA LUSOFONIA

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários À Lei N 13709/2018 (LGPD) -** 4ª edição 2023. Saraiva Educação SA, 2023.

RIBEIRO, F.; MOREIRA, C. **A percepção dos profissionais da área contábil e dos gestores sobre os impactos da implementação da LGPD**. RAGC, v. 9, n. 39, p.119-134, 2021.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. **Proteção de dados pessoais e inteligência artificial.** Rio de Janeiro: Forense, 2023.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). Portal institucional. Brasília, 2026. Disponível em: https://www.tcu.gov.br .Acesso em: 05 mai. 2026.