Proteção de dados e governança pública: uma análise comparativa entre a LGPD (Brasil) e o GDPR (Europa)

Roberta Santarosa de Sousa
(Universidade Federal de São João del-Rei)

Aline Resende
(Universidade Federal de São João del-Rei)

Luiz Gonzaga Chiavegato Filho
(Universidade Federal de São João del-Rei)

Gustavo Melo Silva
(Universidade Federal de São João del-Rei)

RESUMO:
O presente artigo realiza uma análise teórica dos desafios associados à implementação da Lei Geral de Proteção de Dados (LGPD) na Administração Pública brasileira, com ênfase no tratamento e na governança de dados, estabelecendo uma comparação com o Regulamento Geral de Proteção de Dados (GDPR). Analisaram-se as convergências e divergências entre a normativa brasileira e a europeia, visando compreender os avanços e entraves para a efetiva execução no que se refere ao Tratamento e Governança de Dados. A pesquisa, de natureza teórica, abordagem qualitativa e exploratória, consistiu na análise bibliográfica e documental. A análise comparativa entre a LGPD e o GDPR evidencia diferenças estruturais e operacionais na governança de dados no setor público e a implementação de ambas as legislações enfrenta desafios institucionais, operacionais, regulatórios e culturais. Concluiu-se que a prática experimentada pela União Europeia fornece referências relevantes para o Brasil, mas faz-se necessária a adoção de práticas que conciliam a inovação com a garantia dos direitos e que funcionem na Administração Pública Brasileira.
PALAVRAS-CHAVE: Administração Pública, análise comparativa, GDPR, LGPD.

1. Introdução

Na contemporaneidade, a informação consolidou-se como um ativo estratégico, econômico e político de elevado valor, impulsionado pela crescente digitalização das relações sociais e pelo uso massivo de dados por governos e empresas. Esse cenário impõe novos desafios à garantia da privacidade, da segurança e da dignidade humana, tornando a proteção de dados pessoais um dos temas mais relevantes do século XX.

A promulgação do Regulamento Geral sobre a Proteção de Dados (GDPR) pelo Parlamento Europeu em 27 de abril de 2016 representou marco na harmonização da regulação sobre proteção de dados nos Estados-membros da União (Magalhães, 2021; Graf & Bitencourt (2025). Tal regulamento consolidou-se como referência global, influenciando a regulamentação do tema em diversos países, inclusive no Brasil (Mugamba, 2025; Mello et al., 2025; Silva & Ptaszek; 2025).

Inspirado no modelo europeu, o Brasil promulgou a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), buscando harmonizar sua legislação com padrões globais e equilibrar inovação com direitos fundamentais. Contudo, a aplicação dessa norma no âmbito da Administração Pública revela particularidades e desafios exigindo mecanismos institucionais que assegurem a proteção de dados.

O estudo justifica-se, portanto, pela necessidade de aprofundar a compreensão da proteção de dados como questão de governança pública, deslocando o foco da conformidade formal para a dimensão organizacional e institucional da implementação. Portanto, este artigo parte da seguinte questão-problema: A partir de uma análise comparativa com o GDPR, pode-se afirmar que a LGPD estrutura condições institucionais suficientes para uma governança eficaz da proteção de dados no âmbito do setor público brasileiro?

O presente estudo tem como objetivo geral analisar comparativamente os marcos normativos do GDPR e da LGPD com foco nos dispositivos relativos à governança de dados no setor público. Para isso, define-se como objetivos específicos: 1) Apresentar um panorama histórico das leis de proteção de dados no mundo percorrendo o surgimento e a evolução das normativas, a história da valorização da privacidade e introduzir LGPD nesse cenário; 2) Examinar as convergências e divergências entre a LGPD e o GDPR no que se refere à governança da proteção de dados no setor público; 3) Apontar os principais desafios institucionais, operacionais, regulatórios e culturais da implementação da LGPD no setor público brasileiro, à luz dos parâmetros de governança estabelecidos pelo GDPR.

2. Fundamentação teórica

A consolidação da economia de dados e a crescente centralidade da privacidade impulsionaram a formulação de marcos regulatórios robustos em diferentes jurisdições. No Brasil, a Lei Geral de Proteção de Dados (LGPD) disciplina o tratamento de dados pessoais pelo

poder público e pelo setor privado, enquanto na União Europeia, o Regulamento Geral sobre a Proteção de Dados (GDPR) constitui referência normativa internacional.

O Brasil seguiu a tendência global ao eleger o GDPR como modelo, sendo este considerado um dos mais abrangentes do mundo, em termos de princípios e diretrizes, pois coloca o cidadão na centralidade da decisão sobre seus dados pessoais, garantindo que qualquer procedimento envolvendo dados pessoais do cidadão devem ser realizados de acordo com finalidade específica e com sua anuência (Fernandes & Nuzzi, 2022).

A LGPD no Brasil teve como referência o modelo europeu compartilhando estrutura, princípios e a elevação da privacidade à categoria de direito fundamental (Mello et al., 2025; Perrone & Strassburger, 2018). Perrone e Strassburger (2018, p. 84) concluem que "a LGPD é uma GDPR com um toque brasileiro". Ao incorporar princípios, direitos dos titulares e mecanismos de fiscalização alinhados ao modelo europeu, a LGPD posiciona o Brasil no cenário internacional de proteção de dados (Mello et al., 2025).

A análise comparativa da LGPD e do GDPR demonstra convergências e divergências que ajudam a identificar desafios de implementação da Governança de Dados na Administração Pública. Conforme esclarecem Cristóvam et al. (2021), a governança de dados é essencial para o sucesso da implementação da LGPD, consistindo em um conjunto estruturado de processos para gerenciar formalmente os ativos de dados nos setores público e privado. De acordo com os autores, a simples existência de dados na máquina estatal não constitui governança, a qual exige mecanismos institucionais e o exercício de autoridade sobre dimensões como compartilhamento, segurança, qualidade e arquitetura tecnológica.

De acordo com Bioni et al. (2021), a governança de dados pode ser compreendida como uma política pública orientada à promoção da justiça social e ao fortalecimento da relação de confiança entre o Estado e os cidadãos. Nessa perspectiva, tal governança envolve a implementação de reestruturações organizacionais que buscam alinhar as práticas de tratamento de dados à missão institucional e aos princípios que regem a administração pública, contribuindo para o fortalecimento da dimensão democrática na gestão da informação. Na Administração Pública, a governança de dados deve ser entendida como política pública estratégica, voltada ao fortalecimento democrático e à proteção da privacidade dos cidadãos (Cristóvam et al., 2021).

Embora tanto a LGPD quanto o GDPR compartilhem o objetivo de proteger os direitos dos titulares de dados, a aplicação de seus dispositivos ao setor público evidencia diferenças estruturais significativas, especialmente no que se refere às bases legais, à transparência, à interoperabilidade e ao regime sancionatório (Cristóvam et al., 2021; Furlan Di Biase & Fortes Aguilera, 2021), ao passo que convergem em aspectos de governança institucional (Graf & Bitencourt, 2025; Mello et al., 2025).

3. Método de pesquisa

Na presente pesquisa adotou-se a abordagem qualitativa e quanto aos objetivos, a investigação classifica-se como exploratório-descritiva e os procedimentos de coleta, a pesquisa classifica-se como documental (Gil, 2002).

No que se refere aos procedimentos técnicos de coleta, a metodologia empregada utiliza-se articuladamente da pesquisa bibliográfica e da pesquisa documental. A pesquisa bibliográfica, empregada na construção do referencial teórico, a partir basicamente de artigos científicos. A revisão da literatura foi realizada entre outubro de 2025 e março de 2026. Inicialmente, realizaram-se buscas exploratórias no Google Scholar para mapear os desafios da implementação da LGPD na Administração Pública e identificar experiências internacionais. Posteriormente, procedeu-se à busca sistemática na base Web of Science, estruturada em quatro etapas, com diferentes combinações de descritores relacionados a proteção de dados, LGPD, GDPR, setor público, governança e implementação.

As buscas na Web Science totalizaram 339 registros. Após aplicação de filtros (idioma, tipo de documento, período 2018–2026 e acesso aberto), restaram 41 estudos para triagem. Destes, apenas 10 foram selecionados para leitura integral e, ao final, 8 compuseram a amostra efetiva. Verificou-se, contudo, baixa aderência conceitual entre os resultados recuperados e o foco específico em governança na proteção de dados no setor público.

Também foram feitas buscas em bases como SciELO – Science Eletronic Library Online e SPELL - Scientific Periodicals Electronic Library também apresentaram resultados pouco expressivos. A identificação dos estudos, nessas e nas demais bases, ocorreu de forma iterativa, com refinamento progressivo dos descritores à medida que novas categorias analíticas emergiam. Parte dos trabalhos foi localizada por meio de encadeamento das referências bibliográficas dos artigos inicialmente selecionados.

Realizou-se a leitura sistemática e a análise documental dos principais diplomas normativos que estruturam os regimes de proteção de dados examinados neste estudo, a saber: a Lei nº 13.709, de 14 de agosto de 2018, que institui a Lei Geral de Proteção de Dados Pessoais (LGDP) no Brasil, e o Regulamento (UE) 2016/679, Regulamento Geral sobre a Proteção de Dados (GDPR), na União Europeia. A análise concentrou-se na identificação de dispositivos relacionados à governança da proteção de dados no setor público, permitindo a comparação entre os arranjos institucionais, mecanismos de responsabilização e instrumentos regulatórios previstos em cada ordenamento.

Por fim, a análise dos dados organizou-se em três eixos: (1) contextualização histórica da proteção de dados no cenário internacional, situando o surgimento da Lei Geral de Proteção de Dados Pessoais; (2) análise comparativa dos modelos de governança da proteção de dados no setor público, destacando convergências e divergências entre a LGPD e o Regulamento Geral sobre a Proteção de Dados e (3) reflexão sobre os desafios institucionais, operacionais, regulatórios e culturais. da implementação da LGPD na Administração Pública brasileira à luz dos parâmetros de governança estabelecidos pelo modelo europeu.

4. Análise dos resultados

4.1. Panorama histórico das leis de proteção de dados no mundo e o surgimento da LGPD

O conceito de privacidade enquanto direito relacionado à personalidade foi defendido teoricamente no ano de 1890 pelos advogados norte-americanos Samuel Warren e Louis Brandeis, em artigo publicado na Harvard Law Review, intitulado “The Right to Privacy” (Warren & Brandeis, 1890).

A privacidade foi incorporada à Declaração Universal dos Direitos Humanos da Organização das Nações Unidas após a Segunda Guerra Mundial, com a inclusão do artigo 12: “ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (Organização das Nações Unidas [ONU], 1948).

Embora a privacidade seja considerada um direito universal pela Organização das Nações Unidas (ONU) e a proteção a esse tipo de direito fundamental tenha ganhado força desde o fim da Segunda Guerra Mundial (Bioni & Zanatta, 2021; ONU, 1948), as leis específicas de proteção de dados surgiram mais tardiamente, acompanhando o avanço tecnológico e a necessidade de regular o uso dessas informações (Magalhães, 2021).

O primeiro país a regular o tema, ainda por meio de legislação local, foi a Alemanha - a chamada Lei de Hesse - em 1970 (Aguiar &Tonella, 2023), enquanto o Parlamento Europeu aprovou, em 1995, a Diretiva de Proteção de Dados (Diretiva 95/46/CE), que foi o marco regulatório da União Europeia para proteger dados, estabelecendo princípios fundamentais sobre o tratamento de informações pessoais (Magalhães, 2021). Essa normativa foi reformulada culminando na promulgação, em 2016, do Regulamento Geral sobre a Proteção de Dados (GDPR), proporcionando a harmonização na regulação nos estados-membros (Magalhães, 2021; Perrone & Strassburger, 2018).

Dessa forma, o GDPR, que entrou em vigor em 24 de maio de 2016 e tornou-se aplicável a partir de 25 de maio de 2018 foi instituído pela União Europeia como resposta a um histórico de abusos no uso de informações pessoais, estruturando-se com base na centralidade dos direitos dos titulares (Erickson, 2019; Lim & Oh, 2025). Desde então, consolidou-se como referência global em proteção de dados, influenciando diversos países a elaborarem suas próprias legislações adaptadas às suas particularidades históricas, políticas e culturais (Lim & Oh, 2025).

Conforme Magalhães (2021), o Brasil, em consonância com a tendência internacional e inspirado no GDPR, promulgou a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD). Sancionada em 14 de agosto de 2018, sua vigência ocorreu de forma escalonada, com a maior parte dos dispositivos em vigor a partir de setembro de 2020 e as sanções administrativas aplicáveis desde agosto de 2021 (Belli, 2024; Fernandes & Nuzzi, 2022). A LGPD estabelece as normas para o tratamento de dados pessoais no Brasil. A lei é estruturada em dez capítulos e possui 65 artigos, que disciplinam os princípios da proteção de dados, os direitos dos titulares, as bases legais que autorizam o tratamento, bem como as responsabilidades dos agentes de tratamento e os mecanismos de fiscalização e sanção (Brasil, 2018).

Embora o direito fundamental à intimidade, à vida privada, à honra e à imagem, estivesse assegurado pela Constituição Federal desde 1988, em seu artigo 5º, inciso X, o debate sobre privacidade ganhou maior visibilidade no Brasil em 2018, com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados na União Europeia (Fernandes & Nuzzi, 2022).

Bioni e Rielli (2021) mencionam que a aprovação da LGPD foi impulsionada, entre outros fatores, pela intenção do Brasil de ingressar na Organização para a Cooperação e o Desenvolvimento Econômico (OCDE). Pressões nacionais e internacionais, incluindo novas legislações surgidas no mundo e escândalos de vazamento de dados em um contexto de expansão do Big Data, contribuíram para sua aprovação (Bioni & Rielli, 2021). Segundo os autores, esse contexto funcionou como um ultimato para a aprovação da lei, uma vez que apenas com um arranjo regulatório completo o país poderia alcançar um nível adequado de proteção de dados e avançar em sua pretensão de adesão à OCDE (Bioni, 2021; Bioni & Rielli, 2021).

Antes da promulgação da LGPD, a proteção de dados no Brasil caracterizava-se por um modelo fragmentado e de regulação setorial, o que dificultava sua efetiva tutela (Belli, 2024). Até então, os direitos constitucionais eram assegurados de maneira pulverizada por legislações esparsas (Fernandes & Nuzzi, 2022). Entre elas, destacavam-se a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), que foi pioneira ao instituir direitos e garantias relativos às informações pessoais dos consumidores, estabelecendo regras sobre o tratamento de dados em cadastros, e, de modo mais estruturado, a Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet (Fernandes & Nuzzi, 2022); somando-se a elas a Lei nº 12.737, de 30 de novembro de 2012, que tipificou os delitos informáticos (Filgueiras et al., 2025).

Quatro anos após a promulgação da LGPD, a Emenda Constitucional nº 115/2022 incluiu o inciso LXXIX no art. 5º da Constituição Federal, reconhecendo a proteção de dados pessoais, inclusive em meios digitais, como direito fundamental (Brasil, 1988). A inserção do novo dispositivo conferiu maior densidade normativa e ampliou a segurança jurídica ao elevar o tema ao nível constitucional (Medeiros, 2025).

A trajetória que culminou na promulgação da LGPD e na Emenda Constitucional nº 115/2022 revela o reconhecimento da necessidade de um arcabouço normativo robusto e coerente, capaz de resguardar a privacidade e os dados informacionais dos cidadãos brasileiros (Aguiar & Tonella, 2023; Medeiros, 2025), direito este já postulado pela Declaração Universal dos Direitos Humanos da Organização das Nações Unidas, em 1948 (ONU, 1948).

Recentemente, foi promulgada a Lei nº 15.352, de 25 de fevereiro de 2026 que institui a Agência Nacional de Proteção de Dados (ANPD) como agência reguladora, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e sede e foro no Distrito Federal (Brasil, 2026), garantindo maior autonomia institucional para regular e fiscalizar a aplicação da LGPD no Brasil.

4.2. Análise Comparativa da LGPD e do GDPR

A análise comparativa entre a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre a Proteção de Dados (GDPR) revela distinções significativas entre os modelos europeu e brasileiro, especialmente no que tange à profundidade e robustez normativa e à estrutura institucional (Erickson, 2019; Mello et al., 2025). A comparação evidencia diferenças estruturais relevantes quanto ao tratamento de dados pelo setor público (Furlan Di Biase & Fortes Aguilera, 2021), às bases legais (Mello et al., 2025), à autonomia das autoridades de controle (Erickson, 2019; Furlan Di Biase & Fortes Aguilera, 2021) e ao ecossistema normativo de governança de dados na existência de um conjunto regulatório capaz de acompanhar a inovação tecnológica (Graf & Bitencourt, 2025; Lim & Oh, 2025)."

Uma principal divergência encontrada na referida análise é o fato de que a lei brasileira dedica um capítulo específico ao tratamento de dados pelo setor público, o Capítulo IV (arts. 23 a 32) estabelecendo parâmetros próprios de transparência, segurança, governança e responsabilização. Já o regulamento europeu não detalha exaustivamente a base legal para o setor público, delegando essa fundamentação a normas específicas da União Europeia ou de seus Estados-membros (Brasil, 2018; União Europeia, 2016).

Embora o Capítulo IV da LGPD configura-se como eixo de governança informacional no Estado, tal capítulo sofre com lacunas, contradições e problemas estruturais que geram incertezas jurídicas na sua aplicação (Furlan Di Biase & Fortes Aguilera, 2021).

Na LGPD, o Capítulo IV (arts. 23 a 32) é o eixo central de governança informacional no Estado, ao integrar transparência, coordenação institucional, interoperabilidade e accountability, contribuindo para a modernização administrativa e para o fortalecimento do controle social sobre o uso de dados pelo poder público (Belli, 2023; Cristóvam, 2021; Furlan Di Biase & Fortes Aguilera, 2021). Em seu artigo 23, a lei condiciona o tratamento pelo poder público à consecução do interesse público, afastando a utilização de bases legais flexíveis (Brasil, 2018; Furlan Di Biase & Fortes Aguilera, 2021). Em contraste, o Regulamento Geral sobre a Proteção de Dados (GDPR) não contempla disposições específicas ou seção autônoma sobre o tratamento pelo Poder Público, dispondo em seu art. 6º, alínea 'e', apenas a base do exercício de funções de interesse público ou autoridade pública (Furlan Di Biase & Fortes Aguilera, 2021; União Europeia, 2016). Assim, o GDPR adota uma disciplina de caráter geral, delegando o detalhamento e a fundamentação dessas regras a normas específicas da própria União Europeia ou de seus Estados-membros (Furlan Di Biase & Fortes Aguilera, 2021; União Europeia, 2016).

Na União Europeia, a necessidade de uma regulamentação mais específica foi suprida pelo Regulamento nº 1725/2018, que atua de forma conjunta e sistemática com a Regulamento 2016/679 (GDPR) mantendo o rigor sobre a finalidade do tratamento, mas permitindo flexibilidade em casos de interesse público ou exercício de autoridade (Santos Neto et al., 2021). Essa flexibilidade não se reproduz no Brasil, uma vez que a LGPD estabelece, de forma expressa e estruturada em seu Capítulo IV, um regime específico e taxativo para o tratamento de dados pelo Poder Público, delimitando com maior precisão os parâmetros de atuação administrativa. Embora essa estrutura fortaleça a segurança jurídica e o controle da atuação estatal, pode impor desafios à gestão pública ao limitar a adaptação às complexidades administrativas contemporâneas.

O artigo 7º, inciso III, da LGPD é a base legal que autoriza a Administração Pública a tratar e compartilhar dados para a "execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres" (Brasil, 2018). Trata-se de uma base legal distinta do consentimento do titular, conferindo ao Poder Público o direito de tratar os dados pessoais e dispensando o fornecimento de consentimento nas situações legais atreladas às suas finalidades institucionais (Cristóvam et al., 2021). Entretanto, o Poder Público está obrigado a observar as disposições específicas do Capítulo IV, sob pena de aplicação das sanções administrativas previstas no artigo 52 da própria lei, mas com uma restrição fundamental: a legislação restringe as modalidades punitivas aplicáveis aos órgãos e entidades públicas, impedindo que estes recebam multas pecuniárias (Brasil, 2018; Cristóvam et al., 2021).

Diferente da legislação brasileira, o GDPR não concentra as normas voltadas ao setor público em um capítulo específico. O arranjo europeu funciona como uma moldura principiológica geral, cuja aplicação depende das legislações nacionais dos Estados-membros e de normas complementares da União Europeia (Furlan Di Biase & Fortes Aguilera, 2021). No que tange especificamente às instituições europeias, as regras foram estabelecidas pelo Regulamento (UE) 2018/1725, que deve ser interpretado em conjunto com o GDPR (Santos Neto et al., 2021).

No ecossistema europeu, o GDPR está inserido em um conjunto normativo mais amplo, não se limita a uma legislação isolada, mas compõe um arranjo normativo complementar que inclui o *Data Governance Act*, o *Artificial Intelligence Act* e o *Data Act*, buscando conciliar a proteção de dados com o compartilhamento seguro e a inovação tecnológica (Jørgensen & Ma, 2025). O *Data Governance Act*, em vigor desde setembro de 2023, introduziu mecanismos como o altruísmo de dados e intermediários confiáveis para viabilizar o compartilhamento de informações, inclusive do setor público, para finalidades de interesse geral (Jørgensen & Ma, 2025). Conforme Hacker e Neyer (2023), o modelo da GDPR possui uma orientação prospectiva que permite a adaptação às transformações tecnológicas. Essa estrutura busca equilibrar a proteção de dados com o interesse público em áreas estratégicas, como saúde, segurança e cidades inteligentes (Gültekin-Várkonyi, 2024; Hacker & Neyer, 2023; Jørgensen & Ma, 2025).

Em contraste com esse modelo, não há no Brasil um arranjo normativo integrado voltado ao compartilhamento ampliado ou à experimentação regulatória, como o altruísmo de dados, o que demonstra uma menor flexibilidade adaptativa do sistema brasileiro. Contudo, é importante notar que, mesmo no contexto europeu, tais mecanismos introduzidos pela Lei de Governança de Dados ainda enfrentam barreiras práticas e permanecem em estágio inicial de implementação (Jørgensen & Ma, 2025).

Dessa forma, a legislação brasileira vincula a atuação estatal à finalidade pública previamente definida (Furlan Di Biase & Fortes Aguilera, 2021). No modelo europeu, o regulamento veda expressamente o uso de bases flexíveis típicas do setor privado, como o legítimo interesse, para o exercício de autoridades públicas (União Europeia, 2016), exigindo como contrapartida a adoção de abordagens baseadas em risco e rigorosas avaliações de impacto (Gültekin-Várkonyi, 2024; Hacker & Neyer, 2023)

Outras divergências apresentadas entre as legislações estão a centralização da governança e a autonomia institucional, que impactam a eficácia da proteção de dados. No arranjo europeu, para garantir a aplicação uniforme das normas na Europa, foi instituído o European Data Protection Board - EDPB, um órgão independente que promove a cooperação entre as autoridades nacionais e resolve controvérsias transfronteiriças (Lorenzon, 2021). Quanto à autonomia institucional, as autoridades de proteção de dados - DPAs europeias não ficam subordinadas a pressões políticas ou econômicas de governos, o que é fundamental para a proteção efetiva dos direitos (Lorenzon, 2021).

No Brasil, é a ANPD a autoridade nacional responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo o território nacional (Brasil, 2018). Entretanto, sua inicial vinculação à estrutura Administrativa Federal foi apontada como um possível limitador de sua autonomia plena (Furlan Di Biase & Fortes Aguilera, 2021; Lorenzon, 2021).

Em contraste, as autoridades europeias de proteção de dados detêm maior independência funcional, operando dentro de um sistema coordenado pelo EDPB, o qual garante a aplicação uniforme e coerente do regulamento em todos os Estados-membros da União Europeia (Lorenzon, 2021). O sucesso da regulação europeia depende, segundo Erickson (2019), de autoridades de dados plenamente independentes, capazes de fortalecer a fiscalização e promover confiança pública e internacional.

A busca pela autonomia institucional da autoridade brasileira teve início com a promulgação da Lei nº 14.460/2022, que transformou a ANPD em autarquia de natureza especial, ampliando sua autonomia institucional (Graf & Bitencourt, 2025). Atualmente Lei nº 15.352/2026, de 25 de fevereiro de 2026 (Brasil, 2026), consolida o amadurecimento institucional do órgão ao criar formalmente a Agência Nacional de Proteção de Dados (ANPD), configurando-a como uma agência reguladora dotada de autonomia funcional, técnica, decisória, administrativa e financeira.

A mudança pode ser interpretada como um processo de aprendizagem regulatória inspirado no modelo europeu, aproximando o arranjo brasileiro dos padrões internacionais de governança, ao buscar garantir maior independência técnica, administrativa e financeira para a fiscalização do ecossistema de dados, condição fundamental para a adequação do país. Entretanto, por se tratar de alteração normativa recente, seus efeitos práticos sobre a atuação regulatória e a governança do sistema de proteção de dados ainda demandam acompanhamento e avaliação ao longo do tempo.

No campo da transparência, a LGPD privilegia a divulgação digital, determinando em seu artigo 23, inciso I que informações sobre finalidade e base legal sejam disponibilizadas preferencialmente em sítios eletrônicos (Brasil, 2018). Ao passo que, o GDPR enfatiza a clareza, concisão e acessibilidade da informação, permitindo, em seu artigo 12, que seja fornecida por diferentes meios, inclusive oralmente, desde que seja possível verificar a identidade do titular (União Europeia, 2016). Assim, enquanto a legislação brasileira foca no meio digital como instrumento de governança, o regulamento europeu prioriza a qualidade comunicacional e a flexibilidade do canal de divulgação.

A análise da interoperabilidade de dados também revela abordagens distintas entre os regimes. A LGPD estabelece, em seu art. 25, a manutenção de dados em formato interoperável como dever de governança, voltado à eficiência administrativa, ao compartilhamento e à implementação de políticas públicas (Brasil, 2018), enquanto que no GDPR, a interoperabilidade se vincula principalmente ao direito à portabilidade do titular (art. 20), sendo limitada quando o tratamento se destina ao exercício de funções de interesse público conforme previsto no artigo 20, n.º 3 do GDPR (União Europeia, 2016). Dessa forma, enquanto a lei brasileira adota a interoperabilidade como instrumento da gestão estatal, o regulamento europeu a configura como direito individual com aplicação mitigada no contexto público.

No tocante ao regime sancionatório, observa-se uma divergência fundamental: enquanto o GDPR delega aos Estados-Membros a decisão sobre multas a órgãos públicos (União Europeia, 2016), o Art. 52, § 3º da LGPD veda categoricamente a aplicação de multas pecuniárias ao setor público brasileiro (Brasil, 2018; Cristóvam et al., 2021). Consequentemente, a conformidade no Brasil depende predominantemente de mecanismos reputacionais e pedagógicos, como a publicização de infrações, o que pode limitar a eficácia da governança em comparação ao modelo coercitivo europeu.

Embora tal restrição seja frequentemente justificada pelo argumento de que a imposição de multas ao Estado implicaria, em última instância, penalizar o próprio erário, essa opção normativa pode reduzir significativamente o potencial coercitivo da lei no setor público. Diferentemente do modelo europeu, no qual as autoridades de proteção de dados dispõem de maior flexibilidade sancionatória, inclusive com a possibilidade de aplicação de multas a organismos públicos em determinados contextos, o ordenamento brasileiro limita os instrumentos de pressão institucional disponíveis para assegurar a conformidade (Cristóvam et al., 2021; União Europeia, 2016). Essa limitação pode gerar incentivos institucionais mais fracos para a implementação efetiva de práticas robustas de governança e proteção de dados no âmbito estatal, sobretudo em contextos marcados por restrições orçamentárias, baixa priorização administrativa e assimetrias de capacidade institucional. Dessa forma, a ausência de coerção financeira levanta questionamentos sobre a suficiência dos instrumentos de enforcement da LGPD no setor público (Lemes, 2025).

A análise comparativa da LGPD e do GDPR demonstra convergências que também auxiliam a identificar desafios de implementação da Governança de Dados na Administração Pública. Os dois sistemas constituem marcos essenciais para a construção de um ambiente digital seguro e confiável, embora exijam aperfeiçoamento contínuo e harmonização internacional para assegurar efetivamente os direitos fundamentais no contexto digital (Mello et al., 2025).

As legislações compartilham definições de dados pessoais, princípios de tratamento, direitos dos titulares e abrangência extraterritorial, o que favorece operações integradas e estratégias de governança entre os mercados brasileiro e europeu (Mello et al., 2025). Entretanto, diferem quanto à maturidade e aplicabilidade: o GDPR apresenta maior previsibilidade e experiência sancionatória, enquanto a LGPD ainda demanda interpretação

jurídica em dispositivos como o do legítimo interesse, além de enfrentar uma cultura de proteção de dados em estágio inicial, exigindo esforços de conscientização e adaptação tecnológica (Mello et al., 2025).

No que se refere à estrutura organizacional da governança de dados, observa-se convergência significativa entre a LGPD e o GDPR, particularmente quanto à obrigatoriedade da designação do Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO) para órgãos públicos, independentemente do volume de dados tratados**.** A obrigatoriedade da designação do encarregado de dados para todo o setor público confere a essa figura papel central na governança e na transformação institucional (Deprá, 2025). No contexto brasileiro, essa exigência está prevista no art. 23, inciso III, da LGPD (Brasil, 2018), enquanto na União Europeia fundamenta-se no art. 37º, n.º 1, do GDPR (Lim & Oh, 2025; Phillips, 2021; União Europeia, 2016). Em ambos os regimes, a imposição legal elimina a discricionariedade baseada em escala ou risco, consolidando o DPO como elemento central da governança estatal e da accountability institucional. Entretanto, o GDPR admite exceções, como a isenção para tribunais no exercício de funções jurisdicionais, reforçando a autonomia funcional do Poder Judiciário europeu (União Europeia, 2016)."

Segue quadro comparativo entre a LGPD e o GDPR que evidencia as diferenças estruturais na governança de dados no setor público. Essa comparação permite compreender como cada legislação reflete prioridades institucionais distintas, mas convergentes no objetivo de assegurar direitos fundamentais e consolidar práticas de governança de dados.

Tabela 1. Governança de Dados no Setor Público: um comparativo entre a LGPD e o GDPR

Tópico	LGPD	GDPR	Diferença Principal
1. Base Legal e Legítimo Interesse	O tratamento deve atender à finalidade pública e à persecução do interesse público. A lei não cita o "legítimo interesse" como base para o setor público, focando na competência legal (Art. 23).	Estabelece explicitamente que o "Interesse Legítimo" não se aplica ao tratamento efetuado por autoridades públicas na prossecução de suas atribuições (Art. 6º, n.º 1).	GDPR é proibitivo; LGPD é diretiva. O GDPR proíbe textualmente o uso, enquanto a LGPD o afasta pela estrutura vinculada à finalidade pública.
2. Encarregado (DPO)	Indicação obrigatória para todas as pessoas jurídicas de direito público que realizem operações de tratamento (Art. 23, inciso III).	Designação obrigatória para autoridades ou organismos públicos, exceto tribunais no exercício de sua função jurisdicional (Art. 37º, n.º 1, alínea 'a').	Convergência Total. Ambas removem a flexibilidade do setor privado e impõem o DPO como regra absoluta para o governo.

3. Transparência Ativa	Exige informações claras e atualizadas sobre previsão legal e finalidade, preferencialmente em seus sítios eletrônicos (Art. 23, inciso I).	Exige informações concisas, inteligíveis e de fácil acesso, podendo ser prestadas por escrito ou até oralmente, sem obrigar o uso de sites (Art. 12º).	Meio vs. Qualidade. A LGPD prescreve o meio (sites) como governança, enquanto o GDPR foca nos princípios da clareza e acessibilidade.
4. Interoperabilidade	É um dever de governança: dados devem ser mantidos em formato estruturado para uso compartilhado e execução de políticas públicas (Art. 25).	Associada ao direito de portabilidade, o qual é explicitamente excluído quando o tratamento é necessário ao interesse público (Art. 20º, n.º 3).	Divergência de Objetivo. Na LGPD é ferramenta de eficiência do Estado; no GDPR é ferramenta do cidadão excluída nas funções públicas.
5. Regime de Sanções (Multas)	Proíbe categoricamente a aplicação de multas pecuniárias ao Poder Público, mantendo advertências e publicização (Art. 52, § 3º).	Permite que cada Estado-Membro estabeleça suas próprias regras sobre a aplicabilidade de multas a autoridades públicas (Art. 83º, n.º 7).	Rigidez vs. Flexibilidade. A LGPD veda multas financeiras no nível federal; o GDPR delega essa decisão a cada país membro.

Fonte: Elaborado pelos autores (2026)

Assim, a análise comparativa evidencia a convergência global na busca por equilibrar avanço tecnológico e proteção de direitos individuais, ainda que cada país organize essa proteção segundo racionalidades institucionais distintas (Mello et al., 2025; Mugamba, 2025).

4.3. Desafios da Governança de Dados da LGPD na Administração Pública Brasileira

O Brasil, por meio da LGPD, buscou estabelecer um equilíbrio entre a promoção da eficiência administrativa e a proteção de direitos fundamentais. Entretanto, a implementação de uma governança de dados efetiva no âmbito da Administração Pública ainda enfrenta desafios de natureza institucional, operacional, regulatória e cultural.

Entraves estruturais decorrentes da fragmentação organizacional e da cultura de “silos de dados” na administração pública comprometem a interoperabilidade prevista no art. 25 da LGPD, conforme apontado por Lui et al. (2025). Essa lógica, historicamente enraizada no setor público, manifesta-se na gestão autônoma das informações por secretarias distintas, utilizando sistemas tecnológicos redundantes, sem integração ou padronização (Furlan Di Biase & Fortes Aguilera, 2021; Irani et al., 2023; Mergel et al., 2019). Destacam Lui et al. (2025) que a manutenção desses silos gera entendimentos conflituosos sobre sigilo fiscal e dificulta a modernização da governança, o que contrasta com a obrigatoriedade legal de

compartilhamento de dados. Tais obstáculos à transformação digital são agravados por uma abordagem burocrática, falta de coordenação e indefinição de metas nas políticas de proteção de dados (Filgueiras et al., 2025). Enquanto a LGPD ainda tenta consolidar a governança estatal, o modelo europeu (GDPR) oferece uma referência para enfrentar esses desafios ao reforçar o poder de controle do cidadão e o empoderamento por meio do direito à portabilidade.

No âmbito operacional, estudos internacionais indicam que a presença de sistemas legados e tecnologicamente defasados constitui um obstáculo relevante à manutenção da segurança da informação e à efetiva implementação de regulamentos de proteção de dados (Irani et al., 2023; Magnusson et al., 2025). Os autores apontam que tais sistemas não apenas dificultam o atendimento às novas exigências legais, como comprometem a observância do princípio da interoperabilidade, prejudicando a eficácia das medidas de conformidade (Irani et al., 2023; Magnusson et al., 2025). Assim, a conformidade regulatória no setor público não depende apenas de ajustes jurídicos, mas de uma reconfiguração técnica que assegure a integridade dos dados em todo o seu ciclo de vida.

No tocante ao regime sancionatório, a LGPD estabelece, em seu art. 52, § 3º, a vedação à aplicação de multas pecuniárias ao poder público, restringindo as sanções a advertências, publicização das infrações, além do bloqueio e eliminação dos dados (Brasil, 2018). Tal configuração limita o caráter coercitivo do sistema sancionatório e constitui um potencial entrave à efetividade da governança, na medida em que a indução à conformidade passa a depender predominantemente de mecanismos reputacionais, pedagógicos e corretivos (Furlan Di Biase & Fortes Aguilera, 2021; Lemes, 2023). Em contraste, o GDPR adota uma abordagem mais flexível ao delegar aos Estados-Membros a definição sobre a aplicação de multas administrativas a autoridades e organismos públicos, mantendo aberta a possibilidade de instrumentos pecuniários coercitivos (União Europeia, 2016). Nesse contexto, o desafio brasileiro consiste em assegurar a priorização da proteção de dados em um ambiente marcado por fragmentação organizacional e pela presença de sistemas legados, mesmo na ausência da pressão orçamentária que sanções pecuniárias poderiam representar.

No plano cultural, a literatura evidencia que a adequação normativa da LGPD depende da revisão de políticas internas e da transformação das rotinas organizacionais consolidadas (Belli et al., 2024), de modo que a capacidade técnica isolada não é suficiente para garantir resultados (Irani et al., 2023; Magacho & Trento, 2021).

A efetividade da LGPD exige uma mudança na cultura organizacional por meio da gestão do conhecimento. A aplicação do modelo SECI (Socialização, Externalização, Combinação e Internalização) sugere que os princípios de proteção de dados devem ser internalizados por todos os agentes públicos, indo além da produção de documentos formais e alcançando as rotinas administrativas (Silva & Ptaszek, 2025).

A implementação de ambas as legislações, LGPD e GDPR, enfrenta desafios institucionais, operacionais e culturais. A experiência da União Europeia com o GDPR oferece referências essenciais para o contexto brasileiro, tanto no plano jurídico quanto institucional. No campo jurisprudencial, decisões do Tribunal de Justiça da União Europeia (TJUE) em casos emblemáticos como Schrems II e Google Espanha demonstram o equilíbrio necessário entre

garantias individuais e transparência, servindo como guia para a interpretação de lacunas normativas no Brasil (Graf & Bitencourt, 2025). Contudo, a prática europeia também revela que a norma, por si só, não garante a efetividade (Mello et al., 2025). Estudos empíricos apontam que a governança na Polônia e no Reino Unido enfrentou obstáculos como insuficiência orçamentária, regras pouco detalhadas e potenciais conflitos de interesse do Encarregado de Dados (DPO) quando este possui vínculos que comprometem sua independência frente à organização (Lisiak-Felicka & Szmit, 2021; Phillips, 2021).

Compreender os desafios de implementação da LGPD na Administração Pública à luz da experiência internacional indica que sua efetividade exige mais do que a transposição normativa. É necessário considerar infraestrutura tecnológica, capacitação dos agentes públicos e mudanças culturais institucionais, adaptando essas referências às especificidades do contexto brasileiro (Graf & Bitencourt, 2025; Lisiak-Felicka & Szmit, 2021; Phillips, 2021).

Estes desafios da LGPD destacam a necessidade de estratégias adaptadas às características locais e reforçam a relevância de aprender com as experiências internacionais na construção de uma governança de dados eficiente no setor público brasileiro (Lui et al., 2025).

Assim, a implementação da LGPD no setor público não depende apenas da existência da norma jurídica, mas da capacidade institucional, organizacional, regulatória e cultural do Estado para estruturar uma governança eficaz de dados.

5. Considerações finais

O presente artigo realiza uma análise teórica dos desafios associados à implementação da Lei Geral de Proteção de Dados (LGPD) na Administração Pública brasileira, com ênfase no tratamento e na governança de dados, estabelecendo uma comparação com o Regulamento Geral de Proteção de Dados (GDPR).

Em resposta à questão de pesquisa, os resultados indicam que, embora o marco normativo nacional disponha de fundamentos institucionais relevantes para a proteção de dados, sua efetividade está condicionada à superação de desafios interdependentes de natureza institucional, operacional, regulatória e cultural. No plano institucional, destacam-se limitações associadas à capacidade de atuação da Autoridade Nacional de Proteção de Dados e à fragmentação organizacional que favorece a formação de silos informacionais, questões que ainda desafiam a implementação plena da LGPD. No âmbito operacional, evidenciam-se entraves relacionados à interoperabilidade entre sistemas, à obsolescência de infraestruturas tecnológicas e à necessidade de reconfiguração de rotinas administrativas. No campo regulatório, o regime sancionatório vigente impõe restrições aos mecanismos de responsabilização aplicáveis ao setor público. Por fim, desafios de natureza cultural também se mostram relevantes, particularmente no que se refere à superação de práticas institucionais de retenção de informação e ao fortalecimento da gestão do conhecimento, elementos essenciais para a consolidação de uma governança de dados efetiva na Administração Pública brasileira.

Apesar dos desafios identificados, a consolidação da proteção de dados pessoais no Brasil reflete um processo de amadurecimento jurídico e institucional diante das transformações da era digital. A promulgação da LGPD e o posterior reconhecimento constitucional do direito à proteção de dados pela Emenda Constitucional nº 115/2022 evidenciam a construção de um arcabouço normativo voltado à proteção da privacidade e dos dados informacionais dos cidadãos, em consonância com princípios já afirmados em instrumentos internacionais como a Declaração Universal dos Direitos Humanos. Nesse contexto, a LGPD configura-se como um avanço institucional ao reconhecer o titular de dados como sujeito central nas decisões relativas ao tratamento de suas informações pessoais, além de constituir instrumento estratégico para a transformação digital do setor público e para a inserção do Brasil no cenário internacional de governança de dados, ao promover o equilíbrio entre inovação tecnológica e a proteção de direitos fundamentais.

Os desafios identificados a partir da análise comparativa entre a LGPD e o GDPR evidenciam a necessidade de enfrentamento contínuo para a consolidação da governança de dados no setor público brasileiro. A experiência europeia, especialmente aquela associada ao GDPR, oferece importantes referências para esse processo de aprimoramento, embora sua incorporação deva considerar as especificidades institucionais, jurídicas e administrativas do contexto brasileiro. Por fim, a experiência internacional demonstra que a implementação da LGPD no setor público brasileiro deve ir além da transposição normativa. É necessário considerar infraestrutura tecnológica, capacitação contínua de agentes públicos, mudanças culturais e fortalecimento institucional da ANPD, garantindo práticas administrativas consistentes com a proteção de dados e a efetividade plena da lei.

Como proposta para pesquisas futuras, sugere-se o acompanhamento e a avaliação dos efeitos práticos da Lei nº 15.352, de 2026, dada a sua promulgação recente, criando a Agência Nacional de Proteção de Dados (ANPD). Estudos subsequentes devem investigar se a posição da ANPD como agência reguladora contribuirá para a superação dos desafios identificados nesta pesquisa que ainda limitam a governança de dados na Administração Pública brasileira.

Referências

Aguiar, J. L. G. R., & Tonella, L. H. (2023). Proteção de dados como um direito autônomo: A experiência alemã e brasileira através de julgados e benefícios da EC n. 115/2022. *Revista Contemporânea, 3*(12), 28371–28393. https://doi.org/10.56083/RCV3N12-182

Belli, L., Magalhães, L., Nunes, J. L, Vasconcellos, A. P., Gaspar, W. B., Franqueira, B., Bakonyi, E., Scovino, F., & Carabetta, J. (2024). *Governança de dados no setor público: Dados abertos, proteção de dados pessoais e segurança da informação para uma transformação digital sustentável*. Lumen Juris. https://repositorio.fgv.br/items/38a74d51-0bd9-439d-8d21-a9815fff9921

Bioni, B. R., & Rielli, M. M. (2021). A construção multissetorial da LGPD: História e aprendizados. In B. R. Bioni (Org.), *Proteção de dados: Contexto, narrativas e elementos fundantes* (pp. 15-58). B. R. Bioni Sociedade Individual de Advocacia. https://brunobioni.com.br/livros/protecao-de-dados/

Bioni, B. R., & Zanatta, R. A. F. (2021). A infraestrutura jurídica da economia dos dados: Dos princípios de justiça às leis de dados pessoais. In B. R. Bioni (Org.), *Proteção de dados: Contexto, narrativas e elementos fundantes* (pp. 80-129). B. R. Bioni Sociedade Individual de Advocacia. https://brunobioni.com.br/livros/protecao-de-dados/

Bioni, B. R., Zanatta, R. A. F., & Kitayama, M. S. (2021). A governança de dados como política pública: Perspectivas da cooperação entre Defensorias e sociedade civil. *Cadernos da Defensoria Pública do Estado de São Paulo*, *6*(31), 74-92. https://brunobioni.com.br/blog/artigos-cientificos/

Brasil. (1988). *Constituição da República Federativa do Brasil de 1988*. https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

Brasil. (2018). *Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais*. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Brasil. (2026). *Lei nº 15.352, de 25 de fevereiro de 2026*. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/Lei/L15352.htm

Cristóvam, J. S. da S., Bergamini, J. C. L., & Hahn, T. M. (2021). Governança de dados no setor público brasileiro: Uma análise a partir da Lei Geral de Proteção de Dados (LGPD). *Interesse Público, 23*(129), 75–101. https://bd.tjmg.jus.br/items/6cafdfe9-8d7b-4e39-a2e9-c3942c2ac0b7/full

Deprá, C. B. C. (2025). O encarregado pelo tratamento de dados pessoais na administração pública: Um agente de efetivação da governança no tratamento de dados pessoais dos administrados. *Revista Caderno Pedagógico, 22*(11), 1–21. https://doi.org/10.54033/cadpedv22n11-050

Erickson, A. (2019). Comparative analysis of the EU's GDPR and Brazil's LGPD: Enforcement challenges with the LGPD. *Brooklyn Journal of International Law, 44*(2), 859–886. https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9

Fernandes, M. E., & Nuzzi, A. P. E. (2022). Fundamentos da Lei Geral de Proteção de Dados (LGPD): Uma revisão narrativa. *Research, Society and Development, 11*(12). http://dx.doi.org/10.33448/rsd-v11i12.34247

Filgueiras, F., Lui, L., & Veloso, M. T. T. (2025). A gramática institucional da proteção de dados e da privacidade no Brasil. *Dados, 68*(1). https://doi.org/10.1590/dados.2025.68.1.346

Furlan Di Biase, N., & Fortes Aguilera, D. (2021). Dificuldades interpretativas no regime de tratamento de dados pelo poder público: Lacunas, contradições e atecnias na LGPD. *Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro, 4*(2). https://doi.org/10.46818/pge.v4i2.238

Gil, A. C. (2002). *Como elaborar projetos de pesquisa* (4ª ed.). Atlas.

Graf, J. O., & Bitencourt, C. M. (2025). Políticas públicas de protección de datos: Un análisis de las decisiones del Tribunal de Justicia de la Unión Europea y sus posibles repercusiones en Brasil. *Revista de Derecho de la UCB, 9*(17), 61–87. https://doi.org/10.35319/lawreview.202517105

Gültekin-Várkonyi, G. (2024). Navigating data governance risks: Facial recognition in law enforcement under EU legislation. *Internet Policy Review, 13*(3). https://doi.org/10.14763/2024.3.1798

Hacker, P., & Neyer, J. (2023). Substantively smart cities: Participation, fundamental rights and temporality. *Internet Policy Review, 12*(1). https://doi.org/10.14763/2023.1.1696

Irani, Z., Abril, R. M., Weerakkody, V., Omar, A., & Sivarajah, U. (2023). The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis. *Government Information Quarterly*, *40*(1), 101784. https://doi.org/10.1016/j.giq.2022.101784

Jørgensen, B. N., & Ma, Z. G. (2025). Impact of EU regulations on AI adoption in smart city solutions: A review of regulatory barriers, technological challenges, and societal benefits. *Information, 16*(7), 568. https://doi.org/10.3390/info16070568

Lemes, D. (2023). Lei geral de proteção de dados pessoais (LGPD): O setor público e vazamentos de dados pessoais. Revista Eixo, 12(2), 109–118. https://doi.org/10.19123/eixo.v12i2.1089

Lim, S., & Oh, J. (2025). Navigating privacy: A global comparative analysis of data protection laws. *IET Information Security.* https://doi.org/10.1049/ise2/5536763

Lisiak-Felicka, D., & Szmit, M. (2021). GDPR implementation in public administration in Poland – 1.5 year after: An empirical analysis. *Journal of Economics & Management, 43*, 1–21. https://doi.org/10.22367/jem.2021.43.01

Lorenzon, L. N. (2021). Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia, 1*, 39–52. https://periodicos.fgv.br/rpdue/article/view/83423

Lui, L., Aguiar, R. B., Rosa, T. G., Ferreira, G. C., & Oliveira, A. (2025). Proteção e uso de dados: Análise da robustez das estratégias das capitais brasileiras. *Urbe. Revista Brasileira de Gestão Urbana*, *17*, e20240244. https://doi.org/10.1590/2175-3369.017.e20240244

Magacho, B. T. P., & Trento, M. (2021). LGPD e compliance na administração pública: O Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? *Revista Brasileira de Pesquisa Jurídica, 2*(2), 7–26. https://www.sumarios.org/artigo/lgpd-e-compliance-na-administra%C3%A7%C3%A3o-p%C3%BAblica-o-brasil-est%C3%A1-preparado-para-um-cen%C3%A1rio-em

Magalhães, M. A. (2021). Data protection regulation: A comparative law approach. *International Journal of Digital Law, 2*(2), 33–53. https://doi.org/10.47975/IJDL.magalhaes.v.2.n.2

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. *International Journal of Information Security*, *24*(4), 177. https://doi.org/10.1007/s10207-025-01097-x

Medeiros, N. G. L. de. (2025). A evolução da proteção de dados no Brasil: Uma análise histórica e legislativa até o advento da LGPD. *Revista de Ciências Jurídicas e Empresariais*, *25*(2), 86–91. https://doi.org/10.17921/2448-2129.2024v25n2p86-91

Mello, L. E., Serra, C. D. D. G., Fernandes, S. G., Santos, G. M. dos, Souza, M. S. de, Ferreira, R. S., & Feijó, N. (2025). Bases legais para o tratamento de dados: Uma análise comparativa entre a LGPD e o GDPR. *Revista Contemporânea*, *5*(9), e9065. https://doi.org/10.56083/RCV5N9-049

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly, 36*, 101385. https://doi.org/10.1016/j.giq.2019.06.002

Mugamba, M. (2025). Global data governance in digital law: A comparative analysis of EU and global approaches to cybersecurity. *Journal of Smart Computing and Quantum Technologies, 1*(1), 1–19. https://technology.tresearch.ee/index.php/JSCQT/article/view/39

Organização das Nações Unidas. (1948). *Declaração Universal dos Direitos Humanos*. https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos

Perrone, C., & Strassburger, S. (2018). Privacy and data protection: From Europe to Brazil. *Panorama of Brazilian Law, 6*(9-10), 82–100. https://www.e-publicacoes.uerj.br/pbl/article/view/38253

Phillips, B. (2021). UK further education sector journey to compliance with the general data protection regulation and the data protection act 2018. *Computer Law & Security Review*, *42*, 105586. https://doi.org/10.1016/j.clsr.2021.105586

Santos Neto, A. B., Ishikawa, L., & Maciel, M. (2021). O tratamento de dados pessoais pelo Poder Público e o papel dos Tribunais de Contas. *Revista Direitos Culturais*, *16*(40), 163-177. https://doi.org/10.20912/rdc.v16i40.604

Silva, L. C., & Ptaszek, P. (2025). The general data protection law: A study on a data management regulatory framework at university. *Zeszyty Naukowe Akademii Górnośląskiej, 27*(3), 12–22. https://doi.org/10.53259/2025.03.02

União Europeia. (2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados)*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5). https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html