

UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

ALEXANDRE GOMES DE SOUZA

**DESAFIOS E CONSEQUÊNCIAS DA NÃO CONFORMIDADE COM A LEI GERAL
PROTEÇÃO DE DADOS PESSOAIS (LGPD)**

JUAZEIRO DO NORTE-CE
2025

ALEXANDRE GOMES DE SOUZA

**DESAFIOS E CONSEQUÊNCIAS DA NÃO CONFORMIDADE COM A LEI GERAL
PROTEÇÃO DE DADOS PESSOAIS (LGPD)**

Trabalho de Conclusão de Curso – *Artigo Científico*,
apresentado à Coordenação do Curso de Graduação
em Direito do Centro Universitário Doutor Leão
Sampaio, em cumprimento às exigências para a
obtenção do grau de Bacharel.

Orientador: Esp. Francisco Gledison Lima Araujo

JUAZEIRO DO NORTE-CE
2025

ALEXANDRE GOMES DE SOUZA

**DESAFIOS E CONSEQUÊNCIAS DA NÃO CONFORMIDADE COM A LEI GERAL
PROTEÇÃO DE DADOS PESSOAIS (LGPD)**

Este exemplar corresponde à redação final aprovada do
Trabalho de Conclusão de Curso de ALEXANDRE
GOMES DE SOUZA.

Data da Apresentação 20/06/2025

BANCA EXAMINADORA

Orientador: Esp. Francisco Gledison Lima Araujo

Membro: Me. Francisco Thiago da Silva Mendes

Membro: Esp. André Carvalho Barreto

JUAZEIRO DO NORTE-CE
2025

DESAFIOS E CONSEQUÊNCIAS DA NÃO CONFORMIDADE COM A LEI GERAL PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Alexandre Gomes de Souza¹
Francisco Gledison Lima Araujo²

RESUMO

O presente trabalho tem como objetivo analisar a Lei Geral de Proteção de Dados (LGPD), com foco nos desafios enfrentados por organizações em sua implementação, bem como nas consequências da não conformidade com a legislação. A pesquisa adota abordagem qualitativa, de natureza básica e pura, por meio de revisão bibliográfica e análise de legislações, artigos acadêmicos e relatórios técnicos. Observa-se que, mesmo após anos de vigência da LGPD, diversas instituições ainda enfrentam dificuldades significativas de adequação, seja por falta de infraestrutura, cultura organizacional voltada à proteção de dados, ou ausência de capacitação de colaboradores. A atuação da Autoridade Nacional de Proteção de Dados (ANPD), embora relevante, ainda é insuficiente para garantir o cumprimento amplo da lei. Os riscos da não conformidade incluem sanções administrativas, multas elevadas e responsabilidade civil. Observa-se que a efetividade da LGPD depende da integração entre regulação, fiscalização e conscientização, exigindo esforços contínuos de empresas, órgãos públicos e sociedade civil. O presente estudo de pesquisa contribui para o debate acadêmico ao refletir sobre entraves práticos da aplicação da LGPD e reforçar a importância da cultura de proteção de dados no Brasil.

Palavras-Chave: Conformidade. Desafios. Implementação. Privacidade. Responsabilidade Civil. Segurança da informação.

1 INTRODUÇÃO

O ano de 2014 foi marca fundamental para a legislação digital no Brasil com a promulgação do Marco Civil da Internet (Lei nº 12.965/2014), ou seja, a edição de lei infraconstitucional que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, não apenas reforçando o direito a livre expressão e a proteção de dados, mas padronizando as políticas de proteção, assegurando o tratamento de dados pelos provedores. O Marco Civil da Internet tornou-se assim, um pilar para a legislação digital e segurança jurídica dos cidadãos.

Apesar disso, em 2020, uma falha no sistema do Ministério da Saúde expôs cerca de 243 milhões de informações de brasileiros na internet, conforme os dados reportados pelo jornal

¹ Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão-alexandregomesdesouza934@gmail.com

² Professor do Centro Universitário Doutor Leão Sampaio/UNILEÃO, Bacharel em Direito pelo Centro Universitário Dr. Leão Sampaio, Mestrando em Direito Constitucional pela UNIFIEO-SP, Especialista em Direito Digital e Nova Tecnologias do Direito_CEDIN-BH_franciscogledison@leaosampaio.edu.br

G1 (2020). Tal fato se deu seis anos após o marco civil da internet, o que demonstra a dificuldade de implementação de políticas de segurança e proteção de dados dentro das organizações não apenas públicas, mas também as instituições privadas, assim como a carência de uma cultura de proteção de dados no país.

Nesse contexto, torna-se necessário aprimorar os mecanismos de segurança cibernética para evitar que os dados pessoais sensíveis sejam comprometidos e a implementação efetiva de políticas regulatórias, como a Lei Geral de Proteção de Dados (LGPD) bem como, um esforço contínuo para a adaptar as políticas de segurança à crescente complexidade do ambiente digital.

A adequação das normas de proteção de dados – Lei Geral de Proteção de Dados (LGPD), e a Lei (Lei nº 12.965/2014) – tem se mostrado um desafio significativo para muitas organizações no Brasil. Conforme apontado por Bioni (2016), a proteção de dados pessoais no país pode ser interpretada como um verdadeiro jogo de xadrez, no qual o legislador, as empresas e a sociedade civil estão continuamente em movimento, tentando encontrar o equilíbrio entre a proteção da privacidade e o desenvolvimento econômico.

Nesse contexto, quais são os principais desafios enfrentados na implementação da LGPD no Brasil e as consequências da não conformidade com a LGPD?

O presente trabalho tem como objetivo geral compreender a Lei Geral de Proteção de Dados (LGPD), com ênfase nos desafios enfrentados em sua implementação e nas consequências decorrentes da não observância de suas disposições.

Para alcançar esse propósito, busca-se, através dos objetivos específicos, analisar os principais conceitos e princípios que estruturam a LGPD, bem como os fundamentos jurídicos que autorizam o tratamento de dados pessoais, com atenção especial aos direitos dos titulares e às responsabilidades atribuídas aos controladores e operadores.

Além disso, pretende-se identificar os obstáculos mais comuns enfrentados pelas organizações no processo de adequação à norma, tais como a necessidade de mudanças culturais, a complexidade técnica das medidas exigidas e os custos envolvidos nesse processo.

Ademais de identificar as consequências da não implementação das normas da LGPD. Por fim, o estudo visa refletir sobre os riscos e impactos legais, econômicos e reputacionais que podem decorrer da inobservância da legislação.

Nesse contexto, o presente estudo tem como foco a influência da LGPD na proteção de dados pessoais e quais os desafios para sua aplicação dentro da sociedade, haja vista que apesar da existência da presente lei e de normas anexas ainda há muita dificuldade na implementação de suas diretrizes dentro da sociedade, seja em empresas, órgãos públicos ou mesmo no dia a dia dos indivíduos.

Estudo como o aqui proposto são fundamentais ao desenvolvimento do campo científico sob investigação, pois permite que, a partir de uma síntese mais aprofundada, surjam compreensões acerca do tema, facilitando as formas de aplicação na prática da LGPD, na sociedade e com isso, desburocratizando sua integração nas operações das organizações e sua implementação na sociedade, com uma visão mais clara sobre os obstáculos e consequências. Assim será possível desenvolver abordagens mais consistentes para garantir a adequação e a efetiva proteção dos dados dos indivíduos.

Portanto, identificar e abordar esses obstáculos e consequências para garantir que a LGPD cumpra seu objetivo de proteger os dados pessoais de maneira eficiente em todo o país. Sendo assim, este trabalho justifica-se, principalmente pela contribuição que pode oferecer ao aprimoramento das políticas de proteção de dados e à conscientização sobre a importância da privacidade e proteção digital.

2 DESENVOLVIMENTO

2.1 METODOLOGIA

Na visão do autor Gil (2019), o método científico é um conjunto de regras e etapas estruturadas que conduzem o pesquisador a adquirir conhecimento confiável. Esse processo é fundamental para minimizar a subjetividade e aproximar o conhecimento obtido da realidade empírica, permitindo que novas descobertas sejam feitas e que o conhecimento existente seja corrigido e aprimorado. O método científico, portanto, representa um caminho rigoroso e organizado para alcançar a objetividade e a validade nas investigações.

Para buscas detalhadas, como fonte de pesquisa, foram empregados os descritores: LGPD. Desafios. Implementação. Adequação. Proteção de dados. vinculados aos operadores booleanos AND e OR. Utilizou-se diversas bases de dados, como CAPES, Google Acadêmico e Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), além de sites de notícias como G1, CNN Brasil e UOL Notícias, entre outros. As listas de referência dos artigos incluídos também foram examinadas para identificar artigos relevantes não encontrados nas pesquisas eletrônicas.

A questão que orientou a busca por artigos nesta revisão foi: quais são os principais desafios enfrentados na implementação da LGPD no Brasil e as consequências da não conformidade com a LGPD?

Sendo assim, este estudo tem uma natureza básica e pura, pois objetiva ampliar o conhecimento teórico sobre o tema, sem a intenção de aplicabilidade direta, focando na análise conceitual e na reflexão acadêmica. Gerando conhecimento que, a longo prazo, contribuir para a resolução de problemas sociais, tecnológicos ou econômicos, buscando avanços significativos.

A análise das informações foi realizada por meio de uma pesquisa exploratória que visa desenvolver e aprimorar conceitos, bem como esclarecer ideias para a formulação o desenvolvimento da LGPD no Brasil. Este tipo de pesquisa busca desenvolver, esclarecer e aperfeiçoar conceitos e ideias, visando à formulação de problemas mais bem definidos ou de hipóteses a serem verificadas em estudos futuros (Gil, 2019).

Aplicando uma abordagem qualitativa, que Gil descreve como “As pesquisas qualitativas, por sua vez, caracterizam-se pela utilização de dados qualitativos, com o propósito de estudar a experiência vivida das pessoas e ambientes sociais complexos, segundo a perspectiva dos próprios atores sociais., ou seja, busca compreender a complexidade de tal fenômeno por meio de interpretações pré-existentes.

2.2 REFERENCIAL TEÓRICO

2.2.1 Contexto Histórico da Lei Geral de Proteção de dados (LGPD)

Com o significativo avanço da tecnologia e da comunicação em massa a proteção de dados pessoais surgiu como um tema central nas discurso sobre direitos fundamentais, privacidade e segurança na era digital. O conceito de privacidade remonta a várias décadas, conforme Russo (2019), entende-se, assim, que a privacidade pode ser definida como o controle absoluto dos indivíduos sobre a exposição de dados pessoais de naturezas distintas que possam identificá-los.

Em 1824, a Constituição do Império reconhecia o direito à privacidade ao proteger o “segredo da carta” e a “inviolabilidade da casa”. No entanto, naquele momento, a privacidade estava vinculada a um conceito mais fundamentado na propriedade; ou seja, a carta magna protegia o meio físico, e não o conteúdo em si. (Dias de Paula, 2024)

Sendo assim, a privacidade evoluiu de uma ideia limitada à proteção da vida privada e a propriedade para uma concepção mais ampla, na qual o indivíduo exerce total controle sobre seus dados pessoais, especialmente quanto à coleta, uso e disseminação dessas informações no

ambiente digital. Portanto, privacidade não se limita a estar sozinho, mas a controlar como seus dados são utilizados por terceiros.

No Brasil, o direito à privacidade configura-se como princípio fundamental, reconhecido na Constituição Federal de 1988, em seu artigo 5º, inciso X, que considera invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas. (Brasil, 1988). Porém, com o avanço da tecnologia e das mídias sociais, tornou-se necessário desenvolver novos controles e regulações específicas.

No âmbito internacional, o marco inicial para a proteção de dados foi o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que entrou em vigor em 2018, servindo de modelo para legislações ao redor do mundo, mas também evidenciando a urgência de uma legislação regulamentar complexa para a proteção de dados pessoais no ambiente digital. (Feiler, et al. 2024). Já no Brasil, seguindo a GDPR, foi promulgado o Marco Civil da Internet (Lei nº 12.965 de 2014), que estabeleceu os princípios e direitos relacionados à privacidade e proteção de dados na internet.

O Marco Civil da Internet, frequentemente chamado de a constituição da internet brasileira representou um avanço significativo no desenvolvimento da legislação cibernética. Segundo Ibraim (2022), o Marco Civil da Internet foi crucial para salvaguardar as informações pessoais e assegurar a privacidade digital. Ela definiu os princípios fundamentais, como a proteção à vida privada e a responsabilidade civil dos provedores de internet, evidenciando a demanda crescente por regulação em um cenário onde a informação é propagada de forma intensa e sem controle adequado.

No entanto, o Marco Civil da Internet, isoladamente, não é suficiente para garantir a proteção completa dos dados pessoais, sendo necessário o suporte de outras legislações (Ibraim, 2022). Com isso, e com o avanço da comunicação em massa, em 2018 é criada a LGPD, que estabelece um sistema mais robusto para assegurar os direitos dos usuários e proteger suas privacidades de maneira abrangente.

2.2.2 Princípios da Lei Geral de Proteção de dados LGPD

A Lei Geral de Proteção de dados (Lei 13.709/2018) define dados pessoais, em seu artigo 5º, inciso I, como qualquer informação sobre uma pessoa identificada ou identificável, desde dados como número de documentos até aqueles que, combinados com outras informações, podem identificar um indivíduo, como dados de localização, dados de contas, características físicas e psicológicas, ou seja, qualquer informação que possa identificar um

indivíduo direta ou indiretamente. Já para Dados Sensíveis, no seu artigo 5º, inciso II, são como uma subcategoria de dados pessoais que requerem uma proteção maior devido à sua natureza íntima, envolvendo aspectos da vida do indivíduo, como opiniões políticas, filiação, religião, dados biométricos, entre outros.

Segundo Russo (2019), neste contexto em que a coleta de informações ocorre quase automaticamente e o uso da internet se torna cada vez mais comum e indispensável em todo o mundo, é fundamental discutir a compatibilidade entre a proteção dos dados pessoais dos usuários e o uso adequado, transparente e consciente dessas informações pelas empresas. Dessa forma, a LGPD determina, em seu artigo 6º, princípios para a proteção de dados pessoais, como adequação, necessidade, finalidade, entre outros.

Sendo assim, os dados pessoais devem ser utilizados para uma finalidade específica, informada ao usuário/indivíduo, de modo a impedir quaisquer usos para outros fins, sem uma justificativa razoável ou sem autorização do proprietário dos dados. (Bioni; Silva; Martins, 2022). Observa-se, com isso, que a LGPD, por meio do princípio da finalidade, exige que o processamento de dados seja conduzido dentro de um limite, previamente determinado e que seja de conhecimento do titular, impedindo assim que dados adquiridos sejam utilizados de forma irregular e indiscriminada, atuando como uma barreira contra as práticas abusivas dos possuidores dos dados, firmando a segurança do titular dos dados e a transparência do controlador. (Bioni; Silva; Martins, 2022)

Ademais, o princípio da adequação, previsto no art. 6º, III, da Lei Geral de Proteção de dados (Brasil, 2018), estabelece que o tratamento de dados pessoais deve ser compatível com a finalidade original informada ao titular, respeitando o contexto da coleta e evitando usos desproporcionais ou desalinhados com o objetivo inicial (Bioni; Silva; Martins, 2022). Nesse sentido, a adequação exige que os dados coletados estejam diretamente vinculados à finalidade declarada, reforçando a transparência e a confiança na relação entre controlador e titular (Getprivacy, 2023). Complementarmente, o princípio da necessidade (art. 6º, IV, LGPD) determina que apenas os dados essenciais para alcançar a finalidade pretendida devem ser tratados, atuando como um filtro contra o excesso de coleta e armazenamento (Feiler et al., 2024) ao tratar das hipóteses de exclusão de dados pessoais. Assim, ambos os princípios funcionam como pilares éticos e legais para garantir que o tratamento de dados equilibre eficiência e respeito aos direitos fundamentais.

Esses princípios estabelecem diretrizes para o processamento ético e responsável de dados, propondo um equilíbrio na coleta e no tratamento dessas informações. Enquanto o princípio da finalidade traz um propósito específico para a coleta, a adequação limita o

tratamento e a coleta ao que é compatível com essa finalidade, e a necessidade, por sua vez, restringe o a quantidade de dados à sua finalidade. Complementando-se, os três princípios tornam-se pilares para a forma de coleta e tratamento de dados pessoais.

Mister dizer ainda que a Lei Geral de Proteção de Dados (LGPD) traz diversos outros princípios que se complementam, como o princípio da transparência ou publicidade, que garante aos titulares dos dados a compreensão de como suas informações são coletadas, utilizadas e compartilhadas. (Lei 13.709/2018). Assim, assegura a exatidão, clareza, relevância e atualização dos dados conforme a necessidade (Garcel, et al. 2023). E, com isso, por meio do princípio do livre acesso, os titulares têm assegurado o direito de acessar seus dados pessoais, mantendo autonomia sobre suas informações.

De forma interligada, a qualidade dos dados é essencial, exigindo que as informações sejam precisas, relevantes e atualizadas, evitando que dados incorretos comprometam a integridade do tratamento. O princípio da segurança, por sua vez, implica a adoção de medidas técnicas e administrativas adequadas para a proteção contra acessos não autorizados, ameaças e vazamentos, garantindo a integridade das informações. (Lei 13.709/2018). Ou seja, a criação e administração de um sistema abrangente e eficaz de governança e gestão de riscos relacionados à segurança da informação, que considere a complexidade dos desafios envolvidos na proteção de dados (Garcel, et al. 2023). Adicionalmente, o princípio da prevenção abrange a ideia de que responsável pelos dados deve implementar medidas e políticas qualitativas de forma antecipada, visando evitar possíveis danos decorrentes do tratamento das informações. (Garcel, et al. 2023), ou seja, promover ações para evitar ocorrências que prejudiquem os dados do titular e, conseqüentemente, a pessoa física. E, por fim, o princípio da não discriminação assegura que os dados não sejam utilizados para fins discriminatórios ou que prejudiquem a integridade do titular. (Lei nº 13.709/2018).

Esses princípios são essenciais para a proteção, tratamento e coleta de dados, pois garantem os direitos fundamentais dos titulares, conforme previsto no art. 1º da LGPD (Brasil, 2018) e no art. 5º, inciso LXXIX da Constituição Federal (Brasil, 1988).

Esses princípios são essenciais para a proteção, coleta e tratamento de informações, pois garantem os direitos fundamentais dos titulares, orientam as bases para o tratamento e a regulamentação dos dados, promovem a responsabilidade e a ética no uso de dados pessoais, e contribuem para a implementação de diretrizes, normas e práticas de proteção e utilização de dados.

2.2.3 Da implementação da Lei Geral de Proteção de dados no Brasil

Destaca-se, nesse contexto, o tripé fundamental da proteção de dados pessoais, composto por regulação, fiscalização e conscientização. Esses três pilares são indispensáveis para que o legislador exerça seu papel de forma eficaz na consolidação de uma cultura voltada à privacidade e à segurança da informação. A implementação da Lei Geral de Proteção de Dados (LGPD) pode ser comparada a um jogo de xadrez, em que cada movimento deve ser cuidadosamente calculado. (Bioni, 2016).

Nesse tabuleiro, o legislador, as empresas e a sociedade civil assumem papéis estratégicos e interdependentes, movimentando-se constantemente em busca do equilíbrio entre a salvaguarda da privacidade individual e os interesses relacionados ao desenvolvimento econômico e à inovação tecnológica. Isso reforça a complexidade do cenário atual, no qual decisões equivocadas podem comprometer direitos fundamentais, enquanto escolhas acertadas fortalecem a confiança no uso responsável dos dados. (Bioni, 2016).

Conforme o Guia da LGPD do Governo Digital (Brasil, 2023), é fundamental que as organizações adotem práticas de segurança da informação para proteger os dados pessoais. Essas ações devem ser estabelecidas com base em uma política interna clara, que defina orientações e processos específicos para a prevenção de riscos e a correta gestão dos dados. A segurança deve ser considerada um elemento fundamental da governança organizacional.

Em 31 de maio de 2023, e atualizado em 24 de fevereiro de 2025, o Ministério da Economia realizou um questionário com o objetivo de diagnosticar o atual estágio de adequação à LGPD nas organizações, apresentando os seguintes dados:

Tabela 1 – Nível de adequação das organizações à LGPD

Índice	Nível de Adequação
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Fonte: Adaptado de Ministério da Economia. Relatório de Diagnóstico – Adequação à LGPD. Atualizado em 24 fev. 2025.

No contexto atual, fica claro que empresas e organizações, sejam elas públicas ou privadas, estão empenhadas em cumprir as demandas da LGPD e seus princípios básicos. No entanto, esse processo de adequação tem se mostrado desafiador, uma vez que esbarra em diversas barreiras, como a ausência de cultura organizacional voltada à proteção de dados, as dificuldades na revisão de processos internos, a falta de profissionais especializados e

limitações orçamentárias para implementação de medidas técnicas e administrativas exigidas pela legislação.

2.2.4 Das dificuldades na implementação

Com isso, a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil impõe desafios substanciais às empresas, especialmente em termos de adaptação cultural, investimentos em infraestrutura e ajustes na gestão de dados pessoais (Lec, 2024). Com isso, mesmo que a legislação apresente princípios, formas e materialidade, a sua implementação se torna repleta de desafios, dada a alta complexidade da mudança e da adaptação social e empresarial necessárias.

Segundo Reis (2023), aborda os principais desafios que as empresas enfrentam no processo de adequação à LGPD e apresenta as soluções necessárias para garantir a conformidade com a legislação, além de assegurar a proteção da privacidade dos dados pessoais de seus clientes. São elas:

- a) falta de conscientização das empresas;
- b) ausência de treinamento dos colaboradores;
- c) necessidade de avaliação dos processos internos;
- d) falta de investimento em cibersegurança;
- e) custos elevados para implementação da LGPD.

Nesse sentido, Saraiva; Souza; Soares (2024) demonstram que a complexidade da lei envolve também aspectos jurídicos, de segurança da informação e de governança, o que demanda investimentos significativos em políticas, auditorias e modelos de maturidade, além da contratação de equipes especializadas.

Este contexto representa um desafio adicional para pequenas e médias empresas, que frequentemente não dispõem de recursos financeiros e humanos suficientes para implementar as medidas de proteção exigidas. A implementação da LGPD tem sido vista como um obstáculo considerável para as empresas, especialmente as de pequeno e médio porte, que precisam investir em infraestrutura, adaptação de procedimentos e capacitação. Para muitas, a necessidade de suporte especializado eleva o custo da conformidade, dificultando a adaptação plena à legislação (Reis, 2023).

A partir disso, pode-se observar que a implementação da LGPD no Brasil não é apenas uma questão de regulamentação e adequação, mas também de suporte financeiro, o que evidencia que a proteção de dados, embora crucial, requer recursos que muitas empresas e

órgãos públicos não conseguem dispor. Segundo Teles (2024) Em contextos de austeridade fiscal, destinar recursos para adequação tecnológica, capacitação e criação de mecanismos de controle torna-se um grande desafio, especialmente para pequenas prefeituras e estados com sérias dificuldades financeiras, que enfrentam uma legislação exigente sem os meios adequados para cumpri-la.

Com necessidade de investimento em infraestrutura e capacitação, aderir à Lei Geral de Proteção de Dados (LGPD) pode se tornar oneroso e custoso para algumas empresas, o que pode levá-las a negligenciar a adequação às normas. Assim, para que algumas empresas e órgãos públicos consigam custear a adequação e o cumprimento da legislação, é evidente que necessitam de suporte, seja governamental ou por meio de parcerias e capacitação.

Referente às dificuldades na implementação da LGPD, ainda podemos citar Santos (2021) afirma que a supervisão da Lei Geral de Proteção de dados pela ANPD — Autoridade Nacional de Proteção de Dados — é um processo intrincado, que inclui não só a imposição de penalidades, mas também a obrigação de instruir e conscientizar as empresas acerca da proteção de dados. O papel da Autoridade Nacional de Proteção de Dados (ANPD) deve equilibrar a aplicação de penalidades com a promoção de práticas exemplares, garantindo a efetividade da lei sem desestimular o mercado.

As sanções aplicadas e desenvolvidas pela ANPD – Autoridade Nacional de Proteção de Dados – devem buscar não apenas que organizações, indivíduos e empresas cumpram a legislação, mas também que compreendam a importância e a necessidade da proteção de dados nos dias atuais. Ao aplicar sanções de forma educativa, pode não só garantir o cumprimento da legislação, mas promover boas práticas de proteção de dados. (Santos, 2021)

A falta de diretrizes claras por parte da Autoridade Nacional de Proteção de Dados (ANPD) contribui para as dificuldades na implementação da LGPD. Embora o órgão tenha emitido algumas orientações e resoluções, elas ainda são insuficientes, gerando incertezas, confusão e inércia por parte dos órgãos envolvidos. Soma-se a isso a capacidade de acompanhamento e fiscalização da Autoridade Nacional de Proteção de Dados (ANPD), que ainda está em fase de desenvolvimento. (Teles, 2024)

2.2.5 Da cultura organizacional

Além disso, Farina, Antunes (2023) afirmam que a aplicação da LGPD exige uma transformação cultural, conscientização e treinamento adequados, pois muitos funcionários ainda não compreendem a importância da proteção de dados. Portanto, as empresas devem

investir na sensibilização e organização interna para que a privacidade seja considerada prioritária e compreendida em todos os níveis da organização.

A concretização da Lei Geral de Proteção de dados (LGPD) na sociedade e nas empresas é fundamental para sua eficácia, tornando necessária a conscientização e a construção de uma cultura focada na privacidade e proteção dos dados pessoais. No âmbito empresarial, a proteção de dados não pode ser encarada apenas como uma legislação a ser cumprida, com consequentes sanções e penalidades, mas deve se tornar um direito, focado no seu objetivo principal: a construção de uma cultura voltada à proteção de dados. (Lugati; Almeida, 2022)

Entretanto, uma transição cultural requer tempo, comprometimento, fiscalização e programas de treinamento dos colaboradores, assim, as empresas garantem a segurança dos dados, diminuem os riscos de incidentes de segurança e evitam possíveis indenizações decorrentes de tal negligência.

Com isso, cresce a procura por profissionais da área, como os *Data Protection Officers* (DPOs), especialistas no processo de implementação da LGPD. Dessa forma, torna-se extremamente importante criar uma equipe qualificada para orientar as empresas, garantindo que estejam em conformidade com a legislação vigente. (Lugati; Almeida, 2022).

“As pesquisas realizadas vêm mostrando que um dos grandes causadores de incidentes de segurança é a falha humana.” (NDM Advogados, 2023).

Em artigo publicado pela NDM Advogados (2023), destaca-se que a comunicação interna e o treinamento dos colaboradores são pilares essenciais para a adequação à LGPD. Essas ações visam conscientizar todos os membros da organização sobre a importância da proteção de dados e da segurança da informação, permitindo que cada funcionário contribua ativamente para a continuidade e eficácia desse processo.

Reforçando essa ideia, a Autoridade Nacional de Proteção de Dados (ANPD) publicou um Guia voltado à segurança da informação para agentes de tratamento de pequeno porte, no qual destaca que uma das principais medidas administrativas é exatamente a conscientização e o treinamento dos colaboradores, para que estejam cientes de suas obrigações e responsabilidades quanto ao direito à privacidade e ao tratamento de dados pessoais. (Brasil; ANPD, 2021)

Dessa forma, os treinamentos tornam-se cruciais para que os colaboradores contribuam no processo de adequação à Lei Geral de Proteção de dados, ajudando a prevenir sanções. Além disso, por serem titulares de dados pessoais, é fundamental que compreendam seus direitos e deveres, especialmente o princípio da “autodeterminação informativa”, previsto na legislação. (NDM Advogados, 2023). (Lei 13.709/ 2018)

2.2.6 Riscos associados à não conformidade com a legislação.

No ano de 2023, a Autoridade Nacional de Proteção de Dados – ANPD, emitiu o Regulamento de Dosimetria e Aplicação de Sanções Administrativas, que regula a aplicação de multas às empresas por descumprimento da Lei Geral de Proteção de dados (LGPD). O regulamento tem como base os limites previstos na própria lei, que estabelece sanções financeiras de até R\$ 50.000.000,00 por infração. (ANPD, 2023)

A Lei Geral de Proteção de dados prevê dois tipos de sanções pecuniárias: a multa simples, que pode chegar a até 2% do faturamento da pessoa jurídica de direito privado, incluindo grupos ou conglomerados com atuação no país, no último exercício; e a multa diária. Ambas devem respeitar o limite máximo estabelecido no artigo 52, inciso II, da LGPD, fixado em R\$ 50.000.000,00 por infração. Brasil. (ANPD, 2023)

No entanto, além das multas, o legislador previu outras sanções aplicáveis em caso de violação à LGPD.

- a) advertência, com indicação de prazo para adoção de medidas corretivas;
- b) publicização da infração após devidamente apurada e confirmada;
- c) bloqueio dos dados pessoais relacionados à infração até a sua regularização;
- d) eliminação dos dados pessoais a que se refere a infração;
- e) suspensão parcial do funcionamento do banco de dados objeto da infração, pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- f) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração, pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- g) proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

Convém destacar que tais sanções só serão aplicadas após a instauração de procedimento administrativo que assegure o direito ao contraditório e à ampla defesa. A aplicação das penalidades poderá ocorrer de forma gradual, isolada ou cumulativa, conforme as circunstâncias do caso concreto. Para isso, são considerados os critérios: (i) a gravidade e a natureza da infração, além dos direitos pessoais afetados; (ii) a boa-fé do infrator; (iii) a vantagem obtida ou pretendida; entre outros fatores relevantes. Brasil. LGPD (Lei Geral de Proteção de Dados, 2019)

Esses critérios estão detalhados no Regulamento de Dosimetria e Aplicação de Sanções Administrativas, que estabelece com precisão as penalidades previstas e detalha os parâmetros para sua aplicação. (Brasil; ANPD 2023)

Esses critérios visam assegurar a proporcionalidade das sanções e reforçar a proteção jurídica nos procedimentos de fiscalização, garantindo o contraditório e o devido processo legal, além de incentivar a aplicação de medidas que não sejam exclusivamente punitivas, mas também orientativas e corretivas. (ANPD, 2023)

2.2.7 Da responsabilidade civil dos operadores

Considerando que a ausência de reparação de um dano ou prejuízo pode causar desordem social, a responsabilidade civil tem como finalidade principal restabelecer o equilíbrio patrimonial e moral afetado pelo agente que originou o dano.

Assim, cabe à responsabilidade civil, prioritariamente, promover a compensação pelos prejuízos sofridos ou pelos danos indevidamente causados, entendida por Tepedino, Terra e Guedes como a "violação de um interesse jurídico digno de proteção". como "lesão a interesse jurídico merecedor de tutela" (Tepedino; Terra; Guedes, apud Machado, 2021)

A Lei Geral de Proteção de dados (LGPD) estabelece, no capítulo VI, seção II, artigos 42 a 45, as normas que disciplinam a responsabilidade civil dos agentes de tratamento de dados. O art. 42 da LGPD determina que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". (Brasil, 2018).

Observa-se que o art. 42 não restringe a condição de vítima apenas ao titular dos dados, abrangendo qualquer indivíduo que tenha sofrido prejuízos em razão do descumprimento das normas de proteção de dados. (Machado, 2021).

Entende-se por "legislação de proteção de dados" um microssistema de proteção composto por vários os dispositivos legais, entre eles as normas administrativas editadas pela ANPD, tendo a Lei Geral de Proteção de dados como fundamento, para a aplicação desse conjunto normativo. (Machado, 2021).

Ambos os incisos do §1º do artigo 42 da LGPD expressam a responsabilidade solidária para garantir a responsabilização e segurança dos proprietários dos dados pessoais. O inciso I expressa que "o operador responde solidariamente como controlador quando": (i) descumprir

as obrigações da legislação de proteção de dados”; ou (ii) “não tiver seguido as instruções lícitas do controlador”. (LGPD, 2018)

No caso do inciso II, do §1º, expressa que, em caso de múltiplos operadores, eles responderão solidariamente se “diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados”. (LGPD, 2018).

Já o art. 43 traz as situações de exclusão de responsabilidade: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não violaram a legislação de proteção de dados; ou III - que o dano decorre de culpa exclusiva do titular dos dados ou de terceiros. (LGPD, 2018)

Observa-se que, nesses casos, a responsabilidade do agente de tratamento é afastada porque não há ligação direta entre sua conduta e o dano sofrido pelo titular, ou porque, embora tenha ocorrido o tratamento de dados, não houve violação da legislação, o que elimina a ilicitude da sua ação. Assim, faltam componentes fundamentais para a caracterização da responsabilidade civil. (Machado, 2021).

Em linhas gerais, a LGPD estabelece duas circunstâncias que definem a responsabilidade civil dos operadores: violação de regras jurídicas (do microssistema de proteção de dados) e violação de diretrizes técnicas relacionadas à segurança e proteção aos dados pessoais e o descumprimento das normas técnicas referentes à segurança e à proteção de dados. No entanto, a responsabilização só se configura quando o descumprimento dessas normas resultar em “dano material ou moral a um titular ou a uma coletividade (Machado, 2021)

Apesar de apresentar a responsabilidade dos operadores a LGPD não especifica qual tipo deve ser adotado, predominando duas correntes doutrinárias: a objetiva e subjetiva.

Os que sustentam a teoria da responsabilidade objetiva na Lei Geral de Proteção de dados (LGPD) defendem que ela se aplica de forma análoga ao CDC, como a responsabilidade objetiva prevista no art. 42, § 2º, da LGPD, semelhante ao CDC, e o art. 44, cuja redação é similar ao § 1º do art. 14 do CDC.

Com isso, os defensores dessa doutrina entendem que a LGPD compreende que “o dever de reparar o dano estaria vinculado à realização do tratamento de dados pessoais, que pode acarretar riscos aos direitos dos titulares desses dados”. (Machado, 2021).

Os defensores da teoria subjetivista fundamentam-se especialmente no art. 43 da LGPD, que estabelece hipóteses de exclusão de responsabilidade, indicando que a presunção de culpa é uma condição necessária para a responsabilização. Da mesma forma, os capítulos destinados

a boas práticas e os princípios expressos na lei. Ainda em determinadas situações, o legislador decidiu não expressar a culpa objetiva, como no artigo 44, onde condicionou a responsabilidade do operador apenas às situações em que não for possível comprovar que foram adotadas as medidas de segurança legalmente previstas. (Machado, 2021).

Dessa maneira, considerando que a legislação não prevê expressamente a adoção da responsabilidade objetiva e que os artigos relativos à responsabilização estabelecem condições específicas para sua incidência, entende-se que a Lei Geral de Proteção de dados (LGPD) adota a responsabilidade subjetiva. (Machado, 2021).

3 CONSIDERAÇÕES FINAIS

Na sociedade da informação, o reconhecimento da proteção de dados como um preceito fundamental e a edição da Lei Geral de Proteção de dados (LGPD) representa um marco na regularização e no tratamento de dados no Brasil, principalmente dentro da valoração social e econômico dos dados nos dias atuais. Com a finalidade de assegurar a privacidade e a liberdade dos indivíduos, estabelecendo requisitos, direitos e deveres voltados à proteção dos dados pessoais na sociedade. A LGPD traz também princípios que norteiam a proteção de dados, a qual torna-se essenciais para nortear a implementação da legislação.

A implementação da LGPD tem representado um grande desafio para os órgãos, seja público ou privado, especialmente no que diz respeito à adaptação cultural organizacional e aos custos envolvidos na criação de uma infraestrutura adequada. A complexidade das mudanças exigidas, que vão desde ajustes técnicos até transformações nos processos e na mentalidade institucional, tem dificultado a plena conformidade com a legislação. Mesmo após cinco anos desde a sua entrada em vigor, muitas instituições ainda enfrentam dificuldades para se ajustar integralmente, evidenciando que a mudança não se limita ao aspecto normativo, mas exige um verdadeiro comprometimento com a cultura da privacidade de dados.

A LGPD determina uma série de deveres e obrigações que devem ser rigorosamente cumpridos pelos agentes operadores de dados, sob pena de sanções administrativas e responsabilização civil. Essas sanções evidenciam a preocupação do legislador em assegurar a efetiva aplicação da Lei Geral de Proteção de Dados (LGPD) e a segurança dos dados pessoais dos titulares.

A responsabilidade recai principalmente sobre os controladores de dados, especialmente em caso violação de direitos de terceiros, descumprimento das obrigações previstas na

legislação ou negligência no cumprimento das instruções lícitas do controlador realizado pelos operadores, resultando na violação da proteção de dados.

No tocante à responsabilização civil prevista na LGPD, ainda não há consenso consolidado na doutrina. No entanto, observa-se que, embora a lei dialogue com princípios do CDC, ela adota o regime da responsabilidade subjetiva para os operadores de dados, exigindo, portanto, a comprovação de culpa para a sua responsabilização, em consonância com o sistema civilista brasileiro.

O presente estudo baseou-se em fontes confiáveis, como artigos científicos, legislações e publicações jornalísticas especializadas, com a finalidade de analisar os principais desafios enfrentados na aplicação das normas da LGPD, bem como as possíveis consequências decorrentes da não conformidade. Diante das incertezas relacionadas à aplicação prática da legislação e às implicações da responsabilidade civil, observa-se uma notável escassez de estudos aprofundados sobre o tema, especialmente no contexto brasileiro.

Nesse sentido, este trabalho busca contribuir para o debate acadêmico, oferecendo uma reflexão crítica sobre os entraves e riscos envolvidos na adaptação à LGPD. Espera-se, ainda, que os resultados aqui apresentados sirvam de subsídio tanto para futuras pesquisas quanto para auxiliar organizações a compreenderem melhor suas obrigações legais, promovendo a conformidade e fortalecendo a cultura de proteção de dados pessoais no país.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. **Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas**. *Diário Oficial da União*, Brasília, DF, 27 fev. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria>. Acesso em: 2 maio 2025.

BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. **Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso**. *Caderno Técnico do CGU*, [S. l.]: CGU, 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504. Acesso em: 26 out. 2024.

BIONI, B. R. **Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI-USP, 2016. Disponível em: <https://tinyurl.com/2ezbewzx>. Acesso em: 26 de out. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (**Lei Geral de Proteção de Dados Pessoais – LGPD**). *Diário Oficial da União*: seção 1, Brasília, DF, p. 1-10, 15 ago. 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 abril. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (**Marco Civil da Internet**). Diário Oficial da União: seção 1, Brasília, DF, p. 1-5, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 abril. 2024.

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**. Brasília: ANPD, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf>. Acesso em: 25 abr. 2025.

BRASIL. Governo Digital. **Guia da Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 30 out. 2023.

DATACENTERDYNAMICS. **Apenas 36% das organizações brasileiras afirmam estar totalmente aderentes à LGPD. 31 maio 2023**. Disponível em: <https://www.datacenterdynamics.com/br/not%C3%ADcias/apenas-36-das-organizacoes-brasileiras-afirmam-estar-totalmente-aderentes-a-lgpd/>. Acesso em: 24 abr. 2025.

DIAS DE PAULA, Andressa Gabrielly. **Lei Geral de Proteção de Dados: desafios e estratégias nas pessoas jurídicas**. 2024. Artigo (Trabalho de Curso) – Curso de Direito, Escola de Direito e Relações Internacionais, Pontifícia Universidade Católica de Goiás, Goiânia-GO, 17 maio 2024. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/7425/1/ARTIGO%20CIENTI%CC%81FICO%20ANDRESSA%20G%20DIAS.pdf>. Acesso em: 22 jun. 2025.

FARINA, Kariny Antunes; ANTÃO, Vanderlei Mendes. **Desafios na implementação da LGPD: maiores dificuldades para as empresas**. *Farina & Antunes Advocacia*, 31 jul. 2023. Disponível em: <https://farinaeantunes.com.br/blog/lgpd/desafios-na-implementacao-da-lgpd-maiores-dificuldades-para-as-empresas/>. Acesso em: 29 out. 2024.

FEILER, A. R.; GAZANIGA, F.; VIEIRA, T. A. M. **O valor fundamental dos dados pessoais: uma análise comparativa entre a LGPD e GDPR sob a ótica da análise econômica do direito**. *Revista de Direito*, [S. l.]: UFV, v.16, n.2, p.1–29, 2024. DOI: 10.32361/2024160217158. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/17158>. Acesso em: 16 nov. 2024.

G1. **Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal**. *G1*, 02 dez. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml>. Acesso em: 21 de out. 2024

GARCEL, Adriane; MORO, Sergio Fernando; NETTO, José Laurindo de Souza; HIPPERTT, Karen Paiva. **Lei Geral de Proteção de Dados: Diretrizes e Implicações para uma Sociedade Pandêmica**. *ResearchGate*, 2023. Disponível em:

https://www.researchgate.net/publication/367404962_LEI_GERAL_DE_PROTECAO_DE_DADOS_DIRETRIZES_E_IMPLICACOES_PARA_UMA_SOCIEDADE_PANDEMICA. Acesso em: 26 out. 2024.

GET PRIVACY. **10 princípios que norteiam o tratamento dos dados pessoais segundo a LGPD**. Disponível em: <https://getprivacy.com.br/10-principios-tratamento-de-dados-pessoais-lgpd/>. Acesso em: 22 jun. 2025.

GIL, Antonio C. **Métodos e Técnicas de Pesquisa Social**, 7ª edição. Rio de Janeiro: Atlas, 2019. E-book. p.30. ISBN 9788597020991. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788597020991/>. Acesso em: 21 out. 2024.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. **A LGPD e a construção de uma cultura de proteção de dados**. *Revista de Direito*, Viçosa: UFV, v.14, n.1, p.1–20, 2020. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/13764/7380>. Acesso em: 24 abr. 2025.

LEC. **LGPD: desafios e oportunidades em 2024**. LEC, 2024. Disponível em: <https://lec.com.br/lgpd-desafios-e-oportunidades-em-2024/>. Acesso em: 23 de out. 2024.

LGPD Brasil. **Aderência à LGPD: apenas 36% das empresas brasileiras estão em conformidade total**. 6 jun. 2023. Disponível em: <https://www.lgpdbrasil.com.br/aderencia-a-lgpd-apenas-36-das-empresas-brasileiras-estao-em-conformidade-total/>. Acesso em: 24 abr. 2025.

MACHADO, Gabriela. **A natureza da responsabilidade civil dos agentes de tratamento de dados pessoais na LGPD**. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) – Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2021. Disponível em: https://www.pucrs.br/direito/wp-content/uploads/sites/11/2022/02/gabriela_machado.pdf. Acesso em: 25 abr. 2025.

NETO, Ibraim Soares Siqueira. **Marco Civil da Internet: proteção de dados pessoais e o direito à privacidade**. *Conteúdo Jurídico*. Disponível em: <https://conteudojuridico.com.br/consulta/artigos/59599/o-marco-civil-da-internet-proteo-dos-dados-pessoais-e-o-direito-privacidade>. Acesso em: 25 out. 2024.

NDM ADVOGADOS. **Vazamento de dados: a importância dos treinamentos sobre proteção de dados para seus colaboradores**. *JusBrasil*, 26 jun. 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/vazamento-de-dados-a-importancia-dos-treinamentos-sobre-protecao-de-dados-para-seus-colaboradores/1830627368>. Acesso em: 25 abr. 2025.

REIS, Rafael. **Os desafios da implementação da LGPD em empresas brasileiras**. *Becker Direito Empresarial*, 31 maio 2023. Disponível em: <https://www.direitoempresarial.com.br/os-desafios-da-implementacao-da-lgpd-em-empresas-brasileiras>. Acesso em: 29 out. 2024.

RUSSO, Rogério Agueda. **A tutela da privacidade de dados na era do Big Data**. 2019. 136 f. Dissertação (Mestrado em Direito) – Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019. Disponível em: <https://tede2.pucsp.br/handle/handle/23113>. Acesso em: 23 de out. 2024

SANTOS, Camila Salles dos. **Processo de fiscalização e punição pela ANPD**. *Jusbrasil*, 29 out. 2021. Disponível em: <https://www.jusbrasil.com.br/artigos/processo-de-fiscalizacao-e-punicao-pela-anpd/1308455922>. Acesso em: 29 out. 2024.

SARAIVA, Juliana; SOUZA, Cleidson de; SOARES, Sérgio. **Desafios de Compliance da LGPD: Implantação na Indústria de Software Brasileira**. In: WORKSHOP SOBRE ASPECTOS SOCIAIS, HUMANOS E ECONÔMICOS DE SOFTWARE (WASHES), 9. , 2024, Brasília/DF. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2024 . p. 193-198. ISSN 2763-874X. DOI: <https://doi.org/10.5753/washes.2024.3079>.

TELES, Matheus de Sousa. **Desafios da implementação da LGPD nos órgãos públicos: um caminho para a proteção de dados no Brasil**. *Jus.com.br*, 1 out. 2024. Disponível em: <https://jus.com.br/artigos/111158/desafios-da-implementacao-da-lgpd-nos-orgaos-publicos-um-caminho-para-a-protecao-de-dados-no-brasil>. Acesso em: 24 abr. 2025.