XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

JÉSSICA FACHIN

GIOVANI AGOSTINI SAAVEDRA

D597
Direito, governança e novas tecnologias II[Recurso eletrônico on-line] organização CONPEDI
Coordenadores: Jéssica Fachin, Giovani Agostini Saavedra – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-305-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O XXXII Congresso Nacional do CONPEDI, realizado em parceria com o com a Universidade Presbiteriana Mackenzie-São Paulo, ocorreu nos dias 26, 27 e 28 de novembro de 2025, na cidade de São Paulo. O evento teve como temática central "Os Caminhos da Internacionalização e o Futuro do Direito". As discussões realizadas durante o encontro, tanto nas diversas abordagens jurídicas Grupos de Trabalho (GTs), foram de grande relevância, considerando a atualidade e importância do tema.

Nesta publicação, os trabalhos apresentados como artigos no Grupo de Trabalho "Direito, Governança e Novas Tecnologias II", no dia 26 de novembro de 2025, passaram por um processo de dupla avaliação cega realizada por doutores. A obra reúne os resultados de pesquisas desenvolvidas em diferentes Programas de Pós-Graduação em Direito, abordando uma parte significativa dos estudos produzidos no âmbito central do Grupo de Trabalho.

As temáticas abordadas refletem intensas e numerosas discussões que ocorrem em todo o Brasil. Elas destacam o aspecto humano da Inteligência Artificial, os desafios para a democracia e a aplicação do Direito no ciberespaço, bem como reflexões atuais e importantes sobre a regulação das plataformas digitais e as repercussões das novas tecnologias em diversas áreas da vida social.

Esperamos que, por meio da leitura dos textos, o leitor possa participar dessas discussões e obter um entendimento mais amplo sobre o assunto. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e na organização do evento, cujas contribuições inestimáveis foram fundamentais, e desejamos uma leitura proveitosa!

Profa. Dra. Jéssica Fachin – Universidade de Brasília/DF

Prof. Dr. Giovani Agostini Saavedra – Universidade Presbiteriana Mackenzie/SP

A IMPLEMENTAÇÃO DA LGPD EM INSTITUIÇÕES DE ENSINO SUPERIOR: UM ESTUDO DE CASO NA FATEC IVAIPORÃ/PR

THE IMPLEMENTATION OF THE LGPD IN HIGHER EDUCATION INSTITUTIONS: A CASE STUDY AT FATEC IVAIPORÃ/PR

Tainara Conti Peres [1]
Matheus Reuther de Barros [2]

Resumo

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, trouxe importantes mudanças para o tratamento de dados pessoais no Brasil, impactando diretamente as Instituições de Ensino Superior (IES). Este estudo analisa a implementação da LGPD na Faculdade de Tecnologia do Vale do Ivaí (Fatec), localizada em Ivaiporã/PR, com o objetivo de identificar os desafios enfrentados, as práticas adotadas e as lacunas existentes no processo de adequação à legislação. Por meio de uma abordagem qualitativa, foram realizadas entrevistas, análise documental e observação direta em setores estratégicos da instituição, como Recursos Humanos (RH), Tecnologia da Informação (TI) e Secretaria Acadêmica. Conclui-se que a implementação da LGPD na Fatec, embora desafiadora, representa uma oportunidade estratégica para fortalecer a governança de dados e a confiança da comunidade acadêmica. O estudo contribui para o entendimento das especificidades da aplicação da LGPD no contexto educacional e oferece subsídios para outras instituições enfrentarem desafios semelhantes.

Palavras-chave: Lgpd, Proteção de dados, Instituições de ensino superior, Governança de dados, Fatec ivaiporã

Abstract/Resumen/Résumé

The General Data Protection Law (LGPD), established by Law No. 13.709/2018, introduced profound changes to personal data processing in Brazil, significantly affecting Higher Education Institutions (HEIs). This study examines the implementation of LGPD at the Faculty of Technology of Vale do Ivaí (Fatec), located in Ivaiporã/PR, with the purpose of identifying challenges encountered, practices adopted, and gaps observed in the compliance process. Using a qualitative methodology, the research combined interviews, document analysis, and direct observation in essential institutional sectors such as Human Resources (HR), Information Technology (IT), and the Academic Office. The findings indicate that implementing LGPD at Fatec, although complex, represents not only a legal obligation but also a strategic opportunity to reinforce institutional data governance and foster trust within

[1] Doutoranda em Ciências Jurídicas pela Universidade Unicesumar (UNICESUMAR, Maringá/PR). Mestre em Direito, Sociedade e Tecnologia (Faculdades Londrina).

[2] Mestrando em Direito, Sociedade e Tecnologia (Faculdades Londrina).

the academic community. By analyzing this case, the study contributes to understanding the peculiarities of LGPD application in the educational context and provides practical insights for other institutions navigating similar compliance challenges.

Keywords/Palabras-claves/Mots-clés: Lgpd, Data protection, Higher education institutions, Data governance, Fatec ivaiporã

1. INTRODUÇÃO

A proteção de dados pessoais emergiu como um dos temas mais relevantes na era digital, especialmente em contextos onde grandes volumes de informações sensíveis são tratados diariamente, como ocorre nas Instituições de Ensino Superior (IES). No Brasil, a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/201, trouxe um marco regulatório que redefine as práticas de tratamento de dados, estabelecendo diretrizes rigorosas para assegurar a privacidade e a segurança das informações. No âmbito das IES, a LGPD assume papel estratégico, considerando o vasto volume de dados pessoais de estudantes, professores e trabalhadores que essas organizações gerenciam. A digitalização crescente das atividades acadêmicas e administrativas torna ainda mais urgente a necessidade de adequação a essa legislação, como forma de proteger os direitos fundamentais à privacidade e à autodeterminação informativa.

A importância da proteção de dados no setor educacional está diretamente relacionada à natureza sensível das informações tratadas pelas IES. Essas instituições lidam diariamente com dados como histórico acadêmico, informações financeiras, documentos pessoais, registros de saúde e até mesmo dados biométricos. A coleta, armazenamento e tratamento inadequados dessas informações podem resultar em violações graves, comprometendo a privacidade dos titulares e a credibilidade das instituições. Nesse contexto, a implementação de políticas de proteção de dados não é apenas uma exigência legal, mas também uma oportunidade para fortalecer a governança institucional e a relação de confiança com os diferentes públicos atendidos pelas IES, como estudantes, professores e a sociedade em geral.

A LGPD, sancionada em 14 de agosto de 2018, foi inspirada no Regulamento Geral de Proteção de Dados (*General Data Protection Regulation – GDPR*) da União Europeia, considerado um dos marcos mais avançados na proteção de dados pessoais no cenário global. A legislação brasileira estabelece princípios fundamentais para o tratamento de dados pessoais, como a finalidade, a transparência, a segurança e a responsabilização, além de garantir aos titulares uma série de direitos, incluindo o acesso, a correção e a exclusão de seus dados pessoais. No caso das IES, a conformidade com a LGPD exige a adoção de medidas técnicas e administrativas que assegurem a proteção das informações pessoais de seus públicos, promovendo a transparência e a segurança no tratamento de dados.

A relevância da LGPD para as IES é ainda mais evidente diante da crescente digitalização dos processos educacionais. O uso de plataformas digitais para gestão acadêmica,

ensino a distância e comunicação com os estudantes expõe as instituições a riscos significativos de segurança da informação. Vazamentos de dados, acessos não autorizados e usos indevidos de informações são apenas alguns dos desafios enfrentados por essas organizações. Além disso, a ausência de políticas claras de proteção de dados pode gerar sanções legais, danos reputacionais e perda de confiança por parte dos estudantes e da comunidade acadêmica. Assim, a implementação da LGPD nas IES não é apenas uma questão de conformidade legal, mas também uma oportunidade para promover a eficiência operacional e a credibilidade institucional.

O objetivo central deste artigo é analisar a implementação da LGPD na Faculdade de Tecnologia do Vale do Ivaí (Fatec), localizada no Município de Ivaiporã, Paraná, destacando os desafios enfrentados, as práticas adotadas e as lacunas existentes nesse processo. A Fatec[1], como principal polo educacional da região, atende mais de 1.200 estudantes e conta com uma equipe de aproximadamente 130 trabalhadores, gerenciando um volume significativo de informações sensíveis. A análise da aplicação da LGPD nessa instituição permite compreender as implicações práticas da legislação no contexto das IES, além de oferecer insights valiosos para outras organizações que buscam se adequar às exigências legais.

A escolha da Fatec como objeto de estudo é justificada por sua relevância regional e pelo papel estratégico que desempenha no desenvolvimento do Vale do Ivaí, uma região composta por 21 municípios. Como uma instituição de ensino de médio porte, a Fatec enfrenta desafios comuns a muitas IES brasileiras, especialmente aquelas localizadas em regiões menos favorecidas em termos de recursos tecnológicos e financeiros. Dessa forma, o estudo de caso da Fatec pode servir como referência para outras instituições que enfrentam dificuldades semelhantes, contribuindo para o avanço da governança de dados no setor educacional.

A justificativa para a realização deste estudo está ancorada em três dimensões principais: social, científica e histórica. Do ponto de vista social, a proteção de dados pessoais é um direito fundamental que visa assegurar a privacidade e a segurança dos indivíduos em uma sociedade cada vez mais conectada. No contexto educacional, a adequação à LGPD é essencial para proteger os direitos de estudantes, professores e trabalhadores, promovendo um ambiente de confiança e transparência. Sob a perspectiva científica, a análise da aplicação da LGPD em IES contribui para o avanço do conhecimento sobre governança de dados em organizações educacionais, um tema ainda pouco explorado na literatura acadêmica brasileira.

[1] A Fatec Ivaiporã é referência em cursos tecnológicos na região do Vale do Ivaí, abrangendo municípios com baixo índice de oferta de ensino superior público.

2. REFERENCIAL TEÓRICO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei n. 13.709/2018, representa um marco no ordenamento jurídico brasileiro, estabelecendo normas rigorosas para a proteção de dados pessoais e promovendo a segurança e privacidade em um contexto de crescente digitalização. Inspirada no Regulamento Geral de Proteção de Dados (*General Data Protection Regulation – GDPR*) da União Europeia, a LGPD trouxe diretrizes que impactam não apenas o setor privado, mas também instituições públicas, incluindo as Instituições de Ensino Superior (IES). No ambiente acadêmico, onde há o tratamento massivo de dados pessoais de estudantes, professores e funcionários, a adequação à LGPD apresenta desafios significativos, exigindo mudanças estruturais e culturais para garantir a conformidade legal.

2.1 CONCEITOS FUNDAMENTAIS DA LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi criada com o objetivo primordial de regular, de forma abrangente e detalhada, o tratamento de dados pessoais por pessoas naturais e jurídicas, sejam estas de direito público ou privado, estabelecendo diretrizes claras e uniformes para todas as entidades que, de alguma maneira, realizam operações envolvendo informações pessoais. Essa regulamentação visa, sobretudo, proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, reconhecendo que, em um contexto de crescente digitalização das relações sociais, econômicas e institucionais, o controle sobre os próprios dados se torna um elemento essencial para a garantia da dignidade humana e da autonomia individual (Brasil, 2018).

A lei define dados pessoais como qualquer informação relacionada à pessoa natural identificada ou identificável, o que abrange uma ampla gama de elementos, desde informações básicas, como nome completo, endereço residencial, número de telefone, endereço de e-mail, número do Cadastro de Pessoas Físicas (CPF) e data de nascimento, até dados considerados sensíveis, cuja exposição pode acarretar riscos significativos aos direitos e liberdades dos titulares. Entre os dados sensíveis, incluem-se informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, bem como dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural. Devido à sua natureza especialmente delicada e ao potencial de causar discriminação ou dano caso sejam utilizados de forma indevida, esses dados sensíveis recebem proteção ainda mais rigorosa, conforme

disposto no artigo 11 da LGPD, exigindo, por exemplo, consentimento específico e destacado do titular, além da adoção de medidas de segurança reforçadas (Almeida, 2020).

Entre os princípios fundamentais que norteiam a aplicação e a interpretação da LGPD, destacam-se, de maneira especial, a finalidade, a necessidade, a transparência, a segurança e a prevenção. O princípio da finalidade estabelece que o tratamento de dados deve ser realizado para propósitos legítimos, específicos, explícitos e previamente informados ao titular, impedindo que informações pessoais sejam utilizadas para fins genéricos, indeterminados ou incompatíveis com aqueles que motivaram sua coleta. O princípio da necessidade, por sua vez, limita a coleta e o armazenamento de dados ao mínimo indispensável para a realização das finalidades informadas, vedando a obtenção de informações excessivas ou desnecessárias, o que contribui para reduzir os riscos associados ao tratamento de dados pessoais. Quanto à transparência, este princípio exige que as organizações forneçam informações claras, precisas e facilmente acessíveis aos titulares sobre como seus dados estão sendo tratados, quais são as finalidades do tratamento, quem são os responsáveis, quais são os direitos dos titulares e como exercê-los, promovendo, assim, uma relação de confiança e accountability entre as partes envolvidas (Frazão; Oliva; Tepedino, 2019).

O princípio da segurança impõe a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Tais medidas podem incluir, entre outras, a utilização de criptografia, políticas de acesso restrito, treinamentos periódicos de colaboradores, realização de auditorias e implementação de planos de resposta a incidentes. Por fim, o princípio da prevenção determina a implementação de ações e mecanismos proativos que minimizem os riscos de ocorrência de danos aos titulares dos dados, incentivando a cultura de avaliação prévia de riscos e a adoção de boas práticas de governança em privacidade e proteção de dados (Frazão; Oliva; Tepedino, 2019).

A LGPD também introduz um conjunto de direitos importantes para os titulares dos dados, assegurando-lhes, entre outros, o direito de acesso aos próprios dados, o direito à correção de informações incompletas, inexatas ou desatualizadas, o direito à exclusão de dados desnecessários, excessivos ou tratados em desconformidade com a lei, o direito à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, e o direito de oposição ao tratamento de dados realizado com base em uma das hipóteses de dispensa de consentimento, em caso de descumprimento da legislação. Esses direitos conferem aos indivíduos um elevado grau de controle sobre suas informações pessoais, permitindo-lhes não apenas acompanhar e fiscalizar o tratamento de seus dados, mas também questionar, limitar ou

mesmo impedir determinadas operações realizadas por organizações públicas ou privadas (Almeida, 2020).

2.2 DIREITOS DOS TITULARES E OBRIGAÇÕES DAS INSTITUIÇÕES

Os direitos dos titulares de dados, previstos no artigo 18 da LGPD, representam um avanço significativo e inédito na proteção da privacidade e da autodeterminação informativa dos cidadãos brasileiros, conferindo-lhes um conjunto de prerrogativas que lhes permitem exercer controle efetivo sobre suas informações pessoais em um cenário de crescente digitalização e circulação de dados. Entre os principais direitos garantidos pela legislação, destacam-se: o direito de acesso, que permite ao titular obter informações claras, completas, precisas e facilmente compreensíveis sobre todo o ciclo de tratamento de seus dados (desde a coleta até o armazenamento, compartilhamento e eventual eliminação), incluindo a finalidade do tratamento, as categorias de dados tratados, os terceiros com os quais os dados possam ter sido compartilhados e o tempo de retenção dessas informações; o direito à correção, que possibilita a retificação imediata de informações incorretas, inexatas, incompletas ou desatualizadas, assegurando que os dados mantidos pelas organizações reflitam sempre a realidade e evitando, assim, prejuízos decorrentes do uso de informações equivocadas; o direito à exclusão, também conhecido como direito ao apagamento ou direito ao esquecimento, que autoriza o titular a solicitar, em determinadas circunstâncias previstas em lei, a eliminação de seus dados pessoais dos bancos de dados das organizações, especialmente quando o tratamento for fundamentado no consentimento e este for revogado, ou quando os dados forem considerados desnecessários, excessivos ou tratados em desconformidade com a legislação; e o direito à portabilidade, que assegura ao titular a possibilidade de transferir seus dados pessoais a outro fornecedor de serviços ou produtos, mediante solicitação expressa e de acordo com a regulamentação da Autoridade Nacional de Proteção de Dados (ANPD), promovendo, assim, a livre concorrência e a interoperabilidade entre diferentes plataformas e fornecedores (Doneda; Mendes; 2018).

Esses direitos, ao serem previstos de forma expressa e detalhada na LGPD, fortalecem de maneira substancial a posição dos titulares em relação às organizações que tratam seus dados, promovendo maior transparência, responsabilidade e *accountability* no tratamento de informações pessoais. Ao garantir que os titulares possam solicitar informações, correções, exclusões e transferências de seus dados de maneira simples e ágil, a legislação estimula as organizações a adotarem práticas mais transparentes, éticas e responsáveis, reduzindo

assimetrias informacionais e promovendo o respeito à privacidade como valor fundamental. Para garantir a efetividade desses direitos, a LGPD exige que as organizações estabeleçam canais de comunicação acessíveis, eficientes e adequados ao perfil dos titulares, por meio dos quais seja possível exercer suas prerrogativas de forma prática, célere e sem custos excessivos, evitando obstáculos burocráticos que possam inviabilizar ou dificultar o exercício desses direitos. Além disso, as instituições devem adotar medidas para assegurar a rastreabilidade e a documentação detalhada das operações de tratamento de dados, de modo a demonstrar, sempre que necessário, a conformidade com a legislação perante a Autoridade Nacional de Proteção de Dados (ANPD) e perante os próprios titulares, fornecendo registros que comprovem a origem, a finalidade e o destino dos dados, bem como eventuais compartilhamentos realizados (Doneda ; Mendes, 2018).

As obrigações das instituições que tratam dados pessoais incluem, ainda, a implementação de medidas técnicas e organizacionais adequadas, proporcionais e continuamente atualizadas para proteger as informações contra riscos de acessos não autorizados, vazamentos, destruição acidental ou ilícita, perda, alteração, comunicação inadequada e outras formas de tratamento inadequado ou ilícito. A adoção de políticas internas de governança de dados, que envolvem a definição de regras claras para o tratamento de dados pessoais, a delimitação de responsabilidades, a realização de treinamentos periódicos e a promoção de uma cultura organizacional voltada para a proteção da privacidade, é fundamental para assegurar a conformidade com a LGPD. A realização de avaliações de impacto à proteção de dados (AIPD), que consistem em análises sistemáticas e documentadas dos riscos e impactos potenciais decorrentes das operações de tratamento de dados, permite identificar vulnerabilidades, antecipar problemas e adotar medidas preventivas eficazes. A nomeação de um encarregado de proteção de dados (*Data Protection Officer – DPO),* responsável por atuar como canal de comunicação entre a organização, os titulares dos dados e a ANPD, bem como por orientar e fiscalizar as práticas internas de proteção de dados, é outro exemplo de prática recomendada e, em alguns casos, obrigatória para assegurar a conformidade e a responsabilização das instituições (Garcia et al., 2020).

No caso das Instituições de Ensino Superior (IES), essas obrigações são particularmente desafiadoras devido ao grande volume e à diversidade de dados tratados diariamente, que incluem não apenas informações acadêmicas, como histórico escolar, frequência, notas, avaliações, registros de matrícula, mas também dados financeiros relacionados a pagamentos, bolsas, contratos e inadimplências, além de, em muitos casos, dados sensíveis relacionados à saúde dos estudantes, como laudos médicos, atestados, informações sobre necessidades

especiais, uso de serviços de apoio psicológico e participação em programas de assistência estudantil. A implementação de medidas de proteção de dados em instituições educacionais exige não apenas investimentos em tecnologia, como a aquisição de sistemas seguros de gestão de dados, a utilização de ferramentas de criptografia, a realização de backups periódicos e a restrição de acessos, mas também mudanças culturais e organizacionais profundas, como a capacitação contínua de trabalhadores, professores, gestores e demais colaboradores para o uso seguro e ético das informações, a conscientização sobre a importância da privacidade e o desenvolvimento de uma cultura institucional de respeito à privacidade e à segurança da informação, transformando a proteção de dados em um valor compartilhado por toda a comunidade acadêmica (Stelzer et al., 2019).

2.3 DESAFIOS NA IMPLEMENTAÇÃO DA LGPD NAS IES

As IES enfrentam desafios específicos na implementação da LGPD, que vão desde a falta de recursos financeiros e tecnológicos até a ausência de uma cultura organizacional voltada para a proteção de dados, cenário que se agrava pela multiplicidade de setores, departamentos e fluxos informacionais presentes nessas instituições, tornando o processo de adequação ainda mais complexo e exigente. Um dos principais obstáculos é a conscientização dos trabalhadores sobre a importância da LGPD e a necessidade de adequação às suas diretrizes, sendo que a sensibilização de toda a comunidade acadêmica, incluindo docentes, técnicos administrativos, estagiários, prestadores de serviço e até mesmo os próprios estudantes, demanda esforços contínuos e estratégias pedagógicas específicas para que todos compreendam a relevância da privacidade, os riscos do tratamento inadequado de dados e as consequências legais e éticas decorrentes do descumprimento da legislação. Muitas vezes, os trabalhadores não possuem conhecimento suficiente sobre as implicações da lei e as melhores práticas para garantir a conformidade, o que pode levar a erros, omissões, vazamentos acidentais, compartilhamento indevido de informações e ao tratamento inadequado de informações pessoais, seja por desconhecimento das normas, seja pela ausência de rotinas e protocolos padronizados que orientem as atividades diárias de coleta, armazenamento, processamento, compartilhamento e descarte de dados dentro da instituição (Crespo, 2021).

Outro desafio importante é a integração das políticas de proteção de dados com os processos acadêmicos e administrativos das IES, já que muitos desses processos são historicamente estruturados sem considerar requisitos de privacidade e segurança, o que implica a necessidade de revisão, reengenharia e adaptação de fluxos de trabalho, formulários, sistemas

informatizados e procedimentos internos. A coleta de dados durante o processo de matrícula, por exemplo, deve ser realizada de forma transparente, informando claramente ao estudante quais dados estão sendo solicitados, para quais finalidades, com quem serão compartilhados e por quanto tempo serão armazenados, além de ser limitada ao mínimo necessário, conforme os princípios da LGPD, evitando a solicitação de dados irrelevantes ou excessivos. No entanto, a falta de sistemas integrados que centralizem e organizem o armazenamento das informações, bem como a ausência de ferramentas tecnológicas adequadas para monitorar acessos, rastrear operações e aplicar políticas de segurança, pode dificultar significativamente a implementação de medidas de segurança robustas e a gestão eficiente dos dados pessoais, resultando em fragmentação, duplicidade de registros, vulnerabilidades e dificuldades para atender prontamente às solicitações dos titulares, como pedidos de acesso, correção ou exclusão de dados (Crespo, 2021).

Além disso, as IES precisam lidar com a complexidade do tratamento de dados sensíveis, como informações de saúde de estudantes com necessidades especiais, dados psicológicos, laudos médicos, registros de acompanhamento pedagógico, dados socioeconômicos utilizados para concessão de bolsas de estudo, informações sobre orientação sexual, etnia, filiação religiosa ou política, e outras informações que, se expostas ou utilizadas de maneira inadequada, podem causar danos significativos, discriminação, estigmatização e violação da dignidade dos titulares. Esses dados exigem proteção adicional, incluindo consentimento específico, controles de acesso rigorosos, criptografia, anonimização, auditorias regulares e políticas de minimização de dados, e o tratamento inadequado pode resultar não apenas em violações de privacidade, mas também em responsabilização administrativa, civil e até criminal, além de danos reputacionais muitas vezes irreversíveis para a instituição. A ausência de um DPO, responsável por orientar, fiscalizar e atuar como canal de comunicação entre a instituição, os titulares e a Autoridade Nacional de Proteção de Dados, e de políticas internas formalizadas que estabeleçam regras, responsabilidades, procedimentos de resposta a incidentes e planos de contingência, agrava ainda mais esses desafios, expondo as instituições a riscos legais, financeiros e reputacionais, dificultando a promoção de uma cultura de proteção de dados e comprometendo a confiança da comunidade acadêmica e da sociedade no compromisso da IES com a ética, a transparência e a responsabilidade no tratamento das informações pessoais (Frazão; Oliva; Tepedino, 2019).

3. METODOLOGIA

A metodologia deste estudo foi cuidadosamente planejada para explorar os impactos da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) na Faculdade de Tecnologia do Vale do Ivaí (Fatec), localizada no Município de Ivaiporã/PR. A escolha do estudo de caso como abordagem metodológica se justifica pela necessidade de uma análise aprofundada e contextualizada, que permita compreender as especificidades e os desafios enfrentados pela instituição na implementação da LGPD. De acordo com Flick (2009), o estudo de caso é uma estratégia metodológica valiosa quando se busca investigar fenômenos complexos em seu ambiente real, permitindo uma análise detalhada das interações e processos envolvidos.

A coleta de dados foi realizada por meio de múltiplas fontes de evidência, garantindo uma visão abrangente e detalhada do objeto de estudo. Entre as técnicas utilizadas, destacam-se as entrevistas estruturadas e semiestruturadas, realizadas com trabalhadores de diferentes setores da Fatec, incluindo Recursos Humanos (RH), Tecnologia da Informação (TI) e Secretaria Acadêmica. As entrevistas buscaram compreender as percepções e práticas desses setores em relação à LGPD, bem como identificar os principais desafios e estratégias adotadas para a implementação da legislação. Além disso, foi realizada uma análise documental, que incluiu a revisão de políticas internas, contratos, termos de consentimento e outros documentos institucionais relevantes para avaliar a conformidade com a legislação. A observação direta também foi utilizada, com visitas aos setores da instituição para identificar práticas cotidianas relacionadas ao tratamento de dados pessoais.

Os dados coletados foram analisados qualitativamente, utilizando-se a técnica de análise de conteúdo, conforme proposto por Bardin (2016). Essa abordagem permitiu identificar padrões, categorias e temas recorrentes relacionados à implementação da LGPD na Fatec. Para assegurar a validade e a confiabilidade dos resultados, foi empregada a triangulação de dados, cruzando informações provenientes das diferentes fontes de evidência, como recomendado por Flick (2009).

Durante o desenvolvimento da pesquisa, algumas limitações foram identificadas. A primeira delas foi a resistência cultural de alguns trabalhadores, que apresentaram baixa familiaridade com os conceitos da LGPD, dificultando a obtenção de respostas detalhadas em certas entrevistas. Além disso, a estrutura enxuta da Fatec, com poucos funcionários por setor, restringiu a disponibilidade de participantes para entrevistas e observações. Outra limitação foi a ausência de registros históricos sobre práticas de proteção de dados, o que dificultou a análise longitudinal das mudanças implementadas. Essas limitações, no entanto, não comprometeram os resultados obtidos, mas destacam a necessidade de maior sensibilização e capacitação sobre o tema no ambiente institucional.

A pesquisa foi conduzida em conformidade com os princípios éticos estabelecidos na Resolução nº 510/2016 do Conselho Nacional de Saúde. Todos os participantes foram informados sobre os objetivos do estudo e assinaram um Termo de Consentimento Livre e Esclarecido antes de participarem das entrevistas e dos questionários. Além disso, garantiu-se o anonimato e a confidencialidade das informações coletadas, respeitando os direitos e a privacidade dos envolvidos.

4. RESULTADOS E DISCUSSÃO

A análise dos resultados obtidos na implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) na Faculdade de Tecnologia do Vale do Ivaí (Fatec), localizada em Ivaiporã/PR, revelou um cenário complexo e multifacetado, marcado por uma série de desafios estruturais, operacionais e culturais que dificultam o alcance da conformidade integral com as exigências da legislação vigente. A pesquisa evidenciou avanços pontuais, como a conscientização inicial sobre a importância da proteção de dados e a identificação de áreas críticas que demandam atenção prioritária, mas também destacou lacunas significativas que comprometem a conformidade plena com a legislação, especialmente no que diz respeito à institucionalização de práticas, políticas e rotinas voltadas à governança de dados pessoais em todos os setores da instituição.

O setor de Recursos Humanos (RH) desempenha um papel central na gestão de dados pessoais sensíveis dos trabalhadores, incluindo informações como nome, endereço, dados bancários, histórico profissional, registros de frequência, avaliações de desempenho, documentação relativa a processos seletivos, contratos de trabalho, informações previdenciárias, e, em alguns casos, dados relacionados à saúde, como atestados médicos, laudos, exames laboratoriais, informações sobre afastamentos, licenças e eventuais restrições laborais. A natureza sensível e estratégica desses dados exige não apenas o cumprimento rigoroso dos princípios e diretrizes da LGPD, mas também a adoção de medidas técnicas e administrativas que assegurem a confidencialidade, integridade e disponibilidade das informações, prevenindo riscos de acessos não autorizados, vazamentos, perdas ou uso indevido. Contudo, os resultados da pesquisa indicaram que esse setor enfrenta desafios significativos para garantir a conformidade com a LGPD, especialmente em virtude de limitações estruturais e da sobrecarga de trabalho enfrentada pelos profissionais responsáveis.

Um dos principais entraves é a estrutura enxuta do setor, que conta com apenas um responsável para gerenciar todas as demandas relacionadas à proteção de dados, além das

atividades cotidianas do RH, como atendimento a funcionários, processamento de folhas de pagamento, gestão de benefícios, administração de contratos, controle de ponto, organização de processos seletivos, elaboração de relatórios, atendimento a auditorias e acompanhamento de questões trabalhistas, previdenciárias e sindicais. Esse acúmulo de funções dificulta a dedicação exclusiva ou prioritária às atividades de adequação à LGPD, tornando o processo de implementação fragmentado, reativo e, muitas vezes, insuficiente para cobrir todas as exigências legais.

A pesquisa revelou que o RH ainda não implementou medidas formais robustas para garantir a conformidade com a LGPD. Por exemplo, não foram realizadas revisões de contratos para incluir cláusulas específicas sobre proteção de dados, assegurando que fornecedores, parceiros e terceiros também estejam comprometidos com as obrigações legais e com a adoção de boas práticas de segurança da informação. Tampouco foi identificada a existência de políticas internas formalizadas de segurança e privacidade, capazes de orientar, padronizar e disciplinar o tratamento de dados pessoais em todas as etapas do ciclo de vida das informações, desde a coleta até o arquivamento ou descarte. Essa ausência de políticas claras e específicas compromete a capacidade do setor de lidar com as exigências legais e aumenta os riscos de tratamento inadequado de dados pessoais, facilitando a ocorrência de incidentes de segurança, vazamentos, uso indevido e até mesmo a responsabilização civil, administrativa ou criminal da instituição em caso de descumprimento da legislação. Segundo Borelli (2020), a ausência de políticas estruturadas sobre proteção de dados pode expor as instituições a sanções legais, multas, bloqueio de bases de dados, suspensão de atividades e comprometer a confiança dos trabalhadores na gestão institucional, afetando o clima organizacional e a reputação da faculdade perante a sociedade.

Outro desafio identificado foi a falta de treinamentos específicos sobre a LGPD para os trabalhadores do setor. Sem capacitações regulares, os responsáveis pelo RH enfrentam insegurança jurídica, dúvidas operacionais e dificuldades para compreender e aplicar as melhores práticas relacionadas ao tratamento de dados, como o correto preenchimento de bases cadastrais, a utilização de sistemas informatizados de maneira segura, a observância dos princípios da minimização e da finalidade, a identificação e o reporte de incidentes de segurança, o atendimento a solicitações dos titulares e a adoção de medidas preventivas e corretivas. Essa lacuna de conhecimento reflete diretamente na ausência de medidas preventivas e corretivas que poderiam fortalecer a governança de dados no setor, impedindo a criação de uma rotina institucionalizada de proteção de dados e dificultando a disseminação de uma cultura organizacional baseada na ética, transparência e responsabilidade no tratamento das

informações pessoais. Como aponta Doneda (2014), a formação contínua é essencial para criar uma cultura organizacional de proteção de dados, especialmente em setores que lidam diretamente com informações sensíveis e que se tornam alvos frequentes de tentativas de acesso indevido, fraudes, ataques cibernéticos e outras ameaças à privacidade.

A coleta e o armazenamento de informações dos trabalhadores também apresentam fragilidades, tanto no que se refere à organização e guarda de documentos físicos, como fichas cadastrais, prontuários, cópias de documentos pessoais e laudos médicos, quanto à gestão de arquivos digitais, planilhas, bancos de dados e sistemas informatizados. Os dados físicos e digitais não estão adequadamente protegidos, seja pela inexistência de armários trancados, salas restritas, controles de acesso físico, seja pela ausência de senhas robustas, criptografia, backups regulares, logs de acesso e políticas de sigilo implementadas nos ambientes digitais. Essa situação é preocupante, considerando que o RH frequentemente gerencia dados biométricos e de saúde dos trabalhadores, os quais são classificados como dados sensíveis pela LGPD (Lei nº 13.709/2018, art. 11), demandando cuidados redobrados para evitar exposições indevidas, discriminação, constrangimentos ou danos à imagem e à dignidade dos titulares. Segundo Garcia et al. (2020), o tratamento de dados sensíveis exige medidas adicionais de segurança, como anonimização, pseudonimização, segmentação de acessos, revisão periódica de permissões e a implementação de mecanismos de rastreamento e auditoria, de modo a evitar acessos não autorizados e garantir a privacidade dos titulares em todas as etapas do tratamento.

A ausência de um encarregado de proteção de dados (*Data Protection Officer – DPO*) também foi apontada como uma lacuna significativa no setor, dificultando a coordenação, monitoramento e avaliação das ações de adequação à LGPD. O DPO é essencial para liderar as ações de conformidade, promover treinamentos, revisar políticas, responder dúvidas, avaliar riscos, monitorar incidentes, implementar planos de resposta e atuar como ponto de contato entre a instituição, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), além de fomentar a cultura de proteção de dados em todos os níveis da organização. Sua ausência compromete a capacidade do RH de monitorar práticas de tratamento de dados, identificar falhas, propor melhorias, implementar medidas corretivas eficazes e demonstrar boa-fé e diligência em eventuais processos de fiscalização, auditoria ou investigação. Segundo Almeida (2020), a nomeação de um DPO é um requisito indispensável para garantir a conformidade com a LGPD, especialmente em setores que lidam com grandes volumes de dados sensíveis, atuando como agente facilitador da governança, da transparência e da responsabilização institucional perante titulares, autoridades e a sociedade em geral.

O setor de Tecnologia da Informação (TI) é um dos pilares fundamentais da implementação da LGPD, sendo responsável por gerenciar, desenvolver, manter e aprimorar sistemas, plataformas, redes e ferramentas tecnológicas que suportam as operações institucionais e, consequentemente, o tratamento de dados pessoais em todos os níveis e setores da organização. A atuação do setor de TI é estratégica, pois ele não apenas provê a infraestrutura necessária para o armazenamento, processamento e circulação de informações, mas também define, aplica e monitora políticas e mecanismos de segurança que visam proteger os dados pessoais contra ameaças internas e externas, acessos não autorizados, vazamentos, perdas acidentais, ataques cibernéticos, fraudes e demais riscos inerentes ao contexto digital contemporâneo.

Os resultados da pesquisa indicaram que o setor realizou avanços iniciais relevantes, especialmente no que diz respeito à implementação de medidas de segurança tecnológica, como a adoção de protocolos de criptografia de dados em trânsito e em repouso, a realização de backups regulares e automatizados, e a atualização periódica de sistemas operacionais, softwares e ferramentas de proteção contra malwares, vírus e outras ameaças. Essas práticas são fundamentais para proteger os dados contra acessos não autorizados, garantir a integridade e a confidencialidade das informações, além de assegurar a rápida recuperação e restauração dos dados em caso de incidentes de segurança, como falhas técnicas, ataques de *ransomware*, desastres naturais ou erros humanos. Segundo Marques e Cardoso (2021), a criptografia é uma das ferramentas mais eficazes para assegurar a confidencialidade de informações sensíveis, especialmente em ambientes digitais, pois torna os dados ilegíveis para terceiros não autorizados, mesmo em situações de interceptação ou acesso indevido, contribuindo de forma decisiva para o cumprimento dos princípios da segurança e da privacidade previstos na LGPD.

Apesar desses avanços, o setor ainda enfrenta desafios significativos que comprometem a conformidade plena com a LGPD e evidenciam a necessidade de investimentos contínuos em tecnologia, processos e capacitação. Um dos principais problemas identificados é a ausência de controles eficazes de acesso aos sistemas que armazenam e processam dados pessoais, sejam eles dados de estudantes, trabalhadores, fornecedores ou outros titulares. A pesquisa revelou que não há mecanismos robustos para limitar e monitorar o acesso às informações apenas a pessoas devidamente autorizadas, o que aumenta consideravelmente os riscos de vazamentos, acessos indevidos, manipulação não autorizada de dados e eventuais violações à privacidade dos titulares. Em muitos casos, o acesso aos sistemas é concedido de forma ampla, sem segmentação adequada por perfil de usuário, sem autenticação multifatorial, sem logs detalhados de atividades e sem revisões periódicas das permissões concedidas. Segundo Garcia

et al. (2020), o controle de acesso é uma medida indispensável para garantir a segurança e a integridade dos dados pessoais, sendo uma das práticas recomendadas e exigidas pela LGPD, pois permite rastrear, auditar e restringir o uso das informações, prevenindo incidentes e facilitando a identificação de responsáveis em caso de irregularidades.

Além disso, o setor de TI também enfrenta dificuldades relacionadas à falta de mão de obra qualificada e especializada para lidar com as exigências técnicas e legais impostas pela LGPD. A pesquisa apontou que os trabalhadores do setor apresentam dúvidas recorrentes sobre os requisitos legais, os conceitos fundamentais da proteção de dados, as melhores práticas internacionais de segurança da informação, as metodologias de análise de riscos e as ferramentas tecnológicas mais adequadas para assegurar a conformidade. Esse cenário evidencia a necessidade urgente de capacitações regulares, direcionadas e atualizadas, que contemplem tanto os aspectos técnicos quanto os aspectos jurídicos e organizacionais da proteção de dados. Segundo Doneda (2014), a formação técnica dos profissionais de TI é essencial para garantir a implementação eficaz de medidas de segurança e conformidade, pois somente com conhecimento aprofundado e atualizado é possível antecipar riscos, propor soluções inovadoras, responder prontamente a incidentes e adaptar-se às constantes mudanças do cenário tecnológico e regulatório.

Outro ponto crítico identificado foi a ausência de um DPO (*Data Protection Officer*, ou Encarregado de Proteção de Dados) na instituição, figura cuja importância já foi destacada em outros setores, mas que adquire relevância ainda maior no contexto da TI. Como mencionado anteriormente, o DPO desempenha um papel central na governança de dados, sendo responsável por coordenar as ações de conformidade, promover a integração entre os setores, orientar os profissionais, revisar políticas, monitorar práticas de tratamento de dados, avaliar riscos, atuar como canal de comunicação com titulares e com a Autoridade Nacional de Proteção de Dados (ANPD), além de liderar a resposta a incidentes e propor melhorias contínuas nos processos institucionais. Sua ausência no setor de TI compromete a capacidade da instituição de monitorar de forma sistêmica e proativa as práticas de tratamento de dados, identificar vulnerabilidades, corrigir falhas, implementar medidas corretivas eficazes e responder de forma tempestiva e adequada a incidentes de segurança, auditorias ou fiscalizações. Segundo Almeida (2020), o DPO deve atuar como líder estratégico na proteção de dados, garantindo que todas as atividades relacionadas ao tratamento de informações pessoais estejam alinhadas às exigências legais, aos princípios da transparência, finalidade, necessidade, segurança e responsabilização, promovendo uma cultura organizacional voltada à ética, à responsabilidade e à proteção da privacidade.

Por outro lado, a pesquisa revelou que o setor de TI possui um plano de resposta a incidentes de segurança, o que representa um avanço importante e demonstra preocupação com a gestão de crises e a continuidade das operações institucionais. Esse plano inclui medidas detalhadas para identificar rapidamente possíveis violações de dados, conter e mitigar os impactos negativos, restaurar a integridade dos sistemas e das informações, além de estabelecer procedimentos claros para comunicar os incidentes à ANPD e aos titulares dos dados afetados, conforme determina a LGPD. O plano prevê ainda a realização de investigações internas, a documentação dos eventos, a análise das causas e a implementação de ações corretivas e preventivas para evitar a recorrência dos problemas. Segundo Bezerra (2023), a existência de um plano de resposta a incidentes é essencial para minimizar os danos causados por violações de segurança, fortalecer a confiança dos titulares de dados na instituição, demonstrar diligência e boa-fé perante as autoridades reguladoras e preservar a reputação institucional mesmo em situações adversas.

A Secretaria Acadêmica desempenha um papel central e estratégico na gestão dos dados pessoais dos estudantes, acompanhando e registrando cada etapa da trajetória acadêmica, desde o momento da matrícula inicial até a emissão do diploma e o encerramento do vínculo institucional. Ao longo desse processo, são coletados, armazenados e tratados diversos tipos de informações pessoais, incluindo dados de identificação, histórico escolar, registros de frequência, notas, atestados médicos, documentos comprobatórios de situação socioeconômica, dados de contato, informações sobre necessidades especiais, entre outros. A responsabilidade atribuída à Secretaria Acadêmica é, portanto, de suma importância, pois envolve o tratamento de dados sensíveis e confidenciais, cuja proteção é fundamental para garantir a privacidade, a dignidade e os direitos dos estudantes, conforme preconiza a Lei Geral de Proteção de Dados Pessoais (LGPD).

Os resultados da pesquisa indicaram que o setor apresenta boas práticas iniciais relacionadas à proteção de dados, demonstrando preocupação com a segurança das informações e a adoção de procedimentos que visam mitigar riscos de exposição indevida. Uma das práticas positivas identificadas foi o controle rigoroso de acesso a documentos sensíveis, como atestados médicos apresentados pelos estudantes. A pesquisa revelou que apenas os coordenadores de curso e os funcionários da secretaria possuem autorização para acessar esses documentos, o que garante o sigilo necessário e reduz significativamente os riscos de acessos indevidos, vazamentos ou uso não autorizado das informações. O acesso restrito é complementado por medidas administrativas, como o registro de protocolos e o monitoramento dos fluxos de documentos, assegurando rastreabilidade e transparência no tratamento dessas informações.

Além disso, destaca-se a digitalização dos processos relacionados ao recebimento e arquivamento de atestados médicos, que agora são protocolados diretamente no sistema eletrônico da instituição. Essa medida elimina a necessidade de manipulação e armazenamento de documentos físicos para essa finalidade, reduzindo a exposição a riscos como extravio, deterioração, acesso não autorizado e dificuldades de controle. Segundo Garcia et al. (2020), a digitalização de processos é uma prática recomendada para fortalecer a segurança da informação, pois permite a implementação de controles de acesso eletrônicos, facilita auditorias, agiliza a busca e o tratamento dos dados e reduz significativamente os riscos associados ao armazenamento físico de documentos, como perdas, danos ou acessos indevidos por terceiros.

Apesar dessas práticas positivas, a pesquisa revelou que o setor ainda possui pouco conhecimento aprofundado sobre a LGPD e suas implicações práticas e jurídicas. Embora os trabalhadores da Secretaria Acadêmica tenham participado de treinamentos pontuais promovidos pela instituição, esses momentos de formação foram considerados insuficientes para suprir todas as demandas e dúvidas do cotidiano, principalmente diante da complexidade e das constantes atualizações do cenário regulatório. Os profissionais demonstraram interesse genuíno em receber mais orientações, capacitações e materiais de apoio sobre o tema, reconhecendo a necessidade de aprimorar seus conhecimentos para lidar de forma segura, ética e legal com as informações sob sua responsabilidade. Segundo Doneda (2014), a capacitação contínua dos trabalhadores é um dos pilares para a criação de uma cultura organizacional de proteção de dados, pois contribui para o desenvolvimento de competências técnicas, o fortalecimento da responsabilidade individual e coletiva, e a disseminação de boas práticas em todos os níveis da instituição.

Outro desafio relevante identificado pela pesquisa foi a ausência de políticas internas claras, específicas e formalizadas sobre proteção de dados pessoais. Embora o setor demonstre interesse e disposição para avançar na conformidade com a LGPD, a inexistência de normas e diretrizes internas compromete a capacidade de implementar práticas consistentes, coordenadas e alinhadas aos princípios da legislação. Na prática, a falta de políticas institucionais dificulta a padronização dos procedimentos, a definição de responsabilidades, a orientação dos trabalhadores em situações de dúvida ou conflito, e a adoção de medidas preventivas e corretivas em caso de incidentes de segurança ou solicitações dos titulares (Garcia et al., 2020).

5. CONCLUSÃO

A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas Instituições de Ensino Superior (IES) representa um marco para a governança de dados no Brasil, especialmente em um contexto de crescente digitalização e complexidade no tratamento de informações sensíveis. Este estudo de caso, conduzido na Faculdade de Tecnologia do Vale do Ivaí (Fatec), localizada em Ivaiporã/PR, revelou avanços e desafios significativos no processo de adequação à legislação, destacando a importância de esforços coordenados entre diferentes setores institucionais para alcançar a conformidade plena.

Os resultados obtidos evidenciam que, embora a Fatec tenha iniciado medidas pontuais de adequação, como a implementação de práticas de segurança tecnológica no setor de Tecnologia da Informação (TI) e o controle de acesso a documentos sensíveis na Secretaria Acadêmica, ainda há lacunas estruturais e culturais que dificultam a efetivação dos princípios da LGPD. A ausência de políticas internas formalizadas, a falta de capacitação regular dos trabalhadores e a inexistência de um encarregado de proteção de dados (Data Protection Officer – DPO) são fatores que comprometem a capacidade da instituição de lidar com as exigências legais e os riscos associados ao tratamento de dados pessoais.

No setor de Recursos Humanos (RH), que gerencia um grande volume de dados sensíveis, foram identificadas fragilidades relacionadas à implementação de políticas de segurança e à ausência de medidas preventivas para mitigar riscos de acessos não autorizados e vazamentos de informações. O setor de TI, por sua vez, enfrenta desafios relacionados à limitação de mão de obra qualificada e à ausência de controles eficazes de acesso aos sistemas institucionais. Já a Secretaria Acadêmica, apesar de apresentar boas práticas iniciais, como a digitalização de documentos e o controle de acesso a informações sensíveis, ainda carece de uma abordagem mais estruturada para garantir a conformidade plena com a LGPD.

A pesquisa também destacou a necessidade de uma abordagem integrada e interdisciplinar para a implementação da LGPD nas IES. A criação de políticas internas claras, o investimento em capacitações regulares e a designação de um DPO são passos fundamentais para fortalecer a governança de dados e promover uma cultura organizacional voltada para a proteção da privacidade e a segurança da informação. Além disso, a integração entre os diferentes setores da instituição é essencial para coordenar ações de conformidade e garantir que todos os processos acadêmicos e administrativos estejam alinhados às exigências legais.

Do ponto de vista social, a adequação à LGPD nas IES é essencial para proteger os direitos fundamentais de estudantes, professores e trabalhadores, promovendo um ambiente de confiança e transparência. Sob a perspectiva científica, este estudo contribui para o avanço do conhecimento sobre os desafios e as estratégias de implementação da LGPD no setor

educacional, oferecendo insights valiosos para outras instituições que enfrentam dificuldades semelhantes. Além disso, a análise realizada reforça a importância da LGPD como um marco regulatório que promove a proteção de dados pessoais como um direito fundamental, alinhando o Brasil às melhores práticas internacionais.

REFERÊNCIAS

ALMEIDA, André Filipe Ferreira de. **Privacidade e proteção de dados pessoais: desenho de processos de negócio seguros e privados nas organizações.** 2020. Dissertação (Mestrado em Engenharia de Telecomunicações e Informática) – Instituto Universitário de Lisboa. Lisboa, 2020. Disponível em: < https://search.proquest.com/openview/bda11c4595b8d07c4367e058953d6f9b/1?pq-origsite=gscholar&cbl=2026366&diss=y>. Acesso em: 23 set. 2025.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. **Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital**. Perspectivas em Ciência da Informação, v. 27, p. 26-45, 2022. Disponível em: < https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/>. Acesso em: 23 set. 2025.

ALMEIDA, V. A. F. **Privacidade e proteção de dados pessoais: fundamentos regulatórios e desafios tecnológicos.** Rio de Janeiro: Elsevier, 2020.

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

BEZERRA, Eric dos Santos**. Desafios na proteção de dados e segurança da informação em ambientes acadêmicos: um estudo de caso na Ufersa Campus Pau dos Ferros**. 2023. Dissertação (Mestrado) – Universidade Federal Rural do Semi-Árido. Pau dos Ferros, 2023. Disponível em: < https://repositorio.ufersa.edu.br/bitstreams/dbfb1a36-f9d4-45de-9cb8-165d4ec245e7/download>. Acesso em: 23 set. 2025.

BORELLI, Alessandra. O tratamento de dados de crianças e adolescentes no âmbito da Lei Geral de Proteção de Dados brasileira. **Cadernos Jurídicos,** São Paulo, ano 21, n. 53, p. 179-190, jan. 2020. Disponível em: < https://www.legiscompliance.com.br/images/pdf/bibliografia_lgpd_2020.pdf>. Acesso em: 23 set. 2025.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23 set. 2025.

CRESPO, M. A implementação da LGPD no setor educacional: desafios e oportunidades. **Revista Brasileira de Direito Educacional**, v. 10, n. 2, p. 34-56, 2021. Disponível em: <>. Acesso em: 23 set. 2025.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91-108, 2014. Disponível em: < https://dialnet.unirioja.es/servlet/articulo?codigo=4555153>. Acesso em: 23 set. 2025.

DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados (Lei nº 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, v. 120, p. 555-587, 2018. Disponível em: < https://www.academia.edu/download/62959269/2018_Comentario_-_Laura_Mendes_-_RDC_120_220200414-30823-utejkp.pdf>. Acesso em: 23 set. 2025.

FLICK, Uwe. **Introdução à pesquisa qualitativa.** 3. ed. Porto Alegre: Artmed, 2009.

FRAZÃO, A.; OLIVA, M.; TEPEDINO, G. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018**. São Paulo: Editora Revista dos Tribunais, 2019.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD): guia de implantação.** São Paulo: Blucher, 2020.

MARQUES, Gleice Ferreira; CARDOSO, Rafael. A importância da segurança em banco de dados. **Revista Eletrônica da Faculdade Invest de Ciências e Tecnologia**, v. 5, n. 1, p. 13-13, 2021. Disponível em: < http://revista.institutoinvest.edu.br/index.php/revistainvest/article/download/43/37>. Acesso em: 23 set. 2025.

STELZER, J. et al. Segurança da informação e privacidade em instituições de ensino superior: desafios e perspectivas na aplicação da LGPD. **Revista de Educação e Tecnologia**, v. 7, n. 1, p. 89-102, 2019. Disponível em: < https://periodicorease.pro.br/rease/article/view/19122>. Acesso em: 23 set. 2025.