***Campus* Porto Velho Zona Norte**
Coordenação do Curso Superior de Tecnologia em
Redes de Computadores

FERNANDO GUILHERME SOARES LESSA
HALBERT XAVIER DA SILVA
YASMIN LEAL DE OLIVEIRA

LGPD E TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS: CONTROLE DE ACESSO EM AMBIENTES PÚBLICOS ESCOLARES

PORTO VELHO
2026

FERNANDO GUILHERME SOARES LESSA

HALBERT XAVIER DA SILVA

YASMIN LEAL DE OLIVEIRA

LGPD E TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS: CONTROLE DE ACESSO EM AMBIENTES PÚBLICOS ESCOLARES

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *Campus Porto Velho Zona Norte*, como requisito para obtenção do título de Tecnólogo em Redes de Computadores, sob orientação do Prof. Esp. Tiago Lopes de Aguiar.

PORTO VELHO

2026

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO.

Lessa, Fernando Guilherme Soares.
LGPD e tratamento de dados pessoais sensíveis: controle de acesso em ambientes públicos escolares / Fernando Guilherme Soares Lessa, Halbert Xavier da Silva, Yasmin Leal de Oliveira. - Porto Velho, 2026.
22 f.

Orientador(a): Prof. Esp. Tiago Lopes de Aguiar.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Redes de Computadores) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho, 2026.

1. segurança da informação . 2. educação pública. 3. biometria. 4. LGPD. I. Silva, Halbert Xavier da. II. Aguiar, Tiago Lopes de (orient.). III. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. IV. Título.

Bibliotecário(a) Responsável: Gizele de Melo Viana, CRB-11/914

FERNANDO GUILHERME SOARES LESSA
HALBERT XAVIER DA SILVA
YASMIN LEAL DE OLIVEIRA

LGPD E TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS: CONTROLE DE ACESSO EM AMBIENTES PÚBLICOS ESCOLARES

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *Campus Porto Velho Zona Norte*, como requisito para obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em: 23/06/2026 pela banca examinadora.

gov.br Documento assinado digitalmente
TIAGO LOPES DE AGUIAR
Data: 07/07/2026 20:35:12-0300
Verifique em https://validar.iti.gov.br

_____
Tiago Lopes de Aguiar
(Orientador)

gov.br Documento assinado digitalmente
JHORDANO MALACARNE BRAVIM
Data: 08/07/2026 07:36:10-0300
Verifique em https://validar.iti.gov.br

_____
Jhordano Malacarne Bravim
(Examinador Interno)

gov.br Documento assinado digitalmente
SILMAR ANTONIO BUCHNER DE OLIVEIRA
Data: 07/07/2026 20:45:53-0300
Verifique em https://validar.iti.gov.br

_____
Silmar Antonio Buchner de Oliveira
(Examinador Interno)

LGPD E TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS: CONTROLE DE ACESSO EM AMBIENTES PÚBLICOS ESCOLARES

RESUMO: A implantação de sistemas automatizados de controle de acesso físico, como as catracas eletrônicas com reconhecimento facial, impõe à administração pública educacional o desafio de conciliar a eficiência e a segurança patrimonial com a proteção jurídica de dados pessoais sensíveis. O presente artigo analisou a conformidade regulatória do tratamento de dados biométricos no ambiente escolar público, tendo como objeto de estudo empírico o Instituto Federal de Rondônia (IFRO), Câmpus Porto Velho Zona Norte. A pesquisa baseou-se em uma revisão de literatura qualitativa e exploratório-descritiva de artigos científicos publicados entre 2021 e 2026, juntamente com análise documental de respostas oficiais obtidas via plataforma Fala.BR. Os resultados identificaram um cenário de conformidade assimétrico, onde existem práticas regulares, e por outro lado constatou-se a necessidade de adequação às boas práticas de segurança da informação e proteção de dados pessoais. Concluiu-se com recomendações relacionadas à reestruturação técnica e administrativa por meio da migração dos ativos para *datacenter*, elaboração de mapeamento preventivos de risco, formalização de termos de consentimento específico e fomento de programas contínuos de capacitação para servidores. Essas medidas são fundamentais para mitigar riscos de incidentes cibernéticos com dados de indivíduos vulneráveis e resguardar a responsabilidade civil objetiva do Estado através do fortalecimento das garantias de privacidade no ambiente de ensino.

PALAVRAS-CHAVE: segurança da informação; educação pública; biometria; LGPD.

ABSTRACT: The implementation of automated physical access control systems, such as electronic turnstiles with facial recognition technology, poses a challenge to educational public administration in balancing efficiency and asset security with the legal protection of sensitive personal data. This article analyzed the regulatory compliance of biometric data processing in the public school environment, using the Federal Institute of Rondônia (IFRO), Porto Velho Zona Norte Campus, as its empirical case study. The research was based on a qualitative and exploratory-descriptive literature review of scientific articles published between 2021 and 2026, combined with documentary analysis of official responses obtained through the Fala.BR platform. The results revealed a scenario of asymmetric compliance, in which some practices were found to be compliant, while, on the other hand, there was evidence of the need to align with information security and personal data protection best practices. The study concluded with recommendations related to technical and administrative restructuring through the migration of assets to a data center, the development of preventive risk assessments, the formalization of specific consent forms, and the promotion of continuous training programs for public servants. These measures are essential to mitigate the risks of cyber incidents involving the data of vulnerable individuals and to safeguard the State's strict civil liability by strengthening privacy guarantees within the educational environment.

KEYWORDS: information security; public education; biometrics; LGPD.

1 INTRODUÇÃO

A promulgação da Lei Geral de Proteção de Dados (LGPD) estabeleceu um novo paradigma para o tratamento de informações no cenário brasileiro, exigindo profundas adequações na administração pública. Como apontam Rodrigues e Paula (2022), a prestação de serviços públicos deve alinhar-se aos princípios da transparência e da finalidade previstos na lei, transformando a governança. No ecossistema educacional, essa exigência manifesta-se de forma complexa. Conforme explicam Candiani e Pereira (2024), as instituições de ensino enfrentam severos desafios formativos para a gestão da LGPD, pois lidam diariamente com dados de indivíduos vulneráveis.

Nesse cenário, o tratamento de dados pessoais sensíveis dentro dos ambientes escolares evoca discussões críticas sobre vigilância e privacidade. De acordo com Falangola *et al*. (2025), a introdução de ferramentas de vigilância digital nas escolas gera desafios jurídicos complexos que tocam diretamente nos direitos de liberdade dos menores. A coleta de dados biométricos para controle de acesso em escolas públicas pode impactar o direito à educação. Conforme destacam Amorim e Müller (2025), o direito social à educação deve ser interpretado em harmonia com o direito fundamental à proteção de dados pessoais.

A problemática agrava-se ao constatar-se que a infraestrutura das escolas públicas muitas vezes carece de suporte técnico especializado para a governança de dados. Segundo Silva *et al.* (2025), a falta de maturidade em segurança da informação no ambiente escolar eleva a probabilidade de incidentes. O tratamento de dados na educação exige um olhar restritivo por envolver indivíduos em desenvolvimento. Como analisam Laranjeira *et al*. (2025), a ocorrência de vazamento de dados em ambientes escolares acarreta severas consequências jurídicas e atrai a responsabilidade civil das instituições de ensino.

O Instituto Federal de Rondônia (IFRO) foi criado em dezembro de 2008, integrando o plano nacional de expansão da Rede Federal de Educação Profissional, Científica e Tecnológica. A instituição nasceu com o objetivo de democratizar o acesso ao ensino técnico e superior na Amazônia Ocidental, impulsionando a transformação social. Com o tempo, o Campus Porto Velho Zona Norte consolidou-se como referência regional na oferta de cursos voltados ao eixo de Informação e Comunicação, preparando profissionais qualificados para responder às demandas tecnológicas contemporâneas e impulsionar o desenvolvimento digital do estado.

Diante desse processo de consolidação e alinhamento às demandas tecnológicas contemporâneas, a infraestrutura física do Campus Porto Velho passou por uma importante modernização em sua segurança e controle de fluxo. No ano de 2026, a instituição realizou a implantação de catracas eletrônicas com sistemas de acesso biométrico, destinadas ao controle de entrada e saída tanto do corpo discente quanto dos servidores. Essa transição automatizada converteu as portarias do *campus* no cenário factual ideal para este estudo uma vez que a coleta e o tratamento cotidiano de dados biométricos, classificados como sensíveis pela legislação vigente, passaram a exigir uma estrutura robusta de governança e conformidade regulatória dentro da unidade de ensino.

Diante desse cenário de transição tecnológica e jurídica nas instituições de ensino, emerge a seguinte questão norteadora: como o controle de acesso e o tratamento de dados pessoais sensíveis em ambientes escolares públicos podem ser executados em conformidade com as exigências da Lei Geral de Proteção de Dados (LGPD), garantindo os direitos fundamentais à privacidade e à proteção de dados dos discentes?

O objetivo deste trabalho consistiu em analisar a conformidade do tratamento de dados biométricos utilizados para controle de acesso em ambientes escolares públicos, verificando se atendem às exigências da Lei Geral de Proteção de Dados (LGPD) sem comprometer o direito à proteção de dados dos estudantes. E dentre os objetivos específicos, buscaram-se: (a) compreender os aspectos que envolvem os desafios da governança de dados e da cidadania digital nas instituições de ensino; (b) analisar o tratamento de dados de crianças e adolescentes e os limites da vigilância aplicados ao Campus Porto Velho Zona Norte, do IFRO; e (c) propor melhores práticas envolvendo responsabilidade civil, riscos tecnológicos e incidentes de segurança aplicados ao Campus.

A relevância desta pesquisa fundamenta-se na necessidade premente de lançar luz sobre os desafios práticos de conformidade com a LGPD enfrentados pela gestão pública escolar, setor tradicionalmente negligenciado nos debates de segurança da informação avançada. Justifica-se o estudo pelo potencial de orientar gestores educacionais e formuladores de políticas públicas na conciliação entre a segurança patrimonial e humana nas escolas e a estrita legalidade no tratamento de

dados sensíveis, mitigando riscos de responsabilização civil por vazamentos de dados de menores.

2 REFERENCIAL TEÓRICO

2.1 Conceitos sobre conformidade e proteção de dados pessoais

O conceito de conformidade, ou *compliance*, na administração pública, traduz-se no alinhamento irrestrito das atividades institucionais aos preceitos legais e regulatórios vigentes no país. No ecossistema educacional, conforme explicam Rodrigues e Paula (2022), a prestação dos serviços públicos deve conciliar permanentemente a eficiência de suas rotinas com a proteção integral dos direitos dos cidadãos. Estar em conformidade significa mitigar riscos jurídicos e operacionais, assegurando que o tratamento de informações nas escolas não resulte em abusos ou desvios de finalidade na gestão pública.

A proteção de dados pessoais foi elevada ao patamar de direito fundamental autônomo na Constituição Federal, demandando uma postura proativa do Estado para garantir a privacidade. No ambiente escolar, esse mandamento ganha contornos ainda mais rígidos por lidar com pessoas em desenvolvimento. Como destacam Amorim e Müller (2025), o direito social à educação deve ser interpretado em harmonia com a proteção de dados, impedindo que a modernização tecnológica anule as garantias individuais discentes e exponha os estudantes a vulnerabilidades digitais nas redes federais.

A Lei Geral de Proteção de Dados (LGPD) regulamenta o tratamento de informações de pessoas naturais, tanto em meios físicos quanto digitais, por entes públicos ou privados. A norma estabelece princípios mandatórios que visam salvaguardar a dignidade humana contra abusos informacionais. No cenário educacional, como apontam Candiani e Pereira (2024), as instituições de ensino enfrentam severos desafios formativos para a gestão da lei, exigindo dos gestores uma compreensão nítida sobre as bases legais adequadas para justificar a guarda de registros e prontuários acadêmicos.

Como instituição de ensino federal integrante da Rede Federal, o Instituto Federal de Rondônia (IFRO) está submetido às obrigações destinadas ao Poder Público pela legislação protetiva. O cumprimento da norma é mandatório para validar as políticas de ensino desenvolvidas no Campus Porto Velho Zona Norte. A relevância dessa adequação é nítida, pois, conforme explicam Rodrigues e Paula (2022), o

alinhamento aos princípios da transparência transforma a governança, e seu descumprimento configura falha na prestação do serviço essencial, gerando severas responsabilidades para o erário.

Os dados pessoais sensíveis recebem uma proteção legal diferenciada e restritiva pela LGPD devido ao seu alto potencial discriminatório, abrangendo características biométricas. A coleta e o processamento de traços biológicos para a identificação automatizada de estudantes enquadram-se nessa categoria de alta vulnerabilidade. De acordo com Leite (2024), o aperfeiçoamento do tratamento de dados de menores exige a observância do princípio do melhor interesse, demandando salvaguardas técnicas robustas e consentimento específico dos responsáveis para legitimar o controle de acesso físico.

2.2 Boas práticas aplicáveis ao uso de dados biométricos

A LGPD recomenda que o tratamento de dados pessoais sensíveis ocorra sob condições estritas de segurança, priorizando a prevenção à fraude. No controle de acesso escolar, a legislação exige a aplicação rigorosa dos princípios da necessidade e da minimização informacional. Como sustentam Rodrigues e Paula (2022), a atividade estatal deve pautar-se pela finalidade e transparência, exigindo que a introdução de ferramentas tecnológicas nas portarias venha acompanhada de ampla comunicação para que alunos e familiares compreendam os fluxos de armazenamento.

As diretrizes internacionais de segurança estabelecem boas práticas fundamentais para a gestão da privacidade por meio de controles técnicos específicos. A governança eficaz, segundo Albuquerque et al. (2024), exige a identificação precisa de riscos e desafios operacionais antes da adoção de inovações tecnológicas nas instituições. As boas práticas recomendam a criptografia irreversível das matrizes biométricas, o armazenamento de assinaturas matemáticas codificadas em vez de imagens faciais completas e o estabelecimento de rotinas rígidas de auditoria nos servidores escolares.

Indispensável a esse ecossistema de conformidade, a principal boa prática administrativa e jurídica exigida no tratamento de biometria é a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Regulamentado pela LGPD, de acordo com Candiani e Pereira (2024) o RIPD consiste em um documento formal e preventivo que contém a descrição detalhada dos processos de tratamento

de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. No contexto da automação de portarias escolares, este instrumento desempenha um papel duplo: funciona como um mapeamento de riscos detalhado, que diagnostica o ciclo de vida da biometria desde a coleta até o descarte, e serve como evidência institucional das salvaguardas.

Somada ao relatório de impacto, Segundo Silva et al. (2025) a governança de dados em instituições de ensino requer a instituição de políticas estritas de retenção e descarte de dados. Uma governança robusta impede o armazenamento por tempo indeterminado, fixando que as matrizes matemáticas associadas às biometrias de alunos e servidores sejam eliminadas de forma segura e automatizada imediatamente após o encerramento do vínculo formal com a instituição, cumprindo o princípio da exclusão de dados previstos na legislação.

Ademais destaca-se a aplicação prática dos conceitos de *Privacy by Design* (privacidade desde a concepção) e *Privacy by Default* (privacidade por padrão). De acordo com Falangola et al. (2025) na prática, significa que as catracas eletrônicas e seus respectivos softwares integrados devem ser projetados, adquiridos e configurados para operar sob nível máximo de proteção de dados disponível, desativando funções de compartilhamento automático ou armazenamento colateral sem intervenção do usuário. Essa abordagem preventiva estende-se à capacitação contínua do corpo técnico-administrativo e dos agentes de portaria, garantindo que os profissionais que operam o sistema diariamente compreendam os protocolos de sigilo e saibam como reagir de forma imediata diante de qualquer suspeita de incidente de segurança.

As sanções aplicáveis ao descumprimento da LGPD na administração pública possuem natureza predominantemente administrativa, manifestando-se por meio de advertências ou eliminação compulsória dos bancos de dados. Embora as multas não atinjam diretamente o erário das instituições de ensino, os incidentes geram impactos severos. Como analisam Laranjeira et al. (2025), a ocorrência de vazamento de dados em ambientes escolares acarreta graves consequências jurídicas e atrai a responsabilidade civil objetiva das instituições, exigindo ações preventivas imediatas contra ataques cibernéticos.

A adoção de mecanismos menos invasivos desponta como uma das principais recomendações doutrinárias para mitigar os riscos inerentes ao uso de tecnologias inteligentes de identificação nas escolas. Conforme explica Figueiredo et al. (2026), a

cidadania digital deve integrar as políticas pedagógicas e administrativas das escolas, promovendo um ambiente seguro. O planejamento deve prever canais alternativos de identificação física para os discentes, garantindo que a automação das portarias não crie barreiras ao livre acesso às salas de aula.

A formulação de políticas públicas integradas voltadas para a governança digital exige a elaboração prévia de relatórios de impacto à proteção de dados pessoais pelas instituições de ensino. Esse documento funciona como um mapeamento preventivo de riscos, detalhando as salvaguardas adotadas. Conforme asseveram Reis e Do Carmo Direito (2023), a tensão entre o que revelar e o que preservar nas políticas públicas exige critérios técnicos rigorosos de anonimização, garantindo que o ciclo de vida dos dados estudantis permaneça integralmente protegido.

2.3 Conceitos de segurança da informação e gestão de dados

A gestão de dados consiste no conjunto de práticas e procedimentos voltados para administrar o ciclo de vida completo das informações tratadas por uma organização. No cenário escolar, essa governança envolve desde a captação na matrícula até o descarte seguro. Conforme destaca Moreira (2023), o controle e a transparência na gestão de dados pela administração pública são indispensáveis para validar as políticas educacionais, permitindo a coexistência harmônica entre a publicidade dos atos estatais e o sigilo de dados sensíveis.

A segurança da informação ancora-se na preservação de três pilares interdependentes que protegem os ativos tecnológicos contra ameaças: confidencialidade, integridade e disponibilidade. No entanto, a realidade das escolas públicas impõe barreiras complexas. Segundo Silva et al. (2025), a falta de maturidade em segurança da informação no ambiente escolar eleva a probabilidade de incidentes cibernéticos, pois a infraestrutura tecnológica precária e a ausência de políticas institucionais claras desamparam os gestores no manuseio cotidiano dos servidores de rede.

No âmbito da governança pública, a mitigação dessas vulnerabilidades tecnológicas e algorítmicas exige a implementação de uma gestão de riscos estruturada, cujo principal instrumento operacional é o Relatório de Impacto à Proteção de Dados (RIPD). No cenário educacional, o RIPD deixa de ser apenas uma exigência formal de conformidade para se tornar uma salvaguarda estratégica.

Conforme apontam Falangola *et al*. (2025) a gestão preventiva de riscos, materializada no RIPD, é a ferramenta mais eficaz para assegurar que a introdução de novas tecnologias nas escolas não viole os direitos fundamentais dos alunos, funcionando como um freio técnico-administrativo contra vazamento de dados e abusos de vigilância automatizada.

O tratamento de dados engloba toda operação realizada com informações pessoais, abrangendo procedimentos como a coleta, o processamento, o armazenamento e a eliminação nos sistemas digitais. O ato de capturar a imagem de um estudante configura uma atividade formal submetida à lei. Conforme analisam Laranjeira et al. (2025), o tratamento inadequado de dados na educação exige um olhar restritivo por envolver indivíduos vulneráveis, já que a exposição inadequada de informações estudantis atrai a responsabilidade civil e penal dos gestores públicos.

Os princípios de funcionamento das catracas eletrônicas com reconhecimento facial baseiam-se na captura de imagem por sensores, seguida da conversão dos dados em um código binário comparado ao banco cadastral. Se houver equivalência positiva, o sistema libera o giro do torniquete. Contudo, deficiências estruturais geram riscos físicos e lógicos. De acordo com Silva et al. (2025), a vulnerabilidade das redes de ensino facilita o acesso externo aos softwares de automação predial, permitindo que falhas técnicas convertam catracas em vetores de invasão cibernética.

3 METODOLOGIA

Para a consecução desta pesquisa, adotou-se como procedimento metodológico a revisão de literatura de natureza qualitativa, que se concentra na interpretação profunda de conceitos, teorias e normas jurídicas, sem a pretensão de mensurar dados estatísticos ou numéricos, e caráter exploratório-descritivo, focado em aproximar o pesquisador de uma problemática contemporânea para detalhar suas características, mapear riscos operacionais e propor caminhos práticos de adequação. Realizou-se um levantamento bibliográfico e documental fundamentado em artigos científicos, periódicos jurídicos e na legislação nacional correlata ao tema e documentos oficiais. A busca pelas fontes científicas foi realizada por meio de consultas sistemáticas em bases de dados de relevância acadêmica e jurídica, incluindo o Portal de Periódicos Capes, garantindo uma captação abrangente da produção doutrinária sobre o tema.

A seleção do material bibliográfico seguiu critérios rigorosos de elegibilidade. Como critérios de inclusão, estabeleceram-se artigos em periódicos revisados por pares e textos normativos que abordassem o tratamento de dados no setor educacional público, priorizando trabalhos publicados entre os anos de 2021 e 2026 para assegurar debates contemporâneos. Por outro lado, definiram-se como critérios de exclusão de artigos repetidos entre as bases, resumos de congressos, monografias não publicadas e estudos que tratavam da LGPD exclusivamente no setor corporativo ou empresarial, sem correlação com o ecossistema escolar.

A opção pela utilização do Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) justificou-se pela necessidade de conferir rigor científico e alta credibilidade ao referencial teórico construído. Sendo o principal acervo de difusão científica do país, a plataforma permitiu o acesso centralizado a periódicos auditados e revisados por pares com estratos elevados no sistema. Essa escolha metodológica foi fundamental para mitigar o risco de utilização de literatura cinzenta, garantindo que o debate sobre os impactos jurídicos e tecnológicos da biometria estivesse alinhado com a vanguarda doutrinária nacional.

Para a execução das buscas eletrônicas na plataforma, realizadas no primeiro quadrimestre de 2026, foram estruturados cruzamentos booleanos utilizando termos extraídos dos eixos centrais do estudo, cruzando tecnologia, legislação e ambiente educacional por meio das expressões "LGPD" AND "biometria" AND "escola", "proteção de dados" AND "reconhecimento facial" AND "educação pública", bem como "dados sensíveis" AND "segurança da informação" AND "instituições de ensino".Inicialmente foram selecionados 52 artigos, partir do refinamento pelos critérios de elegibilidade previamente estabelecidos, foram selecionados apenas 13 artigos científicos que serviram de alicerce para as discussões teórico-práticas deste trabalho, cuja distribuição sistemática dessas obras está detalhada no Quadro 1.

Quadro 1 - Artigos selecionados no Portal Periódicos Capes para fundamentação da pesquisa.

Autor(es) e Ano	Título do Artigo	Foco Principal da Obra no Estudo
RODRIGUES; PAULA (2022)	Prestação dos serviços públicos à luz da Lei Geral de Proteção de Dados (LGPD)	Princípios da finalidade e transparência estatal.
MOREIRA (2023)	Controle e transparência na gestão de dados pela administração pública...	Tratamento de dados sensíveis na inclusão escolar.
REIS; DO CARMO DIREITO (2023)	Dados pessoais e políticas públicas: O que revelar e o que preservar?	Critérios de anonimização no setor público.

ALBUQUERQUE et al. (2024)	Segurança de dados na educação online: riscos, desafios e boas práticas	Protocolos de TI e boas práticas em dados educacionais.
CANDIANI; PEREIRA (2024)	Lei Geral de Proteção de Dados (LGPD) nas instituições de ensino...	Desafios formativos de gestores e servidores.
LEITE (2024)	O aperfeiçoamento do tratamento de dados de crianças e adolescentes...	Princípio do melhor interesse do menor de idade.
AMORIM; MÜLLER (2025)	Proteção de dados no ensino jurídico público federal...	Diálogo entre direito à educação e privacidade.
FALANGOLA et al. (2025)	Proteção de dados e vigilância digital em ambientes educacionais...	Riscos de hipervigilância e portarias automatizadas.
LARANJEIRA et al. (2025)	Vazamento de dados em ambiente escolar: consequências...	Responsabilidade civil objetiva por incidentes de dados.
MANZATO et al. (2025)	Direitos da personalidade e a lei nº 15.001/2024...	Conflito entre leis locais de monitoramento e privacidade.
SILVA et al. (2025)	A segurança da informação e a lei geral de proteção de dados em ambiente escolar	Vulnerabilidade física e lógica de redes de ensino.
FIGUEIREDO et al. (2026)	Cidadania digital: caminhos para ambientes educacionais seguros e éticos	Cultura ética no uso de tecnologias nas escolas.
MIRANDA et al. (2026)	Lei geral de proteção de dados (lgpd) e o uso da inteligência artificial (ia) na educação...	Opacidade algorítmica e reconhecimento facial.

Fonte: Elaborado pelos autores (2026)

O cenário geográfico e institucional que balizou as análises empíricas desta pesquisa foi o Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), tomando como referência a realidade estrutural de controle de fluxo de pessoas no Campus Porto Velho Zona Norte. A unidade atua como um laboratório empírico ideal para a pesquisa por convergir uma alta densidade de tráfego diário de estudantes de cursos técnicos e superiores com a necessidade de modernização tecnológica de suas portarias. As rotinas institucionais do IFRO permitiram confrontar as exigências abstratas da LGPD com as limitações reais enfrentadas pela Rede Federal, servindo de modelo descritivo para o estudo da governança de dados biométricos em instituições de ensino. Ademais, visando diagnosticar o panorama factual da instituição, O IFRO foi consultado formalmente por meio da plataforma Fala.BR (Plataforma Integrada de Ouvidoria e Acesso à Informação). O Fala.BR funciona como canal centralizado pelo qual qualquer cidadão pode encaminhar pedidos de acesso à informação a órgãos e entidades do Poder Executivo Federal, em estrita conformidade com as diretrizes e prazos estabelecidos pela Lei de Acesso à Informação (LAI - Lei n°12.527/2011). os dados respostas oficiais obtidos por meio desse mecanismo subsidiaram a análise de conformidade prática do campus.

O material coletado e selecionado foi submetido a uma análise de conteúdo integrativa. Esse processo permitiu categorizar e mapear as principais convergências doutrinárias, as lacunas institucionais na administração pública e os riscos jurídicos e operacionais associados ao uso de tecnologias de monitoramento em ambientes escolares. A interpretação crítica desses dados fundamentou a discussão teórica deste artigo, viabilizando a identificação de parâmetros para a aplicação segura de mecanismos de controle de acesso em conformidade com as diretrizes da legislação protetiva de dados.

4 RESULTADOS E DISCUSSÃO

4.1 Desafios da governança de dados e da cidadania digital nas instituições de ensino

A implementação da LGPD na administração pública exige uma transformação estrutural profunda que esbarra na ausência de uma cultura consolidada de governança de dados nas instituições de ensino. De acordo com Rodrigues e Paula (2022), a prestação dos serviços públicos deve conciliar a eficiência operacional com a proteção integral dos direitos dos cidadãos, estabelecendo padrões rígidos de conformidade. No entanto, a realidade das escolas públicas revela o desconhecimento dos agentes administrativos sobre as bases legais para o tratamento de dados pessoais. O tratamento de dados no setor educacional necessita de diretrizes institucionais claras para evitar que a burocracia governamental resulte em violações sistemáticas das garantias individuais e na perda de controle das informações geridas.

A construção de um ambiente escolar seguro e ético depende do fortalecimento de competências voltadas para o ambiente virtual. Conforme explicam Figueiredo *et al*. (2026), a cidadania digital deve integrar as políticas pedagógicas e administrativas das escolas, promovendo o uso consciente e responsável das tecnologias da informação pelos gestores, professores e alunos. A carência de programas de formação continuada para os profissionais da educação compromete a eficácia de qualquer política de privacidade. O desenvolvimento dessa consciência ética nas instituições públicas funciona como um mecanismo preventivo contra incidentes de segurança, transformando a comunidade escolar em um agente ativo de fiscalização e proteção das informações de natureza sensível.

A conformidade com a legislação protetiva esbarra na escassez de recursos técnicos e humanos qualificados no cenário educacional público. Segundo Candiani e

Pereira (2024), as instituições de ensino enfrentam graves desafios formativos para a aplicação prática e a gestão cotidiana da LGPD, o que resulta em interpretações equivocadas da norma. A falta de treinamento específico dos servidores públicos gera uma aplicação deficiente dos princípios da finalidade e da necessidade no manuseio de prontuários, registros e relatórios pedagógicos. Essa lacuna educativa potencializa a ocorrência de erros operacionais graves, fragilizando a confiança pública nas ferramentas tecnológicas adotadas pelo Estado para gerir o fluxo escolar.

A segurança da informação nas escolas públicas demanda investimentos substanciais em infraestrutura tecnológica e na capacitação de pessoal administrativo. De acordo com Silva et al. (2025), a maturidade digital dos estabelecimentos de ensino básico é historicamente baixa, o que expõe as redes internas de computadores a vulnerabilidades severas de segurança. O armazenamento inadequado de dados cadastrais de alunos e servidores facilita o acesso de terceiros não autorizados aos sistemas internos de controle. A ausência de políticas institucionais claras voltadas para a segurança da informação desampara os gestores escolares, que executam o tratamento de dados rotineiros sem o suporte de ferramentas de criptografia.

A governança pública exige transparência ativa sobre a destinação e a finalidade do armazenamento das informações dos estudantes. Conforme destaca Moreira (2023), o controle e a transparência na gestão de dados pela administração pública são indispensáveis para validar as políticas públicas voltadas para o atendimento educacional especializado. A publicidade dos atos administrativos deve coexistir harmonicamente com a preservação do sigilo de dados médicos e psicossociais dos alunos matriculados em salas de recursos. O equilíbrio entre a necessidade de fiscalização social do orçamento público e o direito à privacidade dos estudantes vulneráveis constitui um dos principais desafios operacionais da gestão educacional contemporânea.

A análise das respostas prestadas pela Direção-Geral do IFRO Câmpus Porto Velho Zona Norte por meio da plataforma Fala.BR permitiu mapear detalhadamente a arquitetura técnica e jurídica que sustenta o controle de acesso biométrico da instituição, revelando um cenário de conformidade assimétrica.

Quadro 2 - Análise das respostas prestadas pela Direção-Geral do IFRO Câmpus Porto Velho Zona Norte.

Dimensão de Análise	Prática Declarada pelo Campus (Fala.BR)	Status de conformidade à LGPD
Finalidade e Justificativa	Controle de entrada/saída de alunos e servidores para segurança patrimonial e física.	**Conforme** (Finalidade legítima, carece de teste e proporcionalidade).
Base Legal Adotada	Cláusula aceita no ato da matrícula institucional.	**Conforme** (Consentimento/ciência no ato da matrícula).
Armazenamento e Compartilhamento	Banco de dados local do campus na portaria.	**Inconforme** (Necessário uso de um *datacenter* apropriado e longe do acesso fácil de terceiros).
Retenção e Descarte	Exclusão automática dos dados biométricos após o término do vínculo.	**Conforme** (Atende ao dispositivo relacionado à término do tratamento de dados previsto no art. 16 da LGPD).
Governança (RIPD)	Inexistência de relatório de Impacto à Proteção de Dados Pessoais produzido para o sistema.	**Inconforme** (Obrigatório para dados sensíveis sob risco elevado - art. 32).
Controle de acesso e Retificação	Exclusão de dados biométricos e situações analisadas pela administração do campus.	**Conforme** (Oferece alternativas, segue o critério de exclusão automática e o princípio da minimização)

Fonte: Elaborado pelos autores (2026)

A síntese no Quadro 2 revela que a conformidade do IFRO Câmpus Porto Velho Zona Norte com a LGPD encontra-se fraturada em duas realidades. Se de um lado o campus demonstra êxito operacional, como na parte de retenção e descarte onde o mecanismo automatizado de exclusão pós-vínculo cumpre rigorosamente a legislação e na cláusula de aceite em conformidade, por outro lado as dimensões de governança jurídica e segurança física da informação revelam vulnerabilidade preocupantes, onde conforme Amorim e Müller (2025), a desconformidade verificada pela ANPD (Agência Nacional de Proteção de Dados) pode implicar em sanções administrativas previstas no art. 52.

A primeira grande falha operacional identificada no quadro nos mostra uma falha de segurança física de alta criticalidade na dimensão Armazenamento e Compartilhamento. A guarda do banco de dados biométricos em um servidor

localizado fisicamente na própria portaria do campus, criando uma grave exposição a riscos de incidentes. Conforme explica Candiani e Pereira (2024) um servidor que trata de dados biométricos deve ser dotado de controle restrito de terceiros, criptografia e proteção contra sabotagens, a falta de isolamento em um *datacenter* institucional apropriado facilita o acesso físico não autorizado de terceiros e aumenta a superfície de vulnerabilidade para exfiltração ou destruição desses ativos sensíveis.

Dentre uma das inconformidades a mais gritante se encontra na Governança. A inexistência do Relatório de Impacto à Proteção de Dados (RIPD) materializa a ausência de gestão de riscos prévia e perene. Conforme Falangola *et al*. (2025) a LGPD prevê a obrigatoriedade de elaboração do RIPD no art. 38 sempre que o tratamento de dados puder acarretar riscos relevantes aos direitos e liberdades dos titulares. Sem esse instrumento essencial, a instituição permanece operando às cegas no que tange às salvaguardas jurídicas, transformando o controle de acesso de uma legítima ferramenta de segurança em um vetor de passivos jurídicos e possíveis sanções.

4.2 O tratamento de dados de crianças e adolescentes e os limites da vigilância

A proteção de dados de crianças e adolescentes recebe um tratamento jurídico diferenciado e restritivo devido à condição peculiar de desenvolvimento desse público. Conforme adverte Leite (2024), o aperfeiçoamento do tratamento de dados de menores, nos âmbitos público e privado, exige a observância do princípio do melhor interesse, demandando consentimento específico dos responsáveis. As escolas públicas manipulam diariamente informações de menores sem os devidos termos de consentimento ou justificativas legais válidas. A inobservância desse rigor normativo transforma a coleta rotineira de dados cadastrais e biométricos em uma atividade irregular, sujeitando a administração pública a sanções severas dos órgãos de controle e fiscalização.

De acordo com Leite (2024), a instituição deve dispor de um termo de consentimento que para menores entre 12 e 16 assinado pelos responsáveis legais e para os titulares entre 16 e 18 anos ficam à disposição dos artigos 7° e 11 da LGPD. Nesse contexto, a justificativa da Direção-Geral do IFRO Câmpus Porto Velho Zona Norte menciona a existência da autorização do uso de imagem para fins de identificação e controle no termo de consentimento assinado pelos responsáveis legais durante o ato da matrícula de menores de idade.

A proliferação de tecnologias de monitoramento digital nas dependências escolares redefine as dinâmicas de poder e privacidade na comunidade educativa. De acordo com Falangola et al. (2025), a proteção de dados e a vigilância digital em ambientes educacionais geram desafios jurídicos complexos frente à LGPD, especialmente pelo risco de hipervigilância. A instalação de sistemas automatizados de controle de acesso modifica o comportamento psicossocial dos estudantes sob a justificativa de otimizar a segurança patrimonial escolar. A transformação da escola em um espaço de monitoramento contínuo exige uma justificativa técnica robusta e proporcional, impedindo que o controle físico fira a liberdade individual dos discentes.

A implementação de portarias eletrônicas e biometria facial deve sujeitar-se ao princípio da proporcionalidade regulado pela legislação nacional. De acordo com Albuquerque et al. (2024), a segurança de dados na educação digital exige a identificação precisa de riscos, desafios e boas práticas operacionais antes da adoção de inovações tecnológicas. A coleta de dados sensíveis de menores para o controle de entrada e saída escolares expõe o público infantojuvenil a riscos cibernéticos desproporcionais aos benefícios gerados pela automatização. O planejamento administrativo deve priorizar mecanismos menos invasivos de identificação, reservando o tratamento biométrico para situações excepcionais devidamente justificadas por relatórios de impacto.

A governança do fluxo escolar deve estruturar barreiras físicas e digitais capazes de salvaguardar as informações sensíveis coletadas nas portarias. Conforme pontuam Candiani e Pereira (2024), a gestão de dados escolares demanda uma reestruturação dos espaços físicos e dos servidores da rede para evitar o livre acesso de estranhos. O monitoramento de acesso não se restringe à instalação de catracas eletrônicas, mas envolve o controle estrito sobre quem manipula o banco de dados gerado por esses equipamentos tecnológicos. A ausência de segregação de funções na administração escolar permite que funcionários desqualificados acessem e compartilhem dados de estudantes de forma irregular.

4.3 Responsabilidade civil, riscos tecnológicos e incidentes de segurança na escola

O armazenamento de dados pessoais em sistemas escolares desprovidos de ferramentas avançadas de segurança cibernética potencializa a ocorrência de sinistros graves. A complexidade do cenário educacional exige que os desafios

jurídicos, tecnológicos e institucionais sejam organizados de forma clara, permitindo que gestores e formuladores de políticas públicas compreendam a relação direta entre falhas de governança, riscos operacionais e responsabilidades civis. Nesse sentido, o Quadro 3 foi elaborado para sintetizar os aspectos centrais discutidos nesta seção.

Quadro 3 - Desafios, riscos e boas práticas na implementação da LGPD em ambientes escolares públicos.

Aspecto	Desafios Identificados	Riscos	Boas Práticas / Soluções
Governança de dados	Falta de cultura institucional e formação continuada	Erros operacionais e violações de privacidade	Programas de capacitação e diretrizes claras
Vigilância digital	Uso de biometria e câmeras sem critérios proporcionais	Hipervigilância e violação de direitos da personalidade	Relatórios de impacto e uso restrito de biometria
Segurança da informação	Infraestrutura tecnológica precária	Vazamento de dados e invasões cibernéticas	Criptografia, auditorias e protocolos de resposta
Responsabilidade civil	Descumprimento da LGPD pela administração pública	Indenizações e perda de confiança social	Adoção de políticas de proteção e fiscalização ativa

Fonte: Elaborado pelos autores (2026)

Segundo Laranjeira et al. (2025), o vazamento de dados em ambiente escolar acarreta consequências jurídicas profundas e atrai a responsabilidade civil objetiva da instituição de ensino pelos danos provocados. O Estado responde pelos prejuízos decorrentes da exposição inadequada de dados íntimos de alunos de escolas públicas. A vulnerabilidade dos bancos de dados educacionais atrai a ação de criminosos virtuais, resultando no sequestro de informações e na exposição pública de vulnerabilidades socioeconômicas e médicas de estudantes menores de idade.

A mitigação dos riscos de segurança da informação exige a adoção de boas práticas institucionais focadas na resiliência cibernética dos sistemas internos. De acordo com Albuquerque et al. (2024), as boas práticas na educação envolvem a implementação de rotinas de auditoria, criptografia e controle de acesso lógico aos servidores de dados. A negligência na atualização de sistemas operacionais das secretarias escolares facilita a exploração de falhas técnicas por agentes maliciosos. O estabelecimento de protocolos claros para a notificação de incidentes à Agência Nacional de Proteção de Dados (ANPD) constitui uma obrigação legal que as escolas públicas descumprem sistematicamente por desconhecimento técnico e burocrático.

A responsabilidade civil do Estado em face de vazamentos educacionais fundamenta-se no dever de guarda e na proteção integral da infância. Conforme

asseveram Rodrigues e Paula (2022), o descumprimento das obrigações da LGPD pela administração pública configura falha na prestação do serviço público essencial, gerando o dever de indenizar os indivíduos afetados. O impacto psicossocial do vazamento de dados escolares de crianças é irreversível, afetando a segurança pessoal e a reputação familiar dos discentes. Os gestores públicos devem agir proativamente na blindagem dos sistemas de informática das escolas para evitar litígios judiciais em massa contra o erário.

A fragilidade na segurança das portarias eletrônicas escolares expõe a comunidade a riscos que ultrapassam o ambiente estritamente digital. Segundo Silva et al. (2025), a ausência de mecanismos eficientes de controle de acesso lógico nos softwares de automação predial permite a manipulação externa de portões eletrônicos e câmeras. A interconexão de sistemas de segurança física com a internet sem a devida proteção por firewalls transforma as catracas escolares em vetores de invasão cibernética. O sequestro digital desses sistemas impede o funcionamento regular das escolas, paralisando as atividades letivas e comprometendo a integridade física de alunos e professores.

O tratamento inadequado de dados na gestão pública educacional compromete a eficácia das políticas de inclusão desenvolvidas pelo Estado. Conforme argumenta Moreira (2023), o vazamento de listas de atendimento educacional especializado expõe o histórico clínico e de saúde mental de alunos com deficiência a discriminações externas variadas. A guarda desses dados sensíveis exige níveis elevados de segurança física e lógica, impedindo a circulação de cópias impressas ou digitais fora do ambiente estritamente pedagógico. A publicidade inadequada dessas informações viola a dignidade humana do estudante, gerando exclusão social e sofrimento psicológico no ambiente escolar.

Diante do cenário das desconformidades expostas no Quadro 2 e considerando melhorar a governança de dados e eficiência na segurança física de dados, desenvolve-se uma proposta de intervenção institucional. Essa intervenção busca mitigar os riscos operacionais, técnicos e jurídicos evidenciados nas seções anteriores. A proposta ataca as inconformidades críticas identificadas nas averiguações empíricas do IFRO Câmpus Porto Velho Zona Norte (Quadro 2) e também adiciona recomendações de melhoria na governança de dados, transformando o diagnóstico de vulnerabilidades em diretrizes de adequação.

Quadro 4 - Plano de intervenção das inconformidades do IFRO Câmpus Porto Velho Zona Norte.

Dimensão Afetada	Vulnerabilidade Relacionada	Ação Recomendada	Impacto
Segurança Física e Armazenamento	Servidor local alocado de forma precária na portaria.	Migração imediata do banco de dados para Datacenter Institucional.	Eliminação do risco de sabotagem local e acesso por terceiros não autorizados.
Governança Jurídica e Gestão de Risco	Inexistência do Relatório de Impacto à Proteção de Dados	Elaboração e publicação do Relatório de Impacto à Proteção de Dados Pessoais (RIPD).	Cumprimento estrito do art 38° da LGPD, servindo como blindagem contra sanções administrativas da ANPD.
Base Legal e Direito dos Menores	Consentimento atrelado ao ato da matrícula.	Implementação de Termo de Consentimento específico, destacado e informado para biometria.	Garantia do princípio do melhor interesse do menor e mitigação da hipervigilância.
Treinamento e Cultura de Dados	Desconhecimento dos agentes e manuseio de dados.	Instituição de programas permanentes de capacitação em segurança da informação e cidadania para servidor, terceirizados da portaria e equipe pedagógica.	Redução de erros operacionais sistemáticos e consolidação dos princípios da finalidade e necessidade.

Fonte: Elaborado pelos autores (2026)

O detalhamento apresentado no Quadro 4 consolida a transição de um modelo de conformidade para a governança de dados adequada ao ecossistema escolar. Ao incorporar as soluções recomendadas unindo segurança física do *hardware*, sofisticação e maturidade das bases jurídicas juntamente ao fomento da cultura técnico-pedagógica, o plano estabelece um roteiro prático para que instituições superem as vulnerabilidades, assim como as evidenciadas na portaria do IFRO Câmpus Porto Velho Zona Norte, a conversão de processo precários em fluxos protegidos e validados por relatórios de impacto, não apenas afasta a incidência de pesadas sanções administrativas e civis, onde de acordo com Albuquerque et al. (2024), assegura que o avanço tecnológico caminhe com a dignidade, privacidade e o desenvolvimento da cidadania digital de discentes e servidores.

5 CONSIDERAÇÕES FINAIS

A implementação de sistemas de controle de acesso e o tratamento de dados pessoais sensíveis em ambientes escolares públicos exigem a harmonização entre a segurança física e a proteção jurídica. A conformidade com a LGPD nas instituições de ensino básico vai além do cumprimento de formalidades burocráticas, configurando um requisito indispensável para a garantia dos direitos fundamentais da personalidade e para a preservação da dignidade de crianças e adolescentes.

O principal obstáculo enfrentado pela administração pública educacional reside na acentuada escassez de maturidade institucional em segurança da informação e na ausência de programas formativos contínuos para os gestores e servidores. A precariedade da infraestrutura tecnológica e governança de dados elevam os riscos de incidentes cibernéticos graves, como o vazamento de dados. Diante da responsabilidade civil objetiva do Estado, a negligência na governança dessas informações sensíveis expõe a instituição à severas sanções e fragiliza de forma irreversível a confiança da sociedade na gestão pública escolar.

Constatou-se também que o direito social à educação deve coexistir harmonicamente com o direito fundamental à proteção de dados pessoais, visto que a vulnerabilidade jurídica dos menores exige a aplicação rigorosa do princípio do melhor interesse. A coleta de dados nas portarias eletrônicas necessita de justificativas técnicas pautadas na finalidade, na necessidade e na proporcionalidade, vedando o armazenamento por tempo indeterminado e o desvio de finalidade. Mecanismos menos invasivos de identificação devem ser priorizados pelas secretarias de educação, reservando o monitoramento biométrico inteligente para cenários de absoluta excepcionalidade devidamente auditados.

Para reverter o cenário de vulnerabilidade detectado, faz-se necessária a construção de uma sólida cultura de cidadania digital que envolva ativamente toda a comunidade escolar no processo de fiscalização, governança de dados e segurança física. A formulação de políticas públicas integradas deve contemplar a elaboração prévia de relatórios de impacto à proteção de dados e a segregação estrita de funções no manuseio de arquivos digitais. A presença de encarregados de dados qualificados nas secretarias e a instituição de protocolos rígidos de resposta a incidentes constituem medidas mandatórias para salvaguardar a privacidade estudantil sem comprometer a eficiência administrativa.

Nosso trabalho se limitou ao Instituto Federal Campus Porto Velho Zona Norte, porém possui uma grande variedade de análise em outras instituições sejam públicas ou privadas, pudemos entender a diferença entre cada ponto de vigilância ou de acesso que nos fez ter um olhar crítico sobre se aquela ferramenta está de fato sendo usada da forma correta e de acordo com a legislação e cumprindo os direitos básicos do cidadão.

REFERÊNCIAS

ALBUQUERQUE, Maria Analice et al. **Segurança de dados na educação online**: riscos, desafios e boas práticas. Missioneira, v. 26, n. 2, p. 29-41, 2024. Disponível em: https://cemipa.com.br/revistas/index.php/missioneira/article/view/56. Acesso em: 15 de mai. 2026.

AMORIM, Lauro Jorge; MÜLLER, César Santini. **Proteção de dados no ensino jurídico público federal**: o direito social à educação à luz do direito fundamental à proteção de dados pessoais. Revista Avant, v. 9, n. 1, p. 269-284, 2025. Disponível em: https://ojs.sites.ufsc.br/index.php/avant/article/view/8304. Acesso em: 15 de mai. 2026.

CANDIANI, Israel Ferreira; PEREIRA, Otaviano José. **Lei Geral de Proteção de Dados (LGPD) nas instituições de ensino**: desafios formativos para sua aplicação e gestão. Cadernos da FUCAMP, v. 27, 2024. Disponível em: https://www.revistas.fucamp.edu.br/index.php/cadernos/article/view/3405. Acesso em: 15 de mai. 2026.

FALANGOLA, Renata et al. **Proteção de dados e vigilância digital em ambientes educacionais**: desafios jurídicos frente à lei geral de proteção de dados (LGPD). ERR01, v. 10, n. 3, p. e7897-e7897, 2025. Disponível em: https://periodicos.newsciencepubl.com/err01/article/view/7897. Acesso em: 15 de mai. 2026.

FIGUEIREDO, Simone Oliveira et al. **Cidadania digital**: caminhos para ambientes educacionais seguros e éticos. Revista Tópicos, v. 4, n. 29, p. 1-13, 2026. Disponível em: https://revistatopicos.com.br/artigos/cidadania-digital-caminhos-para-ambientes-educacionais-seguros-e-eticos. Acesso em: 15 de mai. 2026.

LARANJEIRA, Ludimila et al. **Vazamento de dados em ambiente escolar**: consequências, responsabilidade civil e análise à luza da LGPD. Revista Brasileira de Estudos Jurídicos, v. 19, n. 3, p. 1-10, 2025. Disponível em: https://portalunifipmoc.emnuvens.com.br/rbej/article/view/274. Acesso em: 15 de mai. 2026.

LEITE, Felipe Renova Varela. **O aperfeiçoamento do tratamento de dados de crianças e adolescentes, nos âmbitos público e privado**. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 5, p. 556-568, 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/13729. Acesso em: 15 de mai. 2026.

MANZATO, Welington Junior Jorge et al. **Direitos da personalidade e a lei nº 15.001/2024**: conflitos e convergências no ambiente escolar. Boletim de Conjuntura (BOCA), v. 21, n. 61, p. 249-280, 2025. Disponível em: https://revistaboletimconjuntura.com.br/boca/article/view/6664. Acesso em: 15 de mai. 2026.

MIRANDA, Rodrigo Oliveira et al. **Lei geral de proteção de dados (LGPD**) e o uso da inteligência artificial (ia) na educação: desafios e implicações jurídicas. Veredas do Direito, v. 23, p. e235329-e235329, 2026. Disponível em: https://revista.domhelder.edu.br/index.php/veredas/article/view/5329. Acesso em: 15 de mai. 2026.

MOREIRA, Gilmar. **Controle e transparência na gestão de dados pela administração pública: um estudo de caso sobre a política pública de atendimento educacional especializado em sala de recursos e alunos em atendimento em classe regida por professor especializado–da Secretaria Estadual de Educação-SP**. Revista da Escola Superior da PGE-SP, v. 14, n. 1, p. 181-202, 2023. Disponível em: https://revistas.pge.sp.gov.br/revistaespgesp/article/view/1557. Acesso em: 15 de mai. 2026.

REIS, Fernanda Teixeira; DO CARMO DIREITO, Denise. **Dados pessoais e políticas públicas: O que revelar e o que preservar?.** Revista Brasileira de Avaliação, v. 12, n. 1, p. 0-0, 2023. Disponível em: https://rbaval.org.br/journal/rbaval/article/doi/10.4322/rbaval202312016. Acesso em: 15 de mai. 2026.

RODRIGUES, Alison Cleiton; PAULA, Alan Pinheiro. **Prestação dos serviços públicos à luz da Lei Geral de Proteção de Dados (LGPD)**. Academia De Direito, v. 4, p. 1039-1055, 2022. Disponível em: https://periodicos.unc.br/index.php/acaddir/article/view/3907. Acesso em: 15 de mai. 2026.

SILVA, Gerson Souza et al. **A segurança da informação e a lei geral de proteção de dados em ambiente escolar**. Revista de Direito Magis, v. 3, n. 1, 2025. Disponível em: https://periodico.agej.com.br/index.php/revistamagis/article/view/54. Acesso em: 15 de mai. 2026.