REVISTA ERR01 ISSN: 2595-1378

PROTEÇÃO DE DADOS E VIGILÂNCIA DIGITAL EM AMBIENTES EDUCACIONAIS: DESAFIOS JURÍDICOS FRENTE À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

DATA PROTECTION AND DIGITAL SURVEILLANCE IN EDUCATIONAL ENVIRONMENTS: LEGAL CHALLENGES IN THE FACE OF THE GENERAL DATA PROTECTION LAW (LGPD)

PROTECCIÓN DE DATOS Y VIGILANCIA DIGITAL EN ENTORNOS EDUCATIVOS: RETOS JURÍDICOS ANTE LA LEY GENERAL DE PROTECCIÓN DE DATOS (LGPD)

https://doi.org/10.56238/ERR01v10n3-029

Renata de Farias Falangola
Doutoranda em Ciências Jurídicas
Instituição: Facultad Interamericana de Ciencias Sociales
E-mail: renatafalangola@hotmail.com

Natal Vieira Júnior
Doutorando Ciências Jurídicas
Instituição: Facultad Interamericana de Ciencias Sociales
E-mail: nvjunior22@hotmail.com

Rita de Cássia Moura
Doutoranda em Ciências Jurídicas
Instituição: Facultad Interamericana de Ciencias Sociales
E-mail: r_cassia87@hotmsil.com

Isabella da Costa Miranda Ferreira
Doutoranda em Ciências Jurídicas
Instituição: Facultad Interamericana de Ciencias Sociales
E-mail: isabellaicmf@gmail.com

Ilson Vieira Ruiz
Mestrando em Estudos Jurídicos com Ênfase em Direito Internacional
Instituição: Must University
E-mail: ilsonruiz19729@student.mustedu.co

RESUMO
Este trabalho analisa comparativamente os regimes jurídicos de proteção de dados pessoais aplicáveis ao setor educacional em diferentes jurisdições, com foco especial na Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil, no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e nas legislações setoriais dos Estados Unidos, como a FERPA e a COPPA. A pesquisa parte da constatação de que a digitalização intensiva dos ambientes educacionais tem transformado escolas

ISSN: 2595-1378

e universidades em espaços altamente dataficados, nos quais o tratamento de dados pessoais se torna central para o funcionamento institucional. A partir de uma abordagem qualitativa e exploratória, o estudo identifica convergências e divergências entre os modelos regulatórios, especialmente no que se refere ao escopo normativo, às bases legais de tratamento, à proteção de dados sensíveis, aos direitos dos titulares e aos mecanismos de governança e enforcement. Conclui-se que, embora haja princípios comuns entre os diferentes ordenamentos, como finalidade, transparência e segurança, as exigências práticas variam significativamente, demandando das instituições educacionais uma postura proativa e ética na gestão de dados, com vistas à proteção da privacidade e à promoção de uma cultura digital democrática e inclusiva.

Palavras-chave: Proteção de Dados. Educação Digital. LGPD. Governança Informacional.

ABSTRACT

This paper comparatively analyzes the legal frameworks for personal data protection applicable to the education sector in different jurisdictions, with a special focus on Brazil's General Data Protection Law (LGPD), the European Union's General Data Protection Regulation (GDPR), and sectoral legislation in the United States, such as FERPA and COPPA. The research is based on the observation that the intensive digitalization of educational environments has transformed schools and universities into highly datafied spaces, in which the processing of personal data has become central to institutional functioning. Using a qualitative and exploratory approach, the study identifies convergences and divergences between regulatory models, especially regarding the regulatory scope, legal bases for processing, the protection of sensitive data, data subject rights, and governance and enforcement mechanisms. The conclusion is that, although there are common principles across the different legal systems, such as purpose, transparency, and security, practical requirements vary significantly, requiring educational institutions to adopt a proactive and ethical approach to data management, aiming to protect privacy and promote a democratic and inclusive digital culture.

Keywords: Data Protection. Digital Education. LGPD. Information Governance.

RESUMEN

Este artículo analiza comparativamente los marcos legales de protección de datos personales aplicables al sector educativo en diferentes jurisdicciones, con especial énfasis en la Ley General de Protección de Datos (LGPD) de Brasil, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la legislación sectorial estadounidense, como la FERPA y la COPPA. La investigación se basa en la observación de que la intensa digitalización de los entornos educativos ha transformado las escuelas y universidades en espacios altamente datificados, donde el tratamiento de datos personales se ha vuelto fundamental para el funcionamiento institucional. Mediante un enfoque cualitativo y exploratorio, el estudio identifica convergencias y divergencias entre los modelos regulatorios, especialmente en lo que respecta al alcance regulatorio, las bases legales para el tratamiento, la protección de datos sensibles, los derechos de los interesados y los mecanismos de gobernanza y cumplimiento. La conclusión es que, si bien existen principios comunes en los diferentes sistemas legales, como la finalidad, la transparencia y la seguridad, los requisitos prácticos varían significativamente, lo que exige que las instituciones educativas adopten un enfoque proactivo y ético en la gestión de datos, con el objetivo de proteger la privacidad y promover una cultura digital democrática e inclusiva.

Palabras clave: Protección de Datos. Educación Digital. LGPD. Gobernanza de la Información.

ISSN: 2595-1378

1 INTRODUÇÃO

A sociedade contemporânea encontra-se imersa em um processo histórico de digitalização acelerada e irreversível, que atravessa todas as dimensões da vida humana — desde as relações interpessoais mais íntimas até as estruturas econômicas, políticas e institucionais de maior complexidade. No campo educacional, esse fenômeno tem se manifestado com intensidade particular, provocando transformações profundas na forma como o processo de ensino-aprendizagem é concebido, operacionalizado e avaliado. A incorporação de tecnologias digitais, plataformas de aprendizagem online, sistemas de gestão acadêmica baseados em nuvem e, mais recentemente, ferramentas alimentadas por inteligência artificial (IA), tem redefinido os contornos da experiência educacional, deslocando-a de um espaço predominantemente físico para um ecossistema informacional altamente conectado e dataficado.

Historicamente, os ambientes escolares foram estruturados a partir de interações presenciais, com fluxos informacionais restritos ao espaço físico e ao contato direto entre professores, estudantes e a comunidade escolar. Contudo, nas últimas décadas, observa-se uma transição para modelos híbridos e digitais, nos quais o uso de tecnologias educacionais tornou-se não apenas complementar, mas central. Segundo Selwyn (2016), essa transformação não se limita à adoção de ferramentas tecnológicas, mas implica uma reconfiguração epistemológica e institucional do próprio conceito de educação, que passa a ser mediada por algoritmos, métricas de desempenho e sistemas de vigilância digital.

Embora os avanços tecnológicos tragam benefícios inegáveis — como a flexibilização das metodologias pedagógicas, a ampliação do acesso à informação e a personalização das estratégias de ensino —, eles também introduzem novos desafios éticos, jurídicos e pedagógicos. A escola e a universidade deixam de ser apenas espaços de construção do conhecimento e passam a operar como ambientes intensamente dataficados, nos quais a coleta, o processamento, o armazenamento e o compartilhamento de dados pessoais tornam-se atividades contínuas e estruturantes. Nesse contexto, os dados de estudantes, professores e funcionários deixam de ser meros registros administrativos e passam a constituir ativos informacionais estratégicos, com potencial de exploração para fins acadêmicos, gerenciais e, em casos extremos, para práticas abusivas de vigilância e controle (ZUBOFF, 2019).

A coleta automatizada de métricas de desempenho, o uso de câmeras com reconhecimento facial, o registro constante de interações virtuais e a aplicação de algoritmos para avaliação comportamental suscitam questionamentos urgentes sobre os limites da atuação institucional e os riscos à privacidade, à liberdade e à dignidade dos sujeitos envolvidos. A tensão central que emerge dessa realidade reside na necessidade de conciliar dois objetivos frequentemente percebidos como

ISSN: 2595-1378

antagônicos: de um lado, a promoção de ambientes de aprendizagem eficazes, seguros e tecnologicamente atualizados; de outro, a garantia da proteção integral dos direitos fundamentais dos titulares de dados, especialmente em contextos educacionais que envolvem populações vulneráveis, como crianças e adolescentes.

Nesse cenário, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) representa um marco normativo indispensável. Ao estabelecer princípios como finalidade, adequação, necessidade, segurança e transparência, a LGPD impõe às instituições de ensino o dever jurídico de revisar suas práticas de tratamento de dados, com especial atenção àqueles classificados como sensíveis — categoria que inclui dados biométricos, informações de saúde, convicções religiosas, entre outros, e que demanda salvaguardas adicionais (BRASIL, 2018). O tratamento de dados de crianças e adolescentes, por sua vez, deve observar o princípio do melhor interesse, conforme previsto no art. 14 da LGPD, em consonância com o Estatuto da Criança e do Adolescente (BRASIL, 1990).

As obrigações impostas pela LGPD transcendem os protocolos técnicos de segurança cibernética e exigem a construção de uma cultura institucional de governança de dados, na qual decisões sobre coleta, uso e compartilhamento de informações sejam pautadas pela minimização de riscos e pelo respeito incondicional aos direitos dos titulares. Como destaca Doneda (2019), a proteção de dados deve ser compreendida como um direito fundamental, intimamente ligado à autodeterminação informacional e à preservação da liberdade individual em sociedades digitais.

A relevância do tema, portanto, não se limita à conformidade legal, mas se estende ao campo da responsabilidade social e pedagógica das instituições educacionais. É imperativo que essas organizações sejam capazes de explorar o potencial das tecnologias emergentes sem comprometer a autonomia cognitiva, a liberdade de expressão e a formação crítica dos estudantes. Discutir a proteção de dados na educação significa, em última instância, discutir os valores que orientam a construção da sociedade contemporânea: uma sociedade que utiliza a tecnologia como instrumento de emancipação e democratização do conhecimento, ou uma que, inadvertidamente, consolida estruturas de vigilância e controle incompatíveis com os princípios democráticos e os direitos humanos.

Assim, a abordagem da proteção de dados em ambientes educacionais não é apenas pertinente, mas absolutamente necessária. Ela enfrenta, simultaneamente, os riscos e as promessas de uma educação em constante transformação digital, buscando assegurar que o progresso tecnológico seja aliado — e não ameaça — à realização dos direitos fundamentais, à promoção da cidadania e à construção de uma cultura educacional ética, inclusiva e crítica.

ISSN: 2595-1378

1.1 UM BREVE COMPARATIVO

A crescente digitalização dos ambientes educacionais, impulsionada por plataformas de ensino remoto, sistemas de gestão acadêmica e tecnologias de monitoramento, tem intensificado o debate sobre a proteção de dados pessoais no setor educacional. Nesse contexto, a comparação entre os regimes jurídicos de proteção de dados revela diferenças estruturais significativas quanto ao escopo normativo, às bases legais de tratamento e aos mecanismos de governança e enforcement adotados por diferentes países e blocos econômicos.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, estabelece um marco regulatório de aplicação transversal, incidindo sobre todo e qualquer tratamento de dados pessoais, inclusive aquele realizado por instituições de ensino públicas e privadas, bem como por provedores de tecnologia educacional. A LGPD reconhece como dados sensíveis aqueles que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, dados genéticos, biométricos, entre outros, exigindo tratamento diferenciado e medidas adicionais de segurança (BRASIL, 2018). Particular atenção é conferida ao tratamento de dados de crianças e adolescentes, cuja coleta e uso devem observar o melhor interesse do titular, conforme previsto no art. 14 da referida lei.

Na União Europeia, o Regulamento Geral sobre a Proteção de Dados (GDPR), vigente desde 2018, apresenta estrutura normativa semelhante em princípios, como finalidade, necessidade, transparência e segurança, mas com maior densidade regulatória e alcance extraterritorial. O GDPR aplica-se inclusive a instituições fora do território europeu que tratem dados de residentes da União Europeia, o que impacta diretamente universidades e plataformas educacionais que utilizam serviços de nuvem ou infraestrutura tecnológica hospedada na Europa (UNIÃO EUROPEIA, 2016). Essa característica amplia o escopo de responsabilidade das instituições educacionais, exigindo conformidade mesmo em operações transfronteiriças.

No que tange às bases legais para o tratamento de dados, tanto a LGPD quanto o GDPR adotam um modelo multipilar, que inclui o consentimento do titular, o cumprimento de obrigação legal, a execução de políticas públicas, o legítimo interesse do controlador, entre outras hipóteses. Em ambientes educacionais, isso significa que nem toda operação de tratamento dependerá de consentimento expresso, podendo ser legitimada por obrigações contratuais ou legais vinculadas à prestação do serviço educacional. Contudo, é imprescindível que tais operações respeitem os princípios da finalidade, da necessidade e da transparência, conforme orientações da Autoridade Nacional de Proteção de Dados (ANPD) e da European Data Protection Board (EDPB) (BRASIL, 2018; UNIÃO EUROPEIA, 2016).

ISSN: 2595-1378

Nos Estados Unidos, o modelo regulatório é fragmentado e setorial, sem a existência de uma legislação federal geral sobre proteção de dados. A Family Educational Rights and Privacy Act (FERPA), de 1974, regula o acesso e a divulgação de registros educacionais, exigindo consentimento dos pais ou responsáveis para compartilhamento de informações fora das exceções previstas. No entanto, a FERPA não contempla um regime de bases legais estruturado como o europeu ou o brasileiro, o que limita sua aplicabilidade em cenários mais complexos de tratamento de dados (UNITED STATES, 1974). Complementarmente, a Children's Online Privacy Protection Act (COPPA), de 1998, impõe a exigência de consentimento parental verificável para coleta online de dados de crianças menores de 13 anos, sendo especialmente relevante para edtechs e plataformas voltadas ao público infantil (UNITED STATES, 1998).

A proteção de dados sensíveis, como biometria, é tratada com rigor tanto pela LGPD quanto pelo GDPR. O uso de reconhecimento facial para controle de frequência, proctoring em avaliações remotas e outras tecnologias intrusivas exige justificativas robustas, avaliação de proporcionalidade e, quando aplicável, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) ou Data Protection Impact Assessment (DPIA), conforme previsto nas respectivas legislações (BRASIL, 2018; UNIÃO EUROPEIA, 2016). Nos Estados Unidos, a FERPA não abrange integralmente dados como telemetrias e metadados coletados por provedores externos, o que transfere para contratos e políticas internas a responsabilidade pela conformidade e segurança (GELLER, 2022).

A legislação estadual da Califórnia, representada pela California Consumer Privacy Act (CCPA) e sua emenda posterior, a California Privacy Rights Act (CPRA), introduz elementos mais avançados de proteção, como o direito de opt-out da venda ou compartilhamento de dados e a criação da categoria de "informações pessoais sensíveis", que inclui identificadores biométricos. Embora não exija formalmente a figura do DPO, a CPRA estabelece obrigações de governança e avaliação de risco para atividades como publicidade comportamental e decisões automatizadas, o que dialoga com práticas educacionais baseadas em algoritmos de personalização e análise de desempenho (CALIFORNIA, 2018; 2020; KAMINSKI; URBAN, 2021).

No plano dos direitos dos titulares, tanto a LGPD quanto o GDPR asseguram prerrogativas como acesso, correção, eliminação, portabilidade e oposição ao tratamento, além de garantias contra decisões exclusivamente automatizadas. Tais direitos são particularmente relevantes em ambientes educacionais que utilizam sistemas de avaliação algorítmica, detecção de plágio e análise preditiva de comportamento estudantil. A FERPA, por sua vez, confere direitos de inspeção e correção de registros educacionais, mas não contempla a portabilidade nos moldes europeus. A COPPA garante aos pais o direito de revisar, excluir e impedir a coleta futura de dados de seus filhos, enquanto a CCPA/CPRA

reforça os direitos de saber, corrigir e deletar, com especial ênfase na transparência e no controle do compartilhamento por menores (UNITED STATES, 1974; 1998; CALIFORNIA, 2018; 2020).

A governança institucional também apresenta variações relevantes. A LGPD recomenda a designação de encarregado pelo tratamento de dados (DPO) e exige a elaboração de RIPD em casos de risco elevado. O GDPR torna o DPO obrigatório em diversas situações e impõe a realização de DPIA em cenários de alto risco. Já regimes como o sul-africano (POPIA), o canadense (PIPEDA), o britânico (Data Protection Act 2018) e o australiano (Privacy Act) replicam princípios de minimização, finalidade e segurança, mas divergem quanto à estrutura de enforcement e aos requisitos formais (SOUTH AFRICA, 2013; CANADA, 2000; UNITED KINGDOM, 2018; AUSTRALIA, 1988).

A transferência internacional de dados constitui um ponto de tensão nos ambientes educacionais, especialmente em ecossistemas que dependem de serviços de nuvem e infraestrutura transfronteiriça. A LGPD condiciona tais transferências à existência de cláusulas contratuais específicas, garantias adequadas ou decisões de adequação por parte da ANPD. O GDPR, por sua vez, opera com decisões de adequação, cláusulas contratuais padrão (SCCs) e regras corporativas vinculantes (BCRs), exigindo avaliação concreta das salvaguardas do país de destino. Já nos Estados Unidos, a conformidade depende de contratos e políticas internas, sem um mecanismo geral de adequação (BRASIL, 2018; UNIÃO EUROPEIA, 2016; UNITED STATES, 1974; 1998).

Por fim, os mecanismos de resposta a incidentes e de enforcement variam em rigor e estrutura. O GDPR estabelece prazo de até 72 horas para notificação à autoridade competente em caso de violação de dados, além de comunicação aos titulares em situações de alto risco. A LGPD determina medidas proporcionais de segurança e comunicação à ANPD e aos titulares, prevendo sanções como advertência, multa e bloqueio ou eliminação de dados. A CCPA/CPRA combina sanções administrativas com a possibilidade de ação privada por falhas de segurança decorrentes de negligência, ampliando a responsabilização das instituições (CALIFORNIA, 2018; 2020).

Em síntese, a análise comparativa evidencia que, embora haja convergência em princípios fundamentais, os regimes jurídicos de proteção de dados aplicáveis ao setor educacional apresentam diferenças significativas quanto à estrutura normativa, à exigência de governança e à efetividade dos mecanismos de controle. Tais distinções demandam das instituições educacionais uma postura proativa e contextualizada, capaz de adaptar suas práticas às exigências legais e éticas de cada jurisdição.

Tabela 1 - Principais Leis Comparáveis

País / Bloco	Lei	Pontos em Comum com a LGPD	Diferenças Relevantes
União Europeia	**GDPR – General Data Protection Regulation**	Consentimento, transparência, direitos do titular, DPO, notificação de incidentes	Critérios de territorialidade mais amplos; consentimento mais rigoroso; multas mais altas

ISSN: 2595-1378

País / Bloco	Lei	Pontos em Comum com a LGPD	Diferenças Relevantes
Canadá	**PIPEDA – Personal Information Protection and Electronic Documents Act**	Proteção no setor privado; direitos de acesso e correção	Menos abrangente que GDPR/LGPD; aplicação setorial
EUA (Califórnia)	**CCPA – California Consumer Privacy Act**	Direitos de acesso, exclusão e opt-out de venda de dados	Foco no consumidor; ausência de lei federal unificada
Japão	**APPI – Act on the Protection of Personal Information**	Reconhecimento de adequação pela UE; princípios de consentimento e segurança	Ênfase em transferências internacionais; ajustes culturais/regulatórios
China	**PIPL – Personal Information Protection Law**	Direitos do titular; bases legais; regras para transferência internacional	Maior controle estatal; integração com leis de segurança nacional
Austrália	**Privacy Act 1988** (com emendas)	Direitos de acesso e correção; princípios semelhantes	Estrutura menos detalhada que GDPR/LGPD; agência única de aplicação

Fonte: Autores.

A governança da proteção de dados pessoais em instituições educacionais constitui um dos pilares fundamentais para a conformidade normativa e a preservação dos direitos fundamentais dos titulares, especialmente em contextos marcados pela crescente digitalização das práticas pedagógicas. No Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece diretrizes claras para a estruturação de mecanismos internos de controle e transparência, incluindo a figura do encarregado pelo tratamento de dados pessoais, também denominado Data Protection Officer (DPO). Conforme o art. 41 da LGPD, esse profissional atua como elo entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), sendo responsável por orientar, fiscalizar e responder sobre as práticas de tratamento adotadas pela instituição (BRASIL, 2018).

Embora a designação do DPO não seja obrigatória em todos os casos, a própria ANPD, por meio de suas diretrizes interpretativas, recomenda fortemente sua nomeação em organizações que realizam tratamento de dados em larga escala ou lidam com dados sensíveis, como ocorre em instituições educacionais que coletam informações biométricas, registros acadêmicos, dados de saúde e dados de menores de idade (ANPD, 2021). A presença de um encarregado contribui para a institucionalização da cultura de proteção de dados, promovendo maior controle sobre fluxos informacionais e mitigando riscos associados ao uso de tecnologias de vigilância, como sistemas de reconhecimento facial, monitoramento remoto de provas (proctoring) e plataformas de aprendizagem adaptativa.

Além disso, a LGPD prevê, no art. 38, a obrigatoriedade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) sempre que o tratamento puder acarretar riscos relevantes aos direitos e liberdades dos titulares. Esse instrumento, inspirado nas práticas europeias, permite que a

ISSN: 2595-1378

instituição avalie previamente os riscos envolvidos em determinadas operações, proponha medidas de mitigação e documente sua diligência, sendo especialmente relevante em ambientes educacionais que adotam tecnologias intrusivas ou algoritmos de decisão automatizada (BRASIL, 2018; DONEDA, 2019).

No contexto da União Europeia, o Regulamento Geral sobre a Proteção de Dados (GDPR), em vigor desde 2018, apresenta uma estrutura normativa mais rigorosa e detalhada. O art. 37 do GDPR estabelece a obrigatoriedade de designação de DPO para todas as autoridades públicas e para organizações que realizem monitoramento sistemático e em larga escala de dados pessoais, categoria que abrange diversas atividades educacionais, como gestão de desempenho estudantil, análise de comportamento e controle de frequência digital (UNIÃO EUROPEIA, 2016). Ademais, o art. 35 do regulamento impõe a realização de Avaliação de Impacto à Proteção de Dados (Data Protection Impact Assessment – DPIA) em operações de alto risco, como o uso de inteligência artificial em avaliações, vigilância eletrônica e análise preditiva de comportamento, reforçando os princípios de privacy by design e privacy by default (COSTA, 2020).

Em contraste, o ordenamento jurídico dos Estados Unidos apresenta uma abordagem fragmentada e setorial, sem a existência de uma legislação federal geral sobre proteção de dados. Normas como a Family Educational Rights and Privacy Act (FERPA) e a Children's Online Privacy Protection Act (COPPA) concentram-se em aspectos específicos da privacidade educacional, como o controle de acesso a registros acadêmicos e a coleta de dados de menores de 13 anos em ambientes online (UNITED STATES, 1974; UNITED STATES, 1998). A ausência de exigência formal de designação de DPO ou de instrumentos padronizados de avaliação de risco transfere para as instituições e seus contratos internos a responsabilidade pela definição de protocolos de segurança e governança, o que pode gerar lacunas na proteção dos titulares, especialmente em contextos de terceirização de serviços tecnológicos (GELLER, 2022).

A legislação estadual da Califórnia, por sua vez, representa um avanço dentro do modelo norte-americano. A California Consumer Privacy Act (CCPA), complementada pela California Privacy Rights Act (CPRA), introduz mecanismos mais robustos de governança, como o direito de saber, corrigir e excluir dados pessoais, além da exigência de avaliações de impacto em determinadas atividades, como publicidade comportamental e decisões automatizadas com efeitos significativos sobre os titulares (CALIFORNIA, 2018; CALIFORNIA, 2020). Embora não imponha diretamente a figura do DPO, a CPRA cria a California Privacy Protection Agency (CPPA), responsável por fiscalizar e orientar as práticas de tratamento, aproximando-se de modelos de compliance e auditoria regulatória presentes em legislações como a LGPD e o GDPR (KAMINSKI; URBAN, 2021).

ISSN: 2595-1378

Dessa forma, observa-se que os modelos brasileiro e europeu estruturam mecanismos de governança mais claros e formalizados, com previsão expressa de encarregado e instrumentos de avaliação de risco, enquanto regimes como FERPA e COPPA permanecem mais dependentes de políticas institucionais e da autorregulação. A legislação californiana, por sua vez, adota uma postura híbrida, incorporando elementos de governança regulatória sem abandonar a lógica setorial. Em todos os casos, a efetividade da proteção de dados em ambientes educacionais depende não apenas da existência de normas, mas da capacidade institucional de implementá-las de forma ética, transparente e centrada nos direitos dos titulares.

1.2 A NATUREZA REGULATÓRIA DAS LEIS DE PROTEÇÃO DE DADOS

A crescente digitalização das atividades humanas, especialmente no setor educacional, tem intensificado o debate sobre a proteção de dados pessoais. Diversos países têm adotado legislações específicas para regulamentar o tratamento de informações sensíveis, com diferentes escopos, princípios e níveis de abrangência. Este trabalho tem como objetivo analisar o âmbito e a natureza regulatória das principais leis de proteção de dados, com destaque para a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia, e outras legislações relevantes nos Estados Unidos, Canadá, África do Sul, Reino Unido e Austrália.

A governança da proteção de dados em ambientes educacionais demanda mecanismos institucionais capazes de assegurar conformidade normativa e mitigar riscos oriundos do uso de tecnologias de monitoramento e vigilância. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) introduziu a figura do encarregado pelo tratamento de dados pessoais — comumente identificado como *Data Protection Officer* (DPO) — cuja função consiste em atuar como canal de comunicação entre a instituição, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD). Embora a designação não seja obrigatória em todos os casos, é fortemente recomendada para organizações que tratam volume expressivo de informações ou dados sensíveis, como ocorre no setor educacional. Ademais, a LGPD prevê a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) sempre que o tratamento puder gerar riscos relevantes aos direitos fundamentais, instrumento particularmente relevante em práticas como o *proctoring* e o uso de reconhecimento facial para controle de frequência (BRASIL, 2018).

No âmbito europeu, o Regulamento Geral sobre a Proteção de Dados (GDPR) estabelece exigências mais rígidas de governança. O DPO é de designação obrigatória para todas as autoridades e órgãos públicos, bem como para entidades que realizem monitoramento sistemático e em larga escala de titulares, categoria na qual se enquadram diversas atividades de gestão escolar digitalizada. Ademais, o GDPR impõe a obrigatoriedade de condução de Avaliação de Impacto à Proteção de Dados

ISSN: 2595-1378

(*Data Protection Impact Assessment* – DPIA) em tratamentos de alto risco, incluindo vigilância eletrônica, análise de dados comportamentais e uso de inteligência artificial em processos avaliativos, reforçando a lógica de *privacy by design* e *by default* (UNIÃO EUROPEIA, 2016).

Por outro lado, o ordenamento jurídico norte-americano, marcado pela fragmentação regulatória, não prevê a obrigatoriedade de designação de DPO. Normas setoriais como a *Family Educational Rights and Privacy Act* (FERPA) e a *Children's Online Privacy Protection Act* (COPPA) concentram-se em políticas e controles locais, conferindo às instituições de ensino e operadores privados a responsabilidade por adotar salvaguardas adequadas e por garantir consentimento parental verificável no caso de menores. A ausência de uma exigência formal de governança padronizada transfere para contratos e práticas internas a função de delimitar responsabilidades e protocolos de segurança (UNITED STATES, 1974; UNITED STATES, 1998).

Em sentido intermediário, a legislação californiana de consumo — *California Consumer Privacy Act* (CCPA), complementada pela *California Privacy Rights Act* (CPRA) — ainda que não imponha diretamente a figura do DPO, introduz requisitos de governança de risco. Regulamentações recentes exigem avaliações de impacto para determinadas atividades, notadamente no uso de publicidade comportamental e em decisões automatizadas com efeitos relevantes sobre os titulares, aspectos que podem dialogar com ferramentas digitais utilizadas em ambientes educacionais para rastreamento de desempenho ou personalização do ensino (CALIFORNIA, 2018; CALIFORNIA, 2020).

Assim, verifica-se que enquanto a LGPD e o GDPR estruturam mecanismos normativos de governança mais claros e robustos, com previsão de DPO e instrumentos formais de avaliação de risco, regimes como FERPA e COPPA permanecem mais dependentes de políticas institucionais, enquanto a CCPA/CPRA adota postura híbrida, aproximando-se de exigências de *compliance* e de auditoria regulatória.

A governança em proteção de dados nos ambientes educacionais apresenta diferentes graus de maturidade normativa. No caso da LGPD, a figura do encarregado (DPO) é recomendada, cabendo às instituições designar um responsável pelo tratamento e transparência das operações. Além disso, a lei prevê a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) sempre que o tratamento puder gerar riscos relevantes, recurso especialmente aplicável em práticas como *proctoring* e reconhecimento facial. O GDPR, por sua vez, estabelece parâmetros mais rígidos: o DPO é obrigatório em autoridades públicas, bem como em situações de monitoramento sistemático em larga escala, sendo o Relatório de Impacto (DPIA) exigido em tratamentos de alto risco. Diferentemente, FERPA e COPPA, no cenário norte-americano, não impõem a obrigação de um DPO, concentrando-se na responsabilidade das instituições ou distritos escolares quanto à adoção de políticas e controles

ISSN: 2595-1378

internos. Já o regime californiano (CCPA/CPRA) avança ao exigir estruturas de governança de risco e avaliações específicas, sobretudo em atividades de publicidade comportamental e decisões automatizadas.

No que se refere à transferência internacional de dados e provedores de edtech, a LGPD condiciona a prática à existência de salvaguardas adequadas, tais como cláusulas contratuais padrão, certificações reconhecidas ou decisões de adequação pela ANPD. O GDPR segue linha semelhante, mas, após a decisão *Schrems II*, reforçou a necessidade de verificar se as garantias oferecidas são de fato eficazes. Em contraste, legislações como FERPA, COPPA e CCPA não constituem um regime centralizado de transferências, mas exigem contratos robustos entre instituições e fornecedores, que devem contemplar obrigações quanto ao uso limitado, à segurança, à retenção de dados e à proibição de usos secundários.

A segurança da informação e a gestão de incidentes também variam entre os regimes. A LGPD prevê medidas técnicas e administrativas proporcionais, além da notificação de incidentes relevantes à ANPD e, quando necessário, aos titulares afetados. O GDPR impõe um prazo rígido de 72 horas para comunicação às autoridades competentes e, nos casos de alto risco, exige ainda a notificação direta aos titulares. O FERPA não estabelece prazos uniformes, deixando a resposta a incidentes vinculada a políticas locais ou federais, enquanto o CCPA/CPRA, embora não estabeleça prazos específicos, fortalece a possibilidade de ações privadas em caso de violações decorrentes de negligência e impõe a adoção de salvaguardas “razoáveis”.

As sanções refletem o grau de rigor de cada sistema. A LGPD admite desde advertências até multas de até 2% do faturamento limitado a um teto por infração, além da possibilidade de bloqueio e eliminação dos dados. O GDPR, por sua vez, se destaca pela severidade, permitindo multas que alcançam 4% do faturamento global anual da organização. Já no contexto norte-americano, o FERPA prevê como penalidade máxima a perda de financiamento federal das instituições, enquanto o COPPA admite multas civis significativas contra provedores de serviços digitais. O CCPA/CPRA, por fim, conjuga sanções administrativas com a possibilidade de ações privadas, sobretudo em casos de falhas de segurança.

Por fim, as implicações práticas da vigilância digital em educação exigem abordagem crítica. O uso de ferramentas como *proctoring* e reconhecimento facial tende a demandar relatórios de impacto, adoção do princípio do *privacy by default*, prazos curtos de retenção e políticas de transparência reforçadas.

O controle de frequência biométrico, por exemplo, só se justifica diante de estrita necessidade e deve sempre considerar alternativas menos intrusivas. Nos contratos com fornecedores de edtech, é essencial prever cláusulas sobre finalidade, proibição de uso secundário, subcontratações, localização

ISSN: 2595-1378

dos dados, segurança, retenção e garantia dos direitos dos titulares. Além disso, em relação a crianças e adolescentes, torna-se indispensável o consentimento parental informado e específico, em linguagem acessível, assegurando que todas as decisões sejam guiadas pelo princípio do melhor interesse do menor.

Ao se realizar uma análise comparativa dos regimes normativos em matéria de proteção de dados pessoais, observa-se que a LGPD (Brasil) e o GDPR (União Europeia) se projetam como os diplomas mais robustos em termos de densidade principiológica, amplitude de direitos assegurados aos titulares e rigor na governança de dados. Ambos estabelecem um sistema sofisticado de obrigações para agentes de tratamento, notadamente pela previsão da figura do encarregado (*Data Protection Officer* – DPO) e pela exigência de avaliações preventivas de risco, materializadas nos Relatórios de Impacto à Proteção de Dados (*RIPD* na LGPD e *Data Protection Impact Assessment* – DPIA no GDPR).

Tais instrumentos assumem papel crucial no contexto da vigilância digital em ambientes educacionais, sobretudo em práticas como o *proctoring* online e o uso de reconhecimento facial, nas quais a avaliação prévia da proporcionalidade e da necessidade se revela imprescindível para legitimar a intervenção tecnológica (BRASIL, 2018; EUROPEAN UNION, 2016).

O FERPA (Estados Unidos, 1974), por outro lado, apresenta um escopo mais restrito e específico, voltado primordialmente à proteção de registros educacionais formais, tais como históricos escolares e documentos administrativos vinculados a estudantes. Sua lógica é assegurar que a divulgação de tais registros ocorra apenas mediante consentimento expresso dos responsáveis ou nos casos legalmente autorizados. Não se trata, portanto, de um regime abrangente de proteção de dados pessoais, mas de uma norma setorial que encontra sua razão de ser na defesa da privacidade estudantil dentro das instituições de ensino (UNITED STATES, 1974).

O COPPA (Estados Unidos, 1998), por sua vez, tem natureza igualmente setorial, mas assume papel decisivo na tutela da infância no ambiente digital. Ao impor a necessidade de consentimento parental verificável para a coleta de informações de menores de 13 anos, o diploma consolida-se como o principal mecanismo normativo de proteção da criança online. Seu impacto sobre práticas de *edtechs* e plataformas digitais é significativo, uma vez que exige padrões reforçados de segurança, transparência e participação dos pais nos fluxos de tratamento de dados (UNITED STATES, 1998).

Por outro lado, o CCPA (Califórnia, 2018) e sua atualização pelo CPRA (2020) consolidam um modelo inovador de governança de dados assentado na centralidade do consumidor. Diferentemente de FERPA e COPPA, que atuam de forma setorial, o CCPA/CPRA estabelece um regime transversal de direitos de acesso, portabilidade, correção e eliminação, além de introduzir mecanismos de *opt-out* e *opt-in*, com destaque para dados pessoais sensíveis e para atividades de publicidade comportamental.

ISSN: 2595-1378

Essa perspectiva confere protagonismo ao indivíduo na determinação do destino de seus dados, ampliando a noção de autodeterminação informativa. Trata-se de um marco legislativo que, embora menos denso em termos de bases jurídicas de tratamento que o GDPR, avança significativamente na criação de instrumentos de controle direto pelo titular, além de prever sanções administrativas e ações privadas como ferramentas de enforcement (CALIFORNIA, 2018; CALIFORNIA, 2020).

Em um cenário marcado pela crescente dataficação da educação, torna-se urgente repensar não apenas os mecanismos de proteção de dados, mas a própria ontologia dos dados educacionais. A escola contemporânea, ao se converter em um espaço digitalizado, passa a operar como produtora e consumidora de dados em tempo real, transformando cada interação pedagógica em uma unidade informacional passível de análise, categorização e, em muitos casos, monetização. Essa lógica, embora eficiente sob a ótica gerencial, carrega consigo o risco de reduzir sujeitos educacionais a perfis estatísticos, obscurecendo dimensões subjetivas, afetivas e culturais que são constitutivas do processo de aprendizagem.

A proposta de um Ecossistema Ético de Dados Educacionais parte da premissa de que os dados não são neutros. Eles são construções sociais, moldadas por interesses, contextos e finalidades específicas. Portanto, sua coleta, tratamento e uso devem ser orientados por princípios que ultrapassem a legalidade formal e alcancem a legitimidade ética. Isso implica reconhecer que o dado educacional não é apenas um recurso técnico, mas um bem comum, cuja gestão deve ser compartilhada entre todos os atores da comunidade escolar — estudantes, professores, gestores, famílias e sociedade civil.

Nesse ecossistema, a governança de dados deixa de ser uma função exclusivamente administrativa e passa a integrar o projeto pedagógico da instituição. A transparência informacional torna-se um valor educativo, e não apenas um requisito regulatório. Os estudantes são formados para compreender criticamente os fluxos de dados que os envolvem, desenvolvendo competências em cidadania digital, letramento informacional e ética algorítmica. Os professores, por sua vez, são capacitados para utilizar tecnologias de forma consciente, respeitando os limites da privacidade e promovendo práticas pedagógicas que valorizem a autonomia e a diversidade.

A inovação aqui não reside apenas na criação de novos dispositivos técnicos, mas na reconfiguração das relações de poder que estruturam o uso de dados na educação. Propõe-se, por exemplo, a implementação de Conselhos Escolares de Dados, instâncias deliberativas compostas por representantes da comunidade escolar, com a função de avaliar, aprovar e monitorar projetos que envolvam o uso de dados sensíveis. Esses conselhos atuariam como espaços de escuta, negociação e responsabilização, garantindo que decisões sobre tecnologias educacionais sejam tomadas de forma democrática e contextualizada.

Outra dimensão inovadora seria a adoção de Arquiteturas de Dados Pedagógicas, ou seja, sistemas de informação desenhados não apenas para eficiência administrativa, mas para promover valores educacionais como inclusão, equidade e pluralidade. Esses sistemas poderiam incorporar, por exemplo, mecanismos de anonimização seletiva, controle granular de consentimento, e interfaces que permitam aos estudantes visualizar e gerenciar seus próprios dados, fortalecendo sua autonomia informacional.

Por fim, o Ecossistema Ético de Dados Educacionais deve dialogar com a ideia de soberania digital, entendida como a capacidade das instituições educacionais de decidir, de forma consciente e autônoma, sobre os modelos tecnológicos que adotam, os provedores com os quais contratam e os princípios que orientam suas práticas informacionais. Isso implica resistir à lógica da dependência tecnológica e buscar alternativas baseadas em software livre, infraestrutura local e parcerias com comunidades científicas e acadêmicas comprometidas com a ética digital.

2 METODOLOGIA

A presente investigação científica estrutura-se sob uma abordagem qualitativa, de natureza exploratória e comparativa, com vistas a compreender, em profundidade, os contornos normativos e os impactos práticos dos regimes jurídicos de proteção de dados pessoais aplicáveis ao setor educacional em diferentes contextos geográficos e culturais. A escolha por uma metodologia qualitativa justifica-se pela complexidade do objeto de estudo, que envolve não apenas a análise de dispositivos legais, mas também a interpretação de princípios, práticas institucionais e dinâmicas sociotécnicas que permeiam o tratamento de dados em ambientes educacionais mediados por tecnologia. Conforme destaca Minayo (2001), a pesquisa qualitativa é especialmente adequada para o estudo de fenômenos sociais em sua totalidade, permitindo captar significados, intenções e implicações que transcendem a mera literalidade normativa.

A pesquisa foi conduzida por meio de levantamento documental, com análise sistemática de legislações nacionais e supranacionais que versam sobre proteção de dados pessoais, com especial atenção àquelas que incidem diretamente sobre o setor educacional. Foram examinados, entre outros, a Lei Geral de Proteção de Dados Pessoais (LGPD), vigente no Brasil desde 2018; o Regulamento Geral sobre a Proteção de Dados (GDPR), em vigor na União Europeia desde 2016; a Family Educational Rights and Privacy Act (FERPA) e a Children's Online Privacy Protection Act (COPPA), ambas integrantes do ordenamento jurídico dos Estados Unidos; bem como diplomas legais de países como Canadá (PIPEDA), África do Sul (POPIA), Reino Unido (Data Protection Act 2018), Austrália (Privacy Act 1988), Japão (APPI) e China (PIPL). A seleção desses instrumentos normativos foi orientada por critérios de relevância temática, abrangência regulatória e representatividade geopolítica,

de modo a permitir uma análise comparativa que contemplasse diferentes modelos de governança da privacidade e da proteção de dados.

A etapa analítica da pesquisa foi estruturada com base em categorias previamente definidas, que permitiram a sistematização dos dados e a construção de uma matriz comparativa entre os regimes jurídicos estudados. As categorias eleitas — escopo normativo, bases legais para o tratamento de dados, direitos dos titulares, governança institucional, transferência internacional de dados e mecanismos de enforcement — foram inspiradas nos princípios consagrados pela literatura especializada em proteção de dados, como os de finalidade, necessidade, proporcionalidade, segurança e transparência (COSTA, 2020; DONEDA, 2019). A análise comparativa, conforme propõe Yin (2015), permite identificar padrões, contrastes e singularidades entre os diferentes ordenamentos jurídicos, contribuindo para uma compreensão mais refinada das implicações práticas da regulação da privacidade no contexto educacional.

A interpretação dos dados foi realizada de forma crítica e contextualizada, considerando os desafios específicos enfrentados pelas instituições educacionais na implementação de políticas de conformidade com os marcos legais vigentes. Particular atenção foi dedicada às práticas de tratamento de dados sensíveis, como biometria, reconhecimento facial e monitoramento remoto de avaliações (proctoring), que exigem justificativas robustas, avaliações de impacto e salvaguardas adicionais para proteção dos direitos fundamentais dos titulares. A análise também contemplou a relação contratual entre instituições educacionais e provedores de tecnologia (edtechs), especialmente no que tange à responsabilidade compartilhada, à transparência nas cláusulas de uso e à mitigação de riscos decorrentes de transferências internacionais de dados.

Em síntese, a metodologia adotada neste estudo permite não apenas a descrição dos regimes jurídicos de proteção de dados, mas também a problematização de suas implicações práticas, contribuindo para o avanço do debate acadêmico e institucional sobre privacidade, segurança da informação e direitos digitais em ambientes educacionais. Ao lançar luz sobre os pontos de convergência e divergência entre os modelos regulatórios, esta pesquisa busca oferecer subsídios para a formulação de políticas públicas, estratégias de governança e práticas pedagógicas que respeitem e promovam os direitos fundamentais dos estudantes e demais titulares de dados.

3 CONCLUSÃO

A análise comparativa dos regimes jurídicos de proteção de dados pessoais aplicáveis ao setor educacional revela um cenário normativo multifacetado, marcado por convergências principiológicas e divergências estruturais que impactam diretamente a conformidade institucional e a salvaguarda dos direitos dos titulares. A partir da investigação realizada, torna-se evidente que, embora haja uma

ISSN: 2595-1378

tendência global de fortalecimento da proteção da privacidade em ambientes digitais, os caminhos adotados por diferentes jurisdições refletem escolhas regulatórias, culturais e políticas que moldam a forma como os dados são tratados, especialmente em contextos educacionais sensíveis.

No caso brasileiro, a Lei Geral de Proteção de Dados Pessoais (LGPD) representa um marco normativo de caráter transversal, que impõe às instituições educacionais o dever de observar princípios como finalidade, necessidade, transparência e segurança, com especial atenção ao tratamento de dados sensíveis e de crianças e adolescentes (BRASIL, 2018). A figura do encarregado pelo tratamento de dados (DPO) e a exigência de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) em situações de risco elevado demonstram o esforço de institucionalização da governança da privacidade, ainda que a aplicação prática desses instrumentos enfrente desafios de capacitação, estrutura e cultura organizacional.

Na União Europeia, o Regulamento Geral sobre a Proteção de Dados (GDPR) apresenta um modelo mais robusto e detalhado, com exigências formais mais rigorosas, sanções mais severas e efeitos extraterritoriais que influenciam inclusive instituições fora do bloco, especialmente aquelas que utilizam infraestrutura tecnológica europeia (UNIÃO EUROPEIA, 2016). A obrigatoriedade do DPO em determinados contextos e a imposição de avaliações de impacto para tratamentos de alto risco consolidam uma cultura de accountability que serve de referência internacional.

Nos Estados Unidos, a ausência de uma legislação federal unificada resulta em um mosaico regulatório fragmentado, com normas setoriais como a FERPA e a COPPA que, embora relevantes, não oferecem um arcabouço geral de bases legais nem garantias equivalentes às previstas na LGPD e no GDPR. A dependência de contratos e políticas internas para assegurar conformidade, especialmente em relação a provedores de tecnologia educacional, evidencia a necessidade de maior padronização e transparência no tratamento de dados de estudantes (UNITED STATES, 1974; 1998).

A pesquisa também evidenciou que legislações como a CCPA/CPRA, no estado da Califórnia, e normas de países como Canadá, Japão, China e Austrália, embora compartilhem princípios fundamentais com os modelos europeu e brasileiro, apresentam variações significativas quanto à abrangência, enforcement e estrutura institucional. Tais diferenças demandam das instituições educacionais uma postura proativa, capaz de adaptar suas práticas de tratamento de dados às exigências locais e internacionais, especialmente em ecossistemas digitais transfronteiriços.

Em síntese, a proteção de dados em ambientes educacionais não se limita à observância formal da legislação, mas exige uma cultura organizacional orientada pela ética, pela responsabilidade e pela centralidade dos direitos dos titulares. A adoção de práticas como privacy by design, políticas claras de retenção e compartilhamento, capacitação contínua de profissionais e diálogo transparente com estudantes e responsáveis constitui não apenas uma exigência legal, mas um imperativo moral diante

ISSN: 2595-1378

da crescente digitalização da educação. Assim, este estudo contribui para o aprofundamento do debate sobre privacidade e educação, oferecendo subsídios para a construção de ambientes de aprendizagem mais seguros, inclusivos e respeitosos da dignidade humana.

REFERÊNCIAS

AUSTRALIA. Privacy Act 1988. Canberra: Commonwealth of Australia, 1988. Disponível em: https://www.legislation.gov.au/Details/C2004A03712. Acesso em: 18 ago. 2025.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 ago. 2025.

CALIFORNIA. California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100 a 1798.199, 2018. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 18 ago. 2025.

CALIFORNIA. California Privacy Rights Act (CPRA) (Proposition 24), 2020. Disponível em: https://oag.ca.gov/privacy/ccpa/prop24. Acesso em: 18 ago. 2025.

CANADA. Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5. Ottawa: Government of Canada, 2000. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/. Acesso em: 18 ago. 2025.

SOUTH AFRICA. Protection of Personal Information Act (POPIA), Act No. 4 of 2013. Pretoria: Government of the Republic of South Africa, 2013. Disponível em: https://popia.co.za/ (texto consolidado). Acesso em: 18 ago. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – GDPR). Jornal Oficial da União Europeia, L 119, p. 1–88, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 18 ago. 2025.

UNITED KINGDOM. Data Protection Act 2018. Londres: The National Archives, 2018. Disponível em: https://www.legislation.gov.uk/ukpga/2018/12/contents. Acesso em: 18 ago. 2025.

UNITED STATES. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99, 1974. Disponível em: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. Acesso em: 18 ago. 2025.

UNITED STATES. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506; 16 CFR Part 312, 1998. Disponível em: https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act. Acesso em: 18 ago. 2025.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 ago. 2025.

CALIFORNIA. California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100 a 1798.199, 2018. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 18 ago. 2025.

CALIFORNIA. California Privacy Rights Act (CPRA) (Proposition 24), 2020. Disponível em: https://oag.ca.gov/privacy/ccpa/prop24. Acesso em: 18 ago. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – GDPR). Jornal Oficial da União Europeia, L 119, p. 1–88, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 18 ago. 2025.

UNITED STATES. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99, 1974. Disponível em: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. Acesso em: 18 ago. 2025.

UNITED STATES. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506; 16 CFR Part 312, 1998. Disponível em: https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act. Acesso em: 18 ago. 2025.

CALIFORNIA. California Privacy Rights Act (CPRA), Proposition 24, 2020.

COSTA, José Eduardo. Proteção de dados pessoais: fundamentos, direitos e deveres. São Paulo: Saraiva, 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Forense, 2019.

GELLER, Barbara. "Privacy in U.S. Education Law: FERPA and COPPA in the Age of EdTech." Journal of Law and Education, v. 51, n. 2, p. 145–168, 2022.

KAMINSKI, Margot E.; URBAN, Jennifer M. "The California Privacy Rights Act: A New Era for U.S. Data Protection." Berkeley Technology Law Journal, v. 36, n. 1, p. 1–45, 2021.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). Jornal Oficial da União Europeia, Bruxelas, 2016.

UNITED STATES. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99, 1974.

UNITED STATES. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506, 1998.