

IX ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
IV**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, governança e novas tecnologias IV [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Irineu Francisco Barreto Junior; Diogo de Almeida Viana dos Santos – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-588-0

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS IV

Apresentação

Os trabalhos que integram esta publicação foram apresentados no Grupo de Trabalho “Direito, Governança e Novas Tecnologias IV”, realizado virtualmente no dia 25 de junho de 2026, como parte da programação do IX Encontro Virtual do Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI). Esta edição do evento reafirma o compromisso histórico desta sociedade científica, que há décadas promove a excelência na pesquisa jurídica, adaptando-se às novas realidades de interação digital para garantir a continuidade do diálogo acadêmico em nível nacional e internacional.

O presente Grupo de Trabalho consolidou-se como um espaço privilegiado de interlocução, destacando-se não apenas pela densidade teórica dos trabalhos expostos, mas também pelo perfil de seus participantes, composto por professores pesquisadores, doutores, mestres e alunos de pós-graduação, que trouxeram o frescor de suas investigações institucionais para o debate coletivo. A dinâmica das apresentações, conduzida em ambiente virtual, propiciou uma interação instigante entre os autores e o público, permitindo que a pesquisa jurídica fosse discutida sob o prisma da transdisciplinaridade e do enfrentamento dos desafios contemporâneos.

A temática central deste GT, focada na governança e nas novas tecnologias, reflete a inquietude necessária diante das constantes transformações da sociedade da informação. Cientes da complexidade desses fenômenos, os pesquisadores buscaram articular respostas jurídicas para uma realidade que se apresenta em fluxo permanente, onde a técnica e o Direito se entrelaçam. Nesse sentido, as discussões perpassaram por eixos fundamentais que estruturam o debate acadêmico atual, tais como:

Tecnologias Emergentes e Sociedade: A investigação sobre os impactos da cibercultura na esfera pública, o uso da tecnologia como ferramenta de persuasão e os desafios éticos impostos pela biotecnologia e pela segurança pública.

Os trabalhos selecionados para esta coletânea são o resultado de pesquisas rigorosas desenvolvidas em diversos Programas de Pós-graduação em Direito do país. Ressalte-se que todos os artigos foram submetidos a um criterioso processo de seleção, por meio do sistema de dupla avaliação cega por pares (double blind peer review), garantindo o rigor científico e a adequação temática aos propósitos deste Grupo de Trabalho.

Ao apresentar estes anais ao público, os coordenadores manifestam a expectativa de que estas reflexões contribuam efetivamente para o fortalecimento do diálogo interdisciplinar e para o avanço da ciência jurídica brasileira. O objetivo é oferecer aos leitores um panorama crítico e atualizado sobre como o Direito pode e deve mediar as relações em um mundo cada vez mais pautado pela inovação tecnológica, assegurando sempre a prevalência da dignidade humana e dos valores democráticos.

Desejamos a todos uma leitura proveitosa e inspiradora.

Os Coordenadores

Prof. Dr. Irineu Francisco Barreto Junior (Mestrado em Direito das Faculdades Metropolitanas Unidas - FMU-SP)

Prof. Dr. Diogo de Almeida Viana dos Santos (Universidade Estadual do Maranhão; Universidade CEUMA-PPG em Direito e Afirmação de Vulneráveis)

GOVERNANÇA DE DADOS PARA AS ESCOLAS: A PROTEÇÃO DE DADOS PESSOAIS NA ERA DO ENSINO DIGITAL

DATA GOVERNANCE FOR SCHOOLS: PERSONAL DATA PROTECTION IN THE ERA OF DIGITAL EDUCATION

Aleteia Hummes Thaines ¹

Helena Dominguez Paes Landim Bianchi ²

Resumo

Esta pesquisa discute o direito humano de proteção de dados, com recorte delimitado aos dados pessoais de crianças e adolescentes no ambiente de ensino digital. Como problema de pesquisa, questiona-se: de que maneira a implementação do Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025) redefine os parâmetros de governança de dados nas escolas, considerando a vulnerabilidade de crianças e adolescentes e a necessidade de proteger a proteção de dados pessoais em sistemas de ensino digital? A hipótese sustenta que as escolas deverão manter uma governança de dados focada na prevenção para a proteção de dados de crianças e adolescentes ao utilizar plataformas de aprendizagem online e tecnologias pedagógicas. O objetivo geral é analisar os desafios e as obrigações impostas pelo ECA Digital à governança de dados no ensino digital, sob a ótica da proteção de dados como direito humano. Os objetivos específicos são: a) analisar o impacto do ECA Digital para a proteção de dados de crianças e adolescentes nas escolas; e b) investigar os mecanismos de governança de dados escolar necessários para a efetivação de sua responsabilidade no ecossistema digital, adotando uma abordagem de privacy by design. Utiliza-se o método hipotético indutivo, de cunho bibliográfico e documental. Os resultados encontrados apontam que a complexidade do tratamento de dados no ensino digital exige que as escolas estruturem sua governança sob uma postura preventiva e proativa para garantir que o desenvolvimento pedagógico não ocorra em prejuízo à proteção de dados dos estudantes.

Palavras-chave: Proteção de dados de crianças e adolescentes, Governança de dados para as escolas, Eca digital, Direitos humanos, Políticas públicas

children and adolescents, and the need to protect their personal data in digital learning systems? The hypothesis is that schools must maintain data governance focused on prevention to protect children and adolescents' data when utilising online learning platforms and pedagogical technologies. The general objective is to analyse the challenges and obligations imposed by the Digital ECA on data governance in digital education through the lens of data protection as a human right. The specific objectives are: a) to analyse the impact of the Digital ECA on the protection of children and adolescents' data in schools; and b) to investigate the data governance mechanisms necessary for schools to fulfil their responsibilities in the digital ecosystem by adopting a privacy-by-design approach. The research employs a bibliographic and documentary approach using the hypothetical-inductive method. The findings suggest that the complexity of data processing in digital education needs a preventive and proactive approach to data governance in schools, ensuring that pedagogical development does not compromise students' data protection.

Keywords/Palabras-claves/Mots-clés: Data protection for children and adolescents, Data governance for schools, Digital eca, Human rights, Public policy

1. INTRODUÇÃO

A tecnologia tem deixado de ser apenas uma tendência no contexto escolar para se consolidar como uma exigência da sociedade contemporânea, demandando não apenas o acesso de estudantes a dispositivos e plataformas digitais, mas também novas formas de compreensão e garantia de seus direitos nos ambientes digitais (Teixeira et al., 2025). Nesse cenário, a presente pesquisa delimita-se à temática de proteção de dados pessoais de crianças e adolescentes, com enfoque no que se refere à governança de dados para escolas no ambiente de ensino digital.

É cada vez mais frequente a incorporação de recursos digitais ao modo como o ensino é ministrado (Alves, 2025), processo que foi impulsionado com surgimento da pandemia do Covid-19 e a utilização do ensino online e a educação à distância (Dias da Fonseca; Torquato Rego, 2021). Esse panorama corroborou com a maior exposição¹ na *internet* de crianças e adolescentes a aplicativos e conexão em dispositivos online, despertando a necessidade de atenção ao tratamento dos dados pessoais dos alunos dessa faixa etária (Dias da Fonseca; Torquato Rego, 2021).

Assim, a pesquisa se justifica na medida em que a crescente digitalização do ensino expõe crianças e adolescentes à constante e facilitada coleta de dados pessoais, muitas vezes de forma imperceptível (Bianchi, 2025), bem como à exposição a riscos no uso indevido dessas informações. Isso porque apesar dos benefícios aportados ao ensino mediante o uso de tecnologias educacionais, existe uma intensa coleta e armazenamento de dados dos alunos nesses sistemas digitais, fator que atrai o risco de violações de segurança ou uso indevido dessas informações (Alves, 2025).

Na medida em que escolas se veem demandadas por ideais de modernização e inovação constante, a tendência é a submissão aos imperativos de mercado (Costa Júnior et al., 2026), sem que isso necessariamente signifique sua prontidão técnica para tanto. Diante disso, a preocupação na proteção de dados de crianças e adolescentes também decorre da baixa maturidade de escolas para a salvaguarda dos dados e gestão de terceiros fornecedores de plataformas educacionais, como *edtechs*², cenário fértil para fluxos não autorizados e comercialização de dados a intermediários e para alvo de invasões cibernéticas (Alves, 2025).

¹ A TIC Kids Online 2025 indica que 85% da população de 9 a 17 anos possui perfil em, ao menos, uma rede social (NIC.br, 2026), evidenciando que não se trata de um uso excepcional da internet, mas de um ambiente que faz parte da rotina de crianças e adolescentes que não foi projetado para protegê-los (Oliveira e Horta, 2026).

² *Edtechs*: abreviação para “*educational technology*”, as chamadas *startups* ou empresas que utilizam tecnologia para inovar no setor da educação (Costa Júnior et al., 2026).

Diante disso, torna-se imprescindível refletir sobre como as ações das escolas relativas à disponibilização, regulação, acesso, gestão e utilização do ambiente de ensino digital para crianças e adolescentes visem seu melhor interesse (Bianchi, 2025) e a proteção de dados como preocupação primordial.

Da perspectiva jurídica, tem-se que a proteção de dados é reconhecida internacionalmente como um direito humano e, no Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece o tratamento de dados de crianças e adolescentes sob o critério do melhor interesse. A pesquisa ainda ganha relevância com a chegada do Estatuto Digital da Criança e do Adolescente (Lei n. 15.211/2025). Conhecido como Estatuto da Criança e do Adolescente Digital (ECA Digital), o novo marco regulatório ampliou o arcabouço normativo aplicável às questões proteção de dados no ambiente virtual, impondo deveres técnicos às plataformas digitais (Badaró; Menino, 2025) e, com consequência, demandando a atualização urgente das práticas de governança de dados no âmbito do ensino digital.

O ECA Digital surge como resposta ao crescimento exponencial da exposição infantojuvenil em plataformas digitais (Santos, 2025), com tramitação legislativa do projeto de lei que o estabeleceu (Projeto de Lei n. 2.628/2022³) acelerada pela repercussão do vídeo do influenciador Felipe Bressanim Pereira, conhecido como Felca, que denunciou a adultização⁴ de crianças e adolescentes nas redes sociais (G1, 2025).

O risco online na infância digital é considerado um desafio urgente para a pesquisa, as políticas e a prática, implicando na necessidade de investigar como as intervenções regulatórias podem ser eficazes para a mitigação de danos (Livingstone; Stoilova, 2021). Diante disso, apresenta-se como problema de pesquisa: de que maneira a implementação do Estatuto Digital da Criança e do Adolescente (Lei n. 15.211/2025) redefine os parâmetros de governança de dados nas escolas, considerando a vulnerabilidade de crianças e adolescentes e a necessidade de proteger a proteção de dados pessoais em sistemas de ensino digital?

³ O Projeto de Lei n. 2.628/2022, de autoria do senador Alessandro Vieira (MDB-SE), tinha como objetivo de regulamentar o uso de aparelhos eletrônicos por alunos em instituições de ensino, passando a ser vinculado à proteção de crianças e adolescente contra práticas como a denunciada por Felca em reforço à visão social e jurídica de que a exploração infantil no ambiente virtual deve ser combatida com instrumentos normativos mais eficazes (Gomes; Santos, 2025).

⁴ O vídeo “Adultização” de Felca alerta que a manipulação de algoritmos nas plataformas digitais favorece a exposição excessiva de crianças e adolescentes, tornando-os vulneráveis a criminosos (Badaró; Menino, 2025). Em 6 de agosto de 2025, Felca expôs o caso do influenciador paraibano Hytalo Santos, que desde 2020 utilizava adolescentes, chamados de “filhos” e “turma do Hytalo”, em danças sensuais e situações constrangedoras no Instagram para inflar o engajamento, a monetização e o lucro (G1, 2025). A grande repercussão do vídeo de Felca motivou ações judiciais, investigações e medidas políticas imediatas, resultando na prisão de Hytalo em menos de uma semana (G1, 2025).

Como hipótese, sustenta-se que as escolas deverão manter uma governança de dados focada na prevenção para a proteção de dados de crianças e adolescentes ao utilizar sistemas de ensino digital, como plataformas de aprendizagem online e tecnologias pedagógicas.

O objetivo geral do presente trabalho é analisar os desafios e as obrigações impostas pelo Estatuto Digital da Criança e do Adolescente à governança de dados em escolas frente ao uso de sistemas de ensino digital, sob a ótica da proteção de dados como direito humano. Para o alcance do objetivo geral, estabelecem-se os seguintes objetivos específicos: a) analisar o arcabouço de proteção de dados aplicável ao ensino digital, com a LGPD e as disposições do ECA Digital e as obrigações aplicáveis para as escolas; e b) investigar os mecanismos de governança escolar necessários para a efetivação da responsabilidade das escolas e atores no ecossistema de ensino digital, adotando uma abordagem de prevenção para mitigação de riscos à proteção de dados de crianças e adolescentes.

Para enfrentar o problema a que a pesquisa se dedica, do ponto de vista metodológico, utiliza-se a pesquisa bibliográfica e documental aportada no método hipotético indutivo. O caminho teórico utiliza parte dos conceitos e critérios legais elencados na LGPD e no ECA Digital para identificar os parâmetros aplicáveis à governança de dados em escolas. A investigação também consistiu no levantamento de livros e artigos publicados em bases científicas qualificadas, com filtros orientados pelos termos “Proteção de Dados”, “Criança e adolescente”, “Governança de dados”, “Escolas” e “ECA Digital”.

O desenvolvimento do presente trabalho foi dividido em dois tópicos. Num primeiro momento, a pesquisa parte da caracterização da proteção de dados com direito humano, regulado na LGPD e complementado por obrigações que surgem com o ECA Digital para proteger crianças e adolescentes como sujeitos de direito vulneráveis no ambiente digital.

Após, o trabalho se debruça sobre as implicações na governança de dados nas escolas, considerando a necessidade de uma abordagem preventiva de *privacy by design* e de adoção de medidas técnicas e administrativas para proteção de dados no âmbito do ensino online.

2. O ECA DIGITAL E O NOVO PARADIGMA DA PROTEÇÃO DE DADOS NO ENSINO

A integração tecnológica nas escolas brasileiras não é novidade, com programas institucionais que remontam aos anos 1970⁵ (Costa Júnior et al., 2026), estratégias nacionais que reconhecem a importância da incorporação de novas tecnologias no processo educacional, como a Lei de Diretrizes e Bases da Educação Nacional (LDB), Lei n. 9.394/96 (Alves, 2025) e políticas de digitalização como a Política Nacional de Educação Digital (Costa Júnior et al., 2026).

Mas, apesar dessas iniciativas de inovação do ensino, tem-se a preocupação do ordenamento jurídico em direcionar uma tutela atenciosa às crianças e adolescentes no ambiente digital. Isso decorre do fato de serem sujeitos de direito vulneráveis (Costa; Almeida, 2023), em razão do desenvolvimento físico, emocional e psicológico ainda em formação (Gomes; Santos, 2025). Tais fragilidades se intensificam no ambiente digital, que multiplica os riscos pelo desconhecimento e ausência de autonomia para lidar com as dinâmicas tecnológicas: “[...] velocidade de disseminação dos conteúdos, monetização algorítmica e práticas que exploram a necessidade de pertencimento, curiosidade, disciplina ou reconhecimento dos jovens” (Gomes; Santos, 2025).

Para analisar o novo paradigma de proteção de dados na era do ensino digital, o presente tópico conceitua a proteção de dados pessoais como direito humano autônomo e fundamental. Define-se "dado pessoal" a partir da LGPD, expandindo o conceito para sua verificação no atual contexto escolar, bem como caracteriza-se o “titular de dados” como as crianças e adolescentes, consideradas sujeitos de direitos dotados de vulnerabilidade potencializada no ambiente digital pela falta de autonomia e assimetria de informação. Por fim, transporta a realidade do “tratamento de dados pessoais” para o ambiente educacional online, situando os casos de coleta, armazenamento e compartilhamento de dados de alunos.

Na sequência, a pesquisa caminha com a análise das ferramentas jurídicas brasileiras voltadas à governança e fiscalização desse tratamento de dados. Inicialmente, aborda a LGPD e o seu artigo 14, que exige o consentimento destacado dos responsáveis e impõe a primazia do "melhor interesse" da criança. Diante das lacunas práticas da LGPD, introduz-se a atuação da ANPD (Agência Nacional de Proteção de Dados), destacando o Enunciado n. 1/2023, a caracterização do tratamento de dados de menores como atividade de "alto risco" e seu breve histórico de fiscalização no que tange à governança de dados de crianças e adolescentes em plataformas digitais.

⁵ Destaca-se o surgimento de programas como o EDUCOM e, posteriormente, o PROUCA (Programa Um Computador por Aluno), que marcaram uma trajetória de expansão na inserção de computadores e dispositivos digitais (Costa Júnior et al., 2026).

A análise o ECA Digital é feita em dois momentos: primeiro, considera seu diálogo com outros diplomas (LGPD, Marco Civil da Internet, LDB e a Lei n. 15.100/2025 sobre celulares nas escolas) e seu escopo complementar; depois, quais são os riscos no ecossistema escolar digital que este novo marco regulatório permite enfrentar mediante suas disposições aplicáveis às escolas e fornecedores de tecnologia educacional.

2.1. A Proteção de Dados Pessoais de Crianças e Adolescentes

O avanço tecnológico trouxe consigo novas ameaças à dignidade humana, fazendo com que o debate jurídico tradicional evoluísse para o conceito de proteção de dados (Doneda, 2019), que se consolidou como conteúdo essencial dos direitos humanos, alcançando o patamar de um direito autônomo (Doneda, 2011).

A validação da proteção de dados na categoria de direito humano robustece uma tutela já assegurada pela Constituição e por tratados internacionais, o que reflete o avanço da digitalização sobre as garantias fundamentais (Sarlet, 2020). Quando esse cenário alcança crianças e adolescentes, a proteção de dados, alinhada aos preceitos do melhor interesse e da proteção integral, assume um papel central (Sarlet, 2020) diante dos desafios impostos pelas inovações tecnológicas.

No centro dessa proteção encontram-se os dados pessoais, caracterizados pela Lei Geral de Proteção de Dados Pessoais (LGPD — Lei Federal n. 13.709/2018) como qualquer informação capaz de identificar, direta ou indiretamente, um indivíduo. Essa abrangência conceitual baseia-se na premissa de que qualquer informação possui relevância e valor econômico ou social, pois tem o potencial de expor aspectos particulares de alguém (Teffé; Viola, 2020).

Assim, serão considerados dados pessoais desde os identificadores básicos, como nome, endereço ou data de nascimento, até os registros digitais mais complexos, incluindo preferências de comportamento, padrões de interação, rastreamento de localização, histórico de buscas e outros marcos sobre as atividades online. Todas essas informações tornam-se passíveis de serem analisadas, perfiladas e até monetizadas por terceiros que os acessarem (Munna, 2025). Ainda, os dados pessoais podem representar aspectos sobre identificação, localização, comunicação, emoções, saúde e relacionamentos de crianças e adolescentes (Bianchi, 2025), enquanto titulares dessas informações.

Importante situar que os titulares de dados são os indivíduos a quem os dados pessoais dizem respeito e, por serem os verdadeiros donos dessas informações, possuem direitos e

garantias na legislação de proteção de dados. Por natureza os titulares frequentemente estão e uma posição de assimetria e vulnerabilidade frente às organizações que coletam e tratam suas informações, porém quando se está diante de crianças e adolescentes é necessário considerar sua hipervulnerabilidade, uma vez que possuem a condição peculiar de pessoa em desenvolvimento (Dias da Fonseca; Torquato Rego, 2021).

Tal vulnerabilidade decorre de aspectos como: “a inexperiência, o incompleto desenvolvimento das faculdades intelectuais, a facilidade de se deixar influenciar por outrem, a falta de autodeterminação” (Dias da Fonseca; Torquato Rego, 2021) e a ausência de autonomia vinculada à presença do risco à proteção de seus dados pessoais.

Por esta razão que a proteção de dados deve caminhar com a observância do melhor interesse da criança e do adolescente para a efetivação de direitos inclusive no meio digital (Mendes; Santos, 2022) e nos novos modelos educacionais de ensino online (Dias da Fonseca; Torquato Rego, 2021), considerando a aplicação de tutela diferenciada para resguardar este grupo vulnerável.

2.2. Diálogos entre a LGPD, ANPD e o ECA Digital

Em resposta à necessidade de proteção de dados, a LGPD foi promulgada no Brasil em 2018 e trouxe regras para o tratamento de dados pessoais, inclusive no que tange aos dados de crianças e adolescentes (Mendes; Santos, 2022). Esta lei garante uma série de direitos aos titulares dos dados, além de princípios que devem reger a segurança e as boas práticas para as atividades realizadas por agentes de tratamento de dados (Thaines, 2021).

Trata-se de uma lei que também versa sobre medidas técnicas e de governança que devem passar a fazer parte da rotina dos agentes de tratamento de dados, os quais devem adotar as ferramentas, documentos e políticas para o devido cumprimento dessa legislação (Thaines, 2021).

Ao estabelecer em seu artigo 14 regras sobre o tratamento de dados pessoais de crianças e adolescentes, a LGPD destaca a obrigatoriedade na observância do seu melhor interesse (Mendes e Santos, 2022). E em razão da vulnerabilidade das crianças, o §1º do art. 14 da LGPD disciplina sobre o consentimento parental específico e destacado (Badaró; Menino, 2025). No entanto, apesar desta regra, sua aplicação revelou lacunas quanto à obrigatoriedade do consentimento como base legal e quanto à verificação do consentimento concedido pelos pais ou responsáveis legais, assim como sobre a definição do melhor interesse, revelando desafios ao ambiente online (Badaró; Menino, 2025).

No intuito de suprir as lacunas da LGPD, a Agência Nacional de Proteção de Dados (ANPD) publicou o Enunciado CD/ANPD n. 1/20233 para uniformizar a interpretação sobre bases legais aplicáveis ao tratamento de dados de crianças e adolescentes e para reafirmar a primazia do melhor interesse (Badaró; Menino, 2025).

Vale destacar que a ANPD também destacou o envolvimento de dados de crianças e adolescentes como um dos critérios específicos para tornar uma atividade de alto risco, uma vez que somado a ao menos um critério geral (Bianchi, 2025). Ou seja, plataformas de ensino online que tratam dados pessoais de crianças e de adolescentes em larga escala⁶, ou avaliações de aprendizagem automatizadas que possam afetar significativamente⁷ seus direitos fundamentais como acesso à educação poderão ser considerados tratamentos de alto risco. Se configurada a existência de alto risco à garantia dos princípios gerais de proteção de dados pessoais e às liberdades civis e aos direitos fundamentais, será necessária a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), instrumento de governança que pode auxiliar na avaliação do melhor interesse da criança e do adolescente (Bianchi, 2025).

Para além da atuação regulatória, a ANPD também tem atuado na fiscalização de serviços digitais acessados por crianças e adolescentes, com início nas investigações do TikTok nas Notas Técnicas n. 6/2023 e n. 50/2024 (ANPD, 2023; 2024), o que ganhou destaque por se tratar de uma plataforma acessada por 58% dos brasileiros entre 9 e 17 anos (ANPD, 2023). Da perspectiva de governança, a ANPD consolidou o entendimento de que a conformidade para esse público exige mecanismos de verificação etária realmente eficientes, capazes de impedir o ingresso de menores de 13 anos, uma vez que o acesso sem login compromete o controle de idade e a proteção de direitos fundamentais. Somado a isso, a agência estabeleceu que as políticas de privacidade devem ser transparentes e distinguir o tratamento de dados de crianças e adolescentes daquele realizado com adultos, rejeitando finalidades genéricas (ANPD, 2024). Ainda, em ambas as investigações a ANPD reforçou o alto risco envolvido e necessidade de elaboração de RIPD para estes casos (ANPD, 2023; 2024).

⁶ Art. 4º, I da Resolução CD/ANPD n. 2/2022: “critérios gerais: a) tratamento de dados pessoais em larga escala [...] § 1º O tratamento de dados pessoais em larga escala será caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado (ANPD, 2022)

⁷ Art. 4º, I da Resolução CD/ANPD n. 2/2022: “critérios gerais: b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares [...] § 2º O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade. (ANPD, 2022)

Em síntese, o posicionamento da ANPD demonstra a necessidade de medidas de governança rigorosas para o tratamento de dados de titulares hipervulneráveis (Bianchi, 2025), o que é relevante para sua atuação como autoridade administrativa incumbida da fiscalização do ECA Digital⁸.

O ECA Digital atende a um pedido de atualização do Estatuto da Criança e do Adolescente de 13 de julho de 1990 (ECA), em decorrência das transformações sociais e tecnológicas (Gomes; Santos, 2025), para transpor os princípios da proteção integral e prioritária para a esfera digital (Santos, 2025) e materializar a expressão do melhor interesse como a “[...] proteção de sua privacidade, segurança, saúde mental e física, acesso à informação, liberdade de participação na sociedade, acesso significativo às tecnologias digitais e bem-estar” (Brasil, 2025).

O ECA Digital dialoga com a proteção de dados preconizada na LGPD, ao prever expressamente como um de seus fundamentos “a transparência e a responsabilidade no tratamento de dados pessoais de crianças e de adolescentes” (Brasil, 2025). Da mesma maneira, também se complementa a outras normas aplicáveis ao segmento digital, como o Marco Civil da Internet (Lei 12.965/2014⁹) e, no contexto escolar, a recente Lei n. 15.100/2025, que regulamenta o uso de celulares por estudantes em instituições públicas e privadas de educação básica¹⁰ (Gomes; Santos, 2025)

Nesse sentido, o ECA Digital soma no arcabouço normativo contribuindo com uma mudança cultural frente ao tratamento de dados de crianças e adolescentes no ambiente digital, “não mais como consumidores vulneráveis a serem explorados, mas como sujeitos de direitos que exigem tratamento prioritário” (Santos, 2025). Isso porque para além da determinação das práticas necessárias, a previsão de sanções¹¹ específicas no ECA Digital e sua fiscalização pela

⁸ Em um “pacote”, a Medida Provisória n. 1.317/2025 transformou a então Autoridade Nacional de Proteção de Dados em uma agência reguladora, enquanto o Decreto n. 12.622/2025, que regulamenta o ECA Digital, designa a ANPD como autoridade administrativa autônoma de proteção de crianças e adolescentes em ambientes digitais (Badaró; Menino, 2025).

⁹ Cita-se o artigo 29 do Marco Civil da Internet, que traz sobre o controle parental, pelo qual os pais e responsáveis legais podem restringir o acesso à conteúdos que julgarem impróprios às crianças e adolescentes, sendo que as empresas provedoras desses canais digitais devem fornecer essa opção de controle parental (Mendes; Santos, 2022).

¹⁰ Esta lei foi promulgada para proteger a saúde mental, física e psíquica de crianças e adolescentes, proibindo o uso de celulares em salas de aula, recreios ou intervalos, exceto para fins pedagógicos, de acessibilidade ou em situações excepcionais como emergências ou estados de necessidade. Somada a esta lei, remonta-se ao Guia sobre Uso de Dispositivos Digitais criado pelo Governo Federal, visando orientar famílias, escolas e jovens sobre o uso seguro e saudável da internet (Gomes; Santos, 2025).

¹¹ O regime sancionatório do art. 35 do ECA Digital é progressivo e severo, prevendo multas por seu descumprimento que podem alcançar até 10% do faturamento do grupo econômico no Brasil, bem como a possibilidade de imposição de medidas de suspensão ou bloqueio de serviços digitais em caso de descumprimento

ANPD conferem instrumentos coercitivos concretos que possibilitam suprir as lacunas da LGPD (Badaró; Menino, 2025).

2.3. Os Riscos de Proteção de Dados no Ensino Digital

O ECA Digital se aplica ao contexto escolar de ensino digital na medida em que se aplica “[...] a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação” (Brasil, 2025).

Assim, plataformas de aprendizagem online, ensino à distância, gamificação do ensino ou demais tecnologias poderão ser consideradas como “produto ou serviço de tecnologia da informação”¹² para os fins desta lei, ensejando seu cumprimento tanto pela escola, na medida em que utiliza e disponibiliza aos alunos tais tecnologias, quanto aos desenvolvedores desses produtos ou serviços, como *edtechs*.

Considerando estes agentes, produtos e serviços do ambiente digital, Livingstone e Stoilova (2021) apontam para a necessidade de reconhecer os riscos e danos¹³ às crianças e adolescentes inerentes a este espaço, que muitas vezes emergem antes que os adultos saibam como mitigá-los. As autoras propõem a divisão de riscos dos “4 Cs”¹⁴: conteúdo, contato, conduta e contrato (Livingstone; Stoilova, 2021).

Os riscos de conteúdo envolvem a exposição a materiais inadequados, violentos ou prejudiciais; os riscos de contato, caracterizados por interações perigosas com adultos ou terceiros mal-intencionados; os riscos de conduta, nos quais a própria criança adota comportamentos prejudiciais, como a criação de conteúdos de ódio ou de teor sexual; e os riscos contratuais, que ocorrem quando a aceitação de termos de serviço, ou o processamento de dados

reiterado (Brasil, 2025). Tais sanções visam compatibilizar proporcionalidade e dissuasão, para que as penalidades não sejam tratadas como meros custos operacionais (Santos, 2025).

¹² Conforme art. 2º, I do ECA Digital: “I – produto ou serviço de tecnologia da informação: produto ou serviço fornecido a distância, por meio eletrônico e provido em virtude de requisição individual, tais como aplicações de internet, programas de computador, softwares, sistemas operacionais de terminais, lojas de aplicações de internet e jogos eletrônicos ou similares conectados à internet ou a outra rede de comunicações” (Brasil, 2025).

¹³ A distinção entre os conceitos de risco e dano são: “risco é a probabilidade de dano, enquanto dano inclui uma gama de consequências negativas para o bem-estar emocional, físico ou mental da criança” (Livingstone; Stoilova, 2021).

¹⁴ Livingstone e Stoilova (2021) atualizam a classificação original dos riscos online conhecida como “3Cs” da EU Kids Online, que se tornou um clássico ponto de referência desde 2010, amplamente citada por formuladores de políticas e profissionais que trabalham para maximizar as oportunidades online das crianças e minimizar os riscos de danos a elas. Na reformulação, o quarto “C” é concebido como um risco “contratual” que vincula direta ou indiretamente as crianças aos provedores digitais.

por terceiros, vincula a criança a acordos injustos, exploratórios e que violam sua segurança e proteção de dados (Livingstone; Stoilova, 2021).

Livingstone e Stoilova (2021) discorrem que a probabilidade de que um risco se materialize em um dano dependerão da concepção, regulamentação e gestão do ambiente digital, bem como de fatores sociais (como regulamentações, políticas públicas e sistemas educacionais) e fatores individuais que diferenciam as crianças e adolescentes entre si (incluindo idade, habilidades digitais, situação socioeconômica e contexto familiar).

Ademais, a origem do risco pode não decorrer diretamente de uma interação da criança com o ambiente digital, mas daquela realizada por seus pais ou escola com um fornecedor de serviços no ecossistema digital (Livingstone; Stoilova, 2021).

No Brasil, o ECA Digital mostra-se como o normativo que visa atenuar os riscos do ambiente digital para mitigar danos a crianças e adolescentes que naveguem nesse espaço, considerando especificamente em seus artigos os seguintes riscos¹⁵: ao desenvolvimento biopsicossocial, privacidade e segurança geral¹⁶; de exploração e abuso sexual¹⁷; de violência física, intimidação sistemática (*cyberbullying*) e assédio¹⁸; de indução a danos à saúde física ou mental (automutilação, suicídio e distúrbios)¹⁹; de exposição a produtos restritos e jogos de azar²⁰; de práticas publicitárias predatórias e danos financeiros²¹; de exposição a conteúdo pornográfico²²; e, por fim, riscos à privacidade e proteção de dados pessoais²³.

Em destaque a este último risco, considerando o recorte da presente pesquisa, sua materialização decorre do tratamento inadequado de dados pessoais presente no meio virtual, que inclui rastreamento e classificação automatizada de comportamentos para fins comerciais ou de vigilância, considerando ainda a prática de perfilamento²⁴ por fornecedores de tecnologias.

¹⁵ A categorização de riscos realizada nesta pesquisa reflete apenas o agrupamento didático de artigos com temas semelhantes no ECA Digital, sem representar categorias decorrentes da lei em si.

¹⁶ Art. 1º, Parágrafo único, inciso III do ECA Digital (Brasil, 2025).

¹⁷ Art. 6º, inciso I do ECA Digital (Brasil, 2025).

¹⁸ Art. 4º, inciso IV e Art. 6º, inciso II do ECA Digital (Brasil, 2025).

¹⁹ Art. 6º, inciso III do ECA Digital (Brasil, 2025).

²⁰ Art. 6º, inciso IV do ECA Digital (Brasil, 2025).

²¹ Art. 4º, inciso VI e Art. 6º, inciso V do ECA Digital (Brasil, 2025).

²² Art. 6º, inciso VI do ECA Digital (Brasil, 2025).

²³ Art. 4º, inciso IX e Art. 7º, § 2º do ECA Digital (Brasil, 2025).

²⁴ Art. 2º, inciso V do ECA Digital define perfilamento como “qualquer forma de tratamento de dados pessoais, automatizada ou não, para avaliar certos aspectos de uma pessoa natural, com o objetivo de classificá-la em grupo ou perfil de modo a fazer inferências sobre seu comportamento, situação econômica, saúde, preferências pessoais, interesses, desejos de consumo, localização geográfica, deslocamentos, posições políticas ou outras características assemelhadas” (Brasil, 2025).

Este risco denota especial atenção para o ensino digital ao debruçar suas atividades em plataformas que atuam principalmente como intermediárias de acesso e oportunidade, orientadas à coleta de dados e processamento algorítmico (Oliveira; Horta, 2026). As plataformas educacionais representam um ator de destaque no relacionamento com as escolas, na medida em que permitem modelar e vigiar comportamentos de alunos e impactar sua educação a partir de dados sobre padrões de interações para predições, avaliações e direcionamento do aprendizado, colocando o aluno como objeto de dados (Costa Júnior et al., 2026), ao invés de reconhecê-lo como “titular” de dados e sujeito de direitos.

Diante desse cenário, o caminho para mitigação de riscos à proteção de dados de crianças e adolescentes na era do ensino digital em cumprimento efetivo da LGPD e do ECA Digital passa pela necessidade da estruturação de práticas protetivas nas escolas.

3. GOVERNANÇA DE DADOS PARA ESCOLAS E O ENSINO DIGITAL

Primeiramente, define-se “governança de dados” como o conjunto de processos e responsabilidades que garante a gestão formal de informações em determinado setor (Cristóvam; Bergamini; Hahn, 2021).

O ecossistema de ensino digital gera a necessidade de proteção de crianças e adolescentes perante diferentes responsáveis, de forma conjunta, abarcando as plataformas globais, as startups nacionais, o Estado enquanto fomentador de inovação tecnológica e enquanto ente regulador, bem como escolas (públicas e privadas) e famílias (Santos, 2025). Considerando o recorte dessa pesquisa, os direcionamentos para governança de dados terão enfoque nas escolas.

A LGPD já foi um marco relevante para guiar a governança de dados pelos agentes de tratamento, estabelecendo a necessidade de identificar e mapear os dados pessoais tratados em cada parte da organização para cumprir a obrigação de registro das atividades de tratamento prevista no art. 37²⁵ desta lei. Da mesma forma, endereça como boa prática a estruturação de um programa de governança para o cumprimento das obrigações da LGPD nos termos do seu art. 50²⁶. Assim, não é novidade para as escolas o tema de governança de dados, já que é um tema atrelado ao cumprimento de uma lei publicada em 2018.

²⁵ Art. 37 da LGPD. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (Brasil, 2018).

²⁶ Art. 50 da LGPD. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo

Destaca-se que a LGPD não pretende fixar um modelo único para a governança de dados, reconhecendo a necessidade de adequá-lo conforme a estrutura, a escala e o volume das operações realizadas, a natureza dos dados pessoais tratados e os riscos para os titulares dos dados²⁷. Como cada escola possui seu contexto particular (pública ou privada; localidade, maior ou menor investimento e acessibilidade à tecnologia, dentre outros aspectos), é natural que haja variação na robustez e eficiência da sua governança de dados.

De toda forma, com a chegada do ECA Digital, escolas se verão diante da necessidade confrontar suas práticas (ou ausências) de governança de dados para acomodar o cumprimento às obrigações conforme sua participação na era do ensino digital. Assim, este tópico visa demonstrar diretrizes para a proteção de dados a partir da governança, sem pretensão de criar um modelo universal.

A seguir, são analisados os novos requisitos legais do ECA Digital para uma governança que proteja o estudante contra os riscos do tratamento indevido de dados pessoais no ambiente digital de ensino. Num primeiro momento, foca-se na necessidade de uma postura proativa e estrutural de gestão de riscos de proteção de dados no ambiente escolar, impulsionada pelas novas diretrizes do ECA Digital. Nesse tema, aborda-se a ideia de *Privacy by Design* como exigência técnica e legal de incorporar a privacidade e medidas de proteção de dados dos alunos desde a fase de concepção e planejamento de qualquer tecnologia ou projeto de ensino digital.

Na sequência, a pesquisa traduz os princípios preventivos em ações práticas e operacionais no dia a dia da governança de dados escolar, superando a abstração das normas legais mediante a adoção de medidas: (i) técnicas, incluindo ferramentas de segurança; (ii) de gestão de terceiros, com a fiscalização ativa sobre fornecedores de tecnologias (*edtechs*), plataformas e algoritmos de *learning analytics*; e (iii) administrativas, com foco no fator humano e institucional para criação de processos coesos e para preencher as lacunas de conscientização de gestores e professores, transformando a cultura de proteção de dados da instituição e a efetivação de direitos humanos de alunos.

3.1. Prevenção de Risco e a Abordagem de *Privacy by Design*

reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (Brasil, 2018).

²⁷ Art. 50, §2º da LGPD (Brasil, 2018).

Como visto, o ECA Digital se propõe a endereçar os riscos para crianças e adolescentes no ambiente digital e para tanto concentra suas obrigações em uma estrutura de prevenção de risco (Oliveira; Horta, 2026).

Com isso, esta lei estabelece em diversos dispositivos²⁸ sobre a necessidade de adotar medidas desde a concepção de produtos e serviços digitais direcionados ou de acesso provável por crianças e adolescentes, bem como ao longo da operação, a fim de prevenir e mitigar eventuais danos a este público (Oliveira; Horta, 2026).

A abordagem preventiva para lidar com riscos digitais a crianças e adolescentes encontra respaldo em iniciativas internacionais, que não se limita a reagir a violações, mas almeja a redução de riscos sistêmicos antecipadamente (Santos, 2025).

No que tange à proteção de dados, esta abordagem preventiva coaduna com o previsto na LGPD sobre o princípio da prevenção²⁹ e à necessidade de que agentes de tratamento adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais desde a fase de concepção de produtos ou serviços até a sua execução³⁰.

Trata-se da implementação de uma metodologia de princípios criada por Cavoukian³¹ (2010) conhecida como “*Privacy by Design*” ou privacidade desde a concepção. O objetivo dessa proposta é a proteção de dados e a privacidade desde as fases iniciais de planejamento de uma tecnologia, ao invés de adotar medidas nesse sentido apenas ao final ou após o sistema já estar em operação (Munna, 2025).

²⁸ Art. 6º do ECA Digital: Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão tomar medidas razoáveis desde a concepção e ao longo da operação de suas aplicações, com o objetivo de prevenir e mitigar riscos [...]. (Brasil, 2025).

Art. 7º do ECA Digital: Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão, desde a concepção de seus produtos e serviços, garantir, por padrão, a configuração no modelo mais protetivo disponível em relação à privacidade e à proteção de dados pessoais, considerados a autonomia e o desenvolvimento progressivo do indivíduo e justificado o melhor interesse da criança e do adolescente. (Brasil, 2025).

Art. 8º do ECA Digital: Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão: [...] IV – desenvolver desde a concepção e adotar por padrão configurações que evitem o uso compulsivo de produtos ou serviços por crianças e adolescentes [...] (Brasil, 2025).

²⁹ Art. 6º, VIII da LGPD estabelece como princípio da prevenção a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (Brasil, 2018).

³⁰ Art. 46, caput e §2º da LGPD (Brasil, 2018).

³¹ Os sete princípios fundamentais do *Privacy by Design* delineados na metodologia de Cavoukian (2010) são: (1) uma abordagem proativa em vez de reativa; (2) a aplicação da privacidade como configuração padrão; (3) a integração da proteção da privacidade no design do sistema desde o início; (4) a garantia de funcionalidade total sem comprometer a proteção de dados; (5) a aplicação de segurança abrangente de ponta a ponta; (6) a aplicação de visibilidade e transparência na gestão de dados; e (7) o respeito consistente pelos direitos de privacidade de cada usuário.

É importante reconhecer que o ECA Digital torna expresso, assim como o faz a LGPD, o que antes no ECA de 1990 era apenas interpretativo³² (Oliveira; Horta, 2026). Com isso, a implementação de medidas para prevenção de dados torna-se mais evidente e com isso exigível e passível de uma fiscalização mais efetiva.

Para as escolas, a prevenção de riscos digitais de proteção de dados pode ser compreendida como um eixo pedagógico, para além de uma abordagem reativa e de ações pontuais. Esta abordagem deve ser refletida em decisões administrativas e culturais ao lidar com tecnologias no ensino digital (Ramos et al., 2025).

3.2. Novas Diretrizes para Governança de Dados Escolares

Como ficou claro, o tratamento de dados pessoais de crianças e adolescentes é uma realidade incontestável para as escolas, que utilizam esses dados para diversos fins acadêmicos e não acadêmicos (Munna, 2025).

Uma boa gestão de dados é o que permite o cumprimento de normas como a LGPD e o ECA Digital. Assim, a governança de dados é o caminho para que cada atividade de tratamento de dados pessoais dos alunos na era do ensino digital seja projetada para cumprir com as melhores práticas de proteção de dados pessoais (Munna, 2025).

É certo que o desequilíbrio entre o peso das regulamentações e as dificuldades na implementação das práticas escolares afeta a efetividade na proteção de dados dos alunos, já que as leis costumam ser abstratas e não direcionam orientações direcionadas claramente ao contexto escolar (Munna, 2025). De toda forma, propõem-se neste tópico da pesquisa o direcionamento de ações para governança de dados, a partir do novo paradigma aportado com o ECA Digital e sua postura preventiva.

Inicia-se pelas medidas técnicas que fazem parte da governança de dados escolar. Isso porque a ausência de critérios para o uso de dispositivos e de redes Wi-Fi, a falta de mecanismos para controle e registro de acesso às plataformas de ensino digital, e de modo geral a ausência de mecanismos de segurança já representa práticas inseguras frente aos dados coletados e armazenados pelas escolas (Ramos et al., 2025).

³² Segundo Oliveira e Horta (2026) a ideia de proteção desde a concepção já era interpretada do art. 71 do ECA de 1990, ao prever “o direito a produtos e serviços que respeitem sua condição peculiar de pessoas em desenvolvimento”. Ainda, as autoras apontam essa leitura para o ambiente digital com o art. 3º, inciso X da Resolução nº 245/2024 do Conanda, inspirada no Comentário Geral nº 25 do Comitê da ONU, considerando o princípio sobre a “garantia dos direitos das crianças e adolescentes por *design* dos produtos e serviços em ambientes digitais” (Oliveira; Horta, 2026).

Ao implementar mecanismos técnicos consistentes de segurança, as escolas se alinham às melhores práticas e conseguem implementar as medidas de segurança relevantes para cumprimento da LGPD e ECA Digital, como a criptografia de dados de ponta a ponta, autenticação de múltiplos fatores (MFA), controle de acesso baseado em funções, backups regulares de dados com armazenamento segregado e o uso de servidores protegidos por firewalls (Munna, 2025).

No entanto, frequentemente escolas confiam seus sistemas e plataformas de ensino às tecnologias de terceiros, sejam *edtechs* especializados em educação, como Ambientes Virtuais de Aprendizagem (AVA) e sistemas de *learning analytics* (Costa Júnior et al., 2026), ou fornecedores da infraestrutura para que as escolas operem no ambiente digital, como desenvolvedores de salas de reunião à distância, repositórios de documentos em nuvem, dentre outros.

Assim, é responsabilidade das escolas avaliar o cumprimento de requisitos legais pelos terceiros que engajarem no âmbito do ensino digital, apesar da complexidade e o desequilíbrio de poder informacional sobre as práticas de tratamento de dados que dificultam que as escolas verifiquem como esses dados são gerenciados por tais fornecedores (Munna, 2025).

Por exemplo, o ECA Digital exige a adoção de mecanismos de supervisão parental³³, por meio de configurações e ferramentas acessíveis e adotando o mais alto nível de proteção disponível³⁴, constituindo requisito técnico que deve ser embutido na tecnologia de ensino

³³ Art. 3º VIII do ECA Digital: mecanismo de supervisão parental: conjunto de configurações, de ferramentas e de salvaguardas tecnológicas integradas a produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles que possibilitem aos pais ou responsáveis legais supervisionar, limitar e gerenciar o uso do serviço, o conteúdo acessado e o tratamento de dados pessoais realizado (Brasil, 2025)

³⁴ Art. 16, §4º do ECA Digital: § 4º As configurações-padrão das ferramentas de supervisão parental deverão adotar o mais alto nível de proteção disponível, assegurados, no mínimo: I – restrição à comunicação com crianças e adolescentes por usuários não autorizados; II – limitação de recursos para aumentar, sustentar ou estender artificialmente o uso do produto ou serviço pela criança ou pelo adolescente, como reprodução automática de mídia, recompensas pelo tempo de uso, notificações e outros recursos que possam resultar em uso excessivo do produto ou serviço por criança ou adolescente; III – oferta de ferramentas para acompanhamento do uso adequado e saudável do produto ou serviço; IV – emprego de interfaces que permitam a imediata visualização e limitação do tempo de uso do produto ou serviço; V – controle sobre sistemas de recomendação personalizados, inclusive com opção de desativação; VI – restrição ao compartilhamento da geolocalização e fornecimento de aviso prévio e claro sobre seu rastreamento; VII – promoção da educação digital midiática quanto ao uso seguro de produtos ou serviços de tecnologia da informação; VIII – revisão regular das ferramentas de inteligência artificial, com participação de especialistas e órgãos competentes, com base em critérios técnicos que assegurem sua segurança e adequação ao uso por crianças e adolescentes, garantida a possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas; IX – disponibilização, sempre que tecnicamente viável, de recursos ou de conexões a serviços de suporte emocional e de bem-estar, com conteúdo adequado à faixa etária e orientações baseadas em evidências, especialmente nos casos de interações com riscos psicossociais identificados. (Brasil, 2025)

digital. Assim, caberá às escolas verificar e exigir dos fornecedores desses serviços digitais para cumprimento da legislação.

No mais, em caso de plataformas ou tecnologias que envolvem alguma forma de monitoramento infantil³⁵ (frequentemente adotadas no âmbito de ensino online ou difusão de imagens por câmeras de segurança), requer-se a adição de mecanismos para assegurar a inviolabilidade dos dados captados, armazenados e transmitidos, bem como de comunicação clara sobre o monitoramento³⁶.

Por fim, como serviços de ensino digital são direcionados a crianças e a adolescentes, o ECA Digital estabelece a obrigação de adotar mecanismos para proporcionar experiências adequadas à idade, implicando a necessidade de adoção de mecanismos de aferição de idade apropriados à tecnologia e ao contexto de aplicação³⁷.

A verificação de todos esses mecanismos exigidos pelo ECA Digital perante os fornecedores de tecnologias é, portanto, um elemento técnico fundamental para a governança de dados de escolas.

A governança de dados também demanda adoção de medidas administrativas e organizacionais, como políticas e procedimentos claros para proteção de dados, bem como capacitação institucional para professores e pessoas atuantes na gestão de dados (Munna, 2025). Isso porque os riscos digitais não estão relacionados apenas à falta de infraestrutura, sendo que muitas vezes a ausência de repertório crítico sobre proteção de dados é a porta de entrada para ameaças (Teixeira et al., 2025).

As políticas devem ser mais do que um conjunto de regras abstratas, mas direcionamentos aplicados aos processos de cada escola no uso das tecnologias e protocolos claros para lidar com situações de violações de proteção de dados (Ramos et al., 2025).

Trata-se, portanto, de um conjunto de ações orientadas ao estabelecimento da cultura digital e da postura preventiva exigida pelo ECA Digital para responsabilidade e a efetivação da proteção de dados de alunos, viabilizados por uma governança de dados robusta.

4. CONCLUSÃO

³⁵ Art. 3º II do ECA Digital: produto ou serviço de monitoramento infantil: produto ou serviço de tecnologia da informação destinado ao acompanhamento, por pais ou responsáveis legais, das ações executadas por crianças e adolescentes em ambientes digitais, a partir do registro ou da transmissão de imagens, de sons, de informações de localização, de atividade ou de outros dados (Brasil, 2025).

³⁶ Art. 19 caput e §1º do ECA Digital (Brasil, 2025).

³⁷ Art. 10 do ECA Digital (Brasil, 2025).

O panorama analisado permite confirmar a hipótese que orientou esta pesquisa, evidenciando que a complexidade do ecossistema de ensino digital impõe às escolas a necessidade de estruturar uma governança de dados focada na prevenção e proteção de dados pessoais, à luz do ECA Digital e da LGPD.

A transição do ambiente escolar tradicional para plataformas de aprendizagem online e o uso de tecnologias pedagógicas demonstraram que o desenvolvimento educacional não pode ocorrer em detrimento dos direitos fundamentais dos estudantes. Desse modo, os resultados obtidos ratificam que apenas uma postura preventiva, materializada por meio de um programa de governança robusto, é capaz de resguardar crianças e adolescentes, enquanto titulares de dados hipervulneráveis, contra os riscos digitais que afetam a proteção de dados.

Nesse cenário, a promulgação do ECA Digital revela-se como um marco regulatório que redefine as obrigações e os parâmetros de gestão da informação no ambiente escolar. Ao estabelecer deveres claros voltados aos serviços digitais, o novo diploma funciona como um poderoso instrumento coercitivo e protetivo que visa mitigar os danos a esse público vulnerável, elevando os mecanismos para proteção de dados.

Por fim, a efetivação dessas medidas no cotidiano educacional exige que as escolas adotem uma governança de dados capaz de aliar medidas técnicas e administrativas desde a concepção, sob a ótica da abordagem do *privacy by design*, ao mesmo tempo em que exercem uma fiscalização ativa sobre fornecedores e *edtechs* quanto ao cumprimento de requisitos legais como supervisão parental e verificação etária.

Assim, a governança de dados mostra-se como recurso chave para consolidar uma cultura institucional preventiva, assegurando que a inovação pedagógica caminhe lado a lado com a proteção de dados pessoais de crianças e adolescentes na era do ensino digital.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Nota Técnica n. 6/2023/CGF/ANPD**. 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/tiktok-nota_tecnica_6-versao_publica_ret-1.pdf Acesso em 14 mai. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD n. 2**, de 27 de janeiro de 2022. Brasília, DF. 2022. Disponível em: https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022 Acesso em: 14 mai. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Nota Técnica n. 50/2024/FIS/CGF/ANPD**. 2024. Disponível em: https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022

27-de-janeiro-de-2022 Acesso em: 14 mai. 2026.

ALVES, W. dos S. Vantagens, benefícios e riscos do ambiente digital para a educação. **Caderno Pedagógico**, [S. l.], v. 22, n. 7, p. e16367, 2025. DOI: 10.54033/cadpedv22n7-175. Disponível em: <https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/16367>. Acesso em: 1 maio. 2026.

BADARÓ, R. .; MENINO, J. . A semente da lei: a jurisprudência do STJ e a proteção da criança e do adolescente na gênese do ECA digita. **Revista de Direito da ADVOCEF**, [S. l.], v. 21, n. 40, p. 127–148, 2025. Disponível em: <https://revista.advocef.org.br/index.php/ra/article/view/514>. Acesso em: 1 maio. 2026.

BIANCHI, H. D. P. L.. Tratamento de dados de crianças e adolescentes no ambiente digital: abordagens para a garantia de direitos. In: Alessandra Borelli; Renato Opice Blum; Jayme Domingues. (Org.). **Privacidade e Direito Digital: ética, inovação e o futuro dos negócios**. 1ed.São Paulo: Editora JusPodivm, 2025, v. , p. 187-204.

BRASIL. **Lei n. 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm Acesso em: 16 mai. 2026.

BRASIL. **Lei n. 15.211**, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/115211.htm. Acesso em: 16 mai. 2026.

CAVOUKIAN, A. Privacy by design: the definitive workshop. **Identity in the Information Society**, [s. l.], v. 3, n. 2, p. 247–251, 2010. Disponível em: <https://doi.org/10.1007/s12394-010-0062-y>. Acesso em: 3 maio 2026.

COSTA JÚNIOR, J. F.; LUZ, A. M.; FERREIRA, M. E.; GODINHO, C. E. R.; SIMAS, S. S.; OLIVEIRA, L. C. F. de; SANTOS, C. F. dos; PEREIRA, E. A.; SANTOS, P. F. dos; HOLANDA, M. J. F. dos S. Risco digital: como a tecnologia pode sabotar o desenvolvimento escolar. *Revista edUCA - Revista Multidisciplinar da Faculdade Católica Paulista*, [S. l.], v. 9, p. e211, 2026. DOI: 10.54901/educa.v9-211. Disponível em: <https://www.revistaeduca.com.br/index.php/EDUCA/article/view/211>. Acesso em: 1 maio. 2026..

CRISTÓVAM, J. S. da S.; BERGAMINI, J. C. L.; HAHN, T. M.. Governança de dados no setor público brasileiro: uma análise a partir da Lei Geral de Proteção de Dados (LGPD). **Interesse Público**, Belo Horizonte, ano 23, n. 129, p. 75-101, set./out. 2021. Disponível em: <https://bd.tjmg.jus.br/items/6cafdfe9-8d7b-4e39-a2e9-c3942c2ac0b7/full> Acesso em: 16 mai. 2026.

DIAS DA FONSECA, I.; TORQUATO REGO, M. B. A proteção de dados pessoais das crianças e adolescentes no âmbito da educação online. **Revista FIDES**, [S. l.], v. 11, n. 2, p. 469–488, 2021. Disponível em: <https://revistafides.ufrn.br/index.php/br/article/view/518>.

Acesso em: 3 maio. 2026.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, ISSN-e 2179-7943, ISSN 1519-5899, Vol. 12, Nº. 2, 2011, págs. 91-108. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=4555153> Acesso em: 14 jan. 2026.

DONEDA, D. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters: Revista dos Tribunais, 2019. 432 p.

GOMES, F. C. de A.; SANTOS, C. S.. A atualização do ECA frente à proteção de crianças e adolescentes no ambiente digital. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 11, n. 11, p. 5463–5475, 2025. DOI: 10.51891/rease.v11i11.22294. Disponível em: <https://periodicorease.pro.br/rease/article/view/22294>. Acesso em: 1 maio. 2026.

G1. **Felca, Hytalo e 'adultização'**: como caso foi de vídeo viral a projeto de lei e prisão em 10 dias; entenda passo a passo. 16 ago. 2025. Disponível em: <https://g1.globo.com/politica/noticia/2025/08/16/felca-hytalo-e-adultizacao-como-caso-foi-de-video-viral-a-projeto-de-lei-e-prisao-em-10-dias-entenda-passo-a-passo.ghtml>. Acesso em: 14 maio 2026.

LIVINGSTONE, S.; STOILOVA, M.. The 4Cs: Classifying Online Risk to Children. Hamburg: Leibniz-Institut für Medienforschung; Hans-Bredow-Institut (HBI); **CO:RE - Children Online: Research and Evidence**. 2021. Disponível em: <https://www.ssoar.info/ssoar/handle/document/71817>. Acesso em: 1 maio. 2026.

MENDES, D. S. T.; SANTOS, I. B. M.. Abandono digital e tratamento de dados pessoais de crianças e adolescentes: novas perspectivas a partir da LGPD e do direito de família. **Revista Brasileira de Direito de Família e Sucessões**, v. 8, n. 3, 2022. Disponível em: <https://indexlaw.org/index.php/direitofamilia/article/view/8766>. Acesso em: 1 maio. 2026.

MUNNA, N. N.. Legal construction of child and adolescent privacy protection in the digital age: the dilemma between cyber protection and information access in schools. **Law and Judicial Review**, [s. l.], v. 1, n. 2, p. 109-126, 2025. Disponível em: <https://generatedp.com/index.php/ljr/article/view/100/95>. Acesso em: 3 maio 2026.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil**: TIC Kids Online Brasil 2025. São Paulo: Comitê Gestor da Internet no Brasil, 2026. 1 recurso online (PDF). ISBN 978-65-6165-007-6. Disponível em: <https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2025/>. Acesso em: 14 maio 2026.

OLIVEIRA, L. de M.; HORTA, N.. Algoritmos e direitos: o ECA Digital frente à dependência tecnológica. **RECIIS**, [S. l.], v. 20, p. 1–10, 2026. DOI: 10.29397/reciis.v20.5603. Disponível em: <https://www.reciiis.iciet.fiocruz.br/index.php/reciis/article/view/5603>. Acesso em: 1 maio. 2026.

RAMOS, S. B.; et. al.. Segurança digital no ambiente escolar entre formação e prevenção. **Revista Educação e Linguagem RedLi**, [S. l.], v. 12, n. 1, p. e34, 2025. DOI: 10.23900/redli.v12n1-008. Disponível em: <https://www.cienciaesociedade.com/index.php/redli/article/view/34>. Acesso em: 1 maio. 2026

SANTOS, P. P. R.. Estatuto digital da criança e do adolescente: desafios regulatórios e de fiscalização. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 11, n. 10, p. 427–441, 2025. DOI: 10.51891/rease.v11i10.20972. Disponível em: <https://periodicorease.pro.br/rease/article/view/20972>. Acesso em: 1 maio. 2026

SARLET, I. W.. Proteção De Dados Pessoais Como Direito Fundamental Na Constituição Federal Brasileira De 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 14, n. 42, p. 179–218, 2020. DOI: 10.30899/dfj.v14i42.875. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/875> Acesso em: 14 mai. 2026.

TEFFÉ, C. S. de; VIOLA, M.. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Rev. civilistica.com**. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510> Acesso em: 14 mai. 2026.

TEIXEIRA, M. L. L. D.; et. al. Cidadania digital na escola diante dos riscos e responsabilidades no uso da tecnologia. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 11, n. 7, p. 2064–2071, 2025. DOI: 10.51891/rease.v11i7.20413. Disponível em: <https://periodicorease.pro.br/rease/article/view/20413>. Acesso em: 1 maio. 2026

THAINES, Aleteia Hummes. Proteção de Dados Pessoais. In: GRIEBELER, Marcos Paulo Dhein. (Org.). **Dicionário de desenvolvimento regional e temas correlatos**. 2ed. Uruguaiana: Conceito, 2021, v. 1, p. 741-742. Disponível em: <https://observadr.org.br/wp-content/uploads/2021/09/e-Book-2021-Dicionário-Português.pdf> Acesso em: 14 mai. 2026.

THAINES, Aleteia Hummes; WELTER, Tatiéle. A necessidade de se estabelecer uma governança em inteligência artificial visando a mitigação das discriminações algorítmicas e a concretização dos direitos fundamentais, em especial, do direito à proteção de dados pessoais. In: V Seminário Internacional em Direitos e Sociedade, 2023, Criciúma. **Anais do Seminário Internacional em Direitos e Sociedade**. Criciúma: Editora Unesc, 2023. v. 5. p. 1-5. Disponível em: <https://www.periodicos.unesc.net/ojs/index.php/AnaisDirH/article/view/8729/6915> Acesso em: 14 mai. 2026.