

**DIRETRIZES REGULATÓRIAS
PARA O USO DE
INTELIGÊNCIA ARTIFICIAL
EM INSTITUIÇÕES DE
ENSINO A DISTÂNCIA NO
BRASIL: UM FRAMEWORK
DE COMPLIANCE
INSTITUCIONAL E
SEGURANÇA DA
INFORMAÇÃO**

**REGULATORY GUIDELINES FOR THE USE OF ARTIFICIAL INTELLIGENCE IN
DISTANCE EDUCATION INSTITUTIONS IN BRAZIL: AN INSTITUTIONAL
COMPLIANCE AND INFORMATION SECURITY FRAMEWORK**

Ciências Exatas e da Terra, Ciências Sociais Aplicadas • 11/09/2026

REGISTRO DOI: [10.70773/revistatopicos/789072610](https://doi.org/10.70773/revistatopicos/789072610)

Paulo Rodrigues de Oliveira¹

Samylla de Moura Feitosa²

Roseane Maria Campelo dos Santos³

Maria Viviane de Araújo Sousa⁴

Raí Araújo de Miranda⁵

RESUMO

A rápida adoção de sistemas de Inteligência Artificial (IA) nas Instituições de Ensino Superior (IES) que ofertam Educação a Distância (EaD) no Brasil tem gerado um hiato entre o avanço tecnológico e a segurança jurídica. Este artigo investiga o vácuo normativo atual e propõe um *framework* de governança focado na proteção de dados discentes, na segurança da informação corporativa e na garantia da propriedade intelectual. Por meio de pesquisa documental e bibliográfica com abordagem qualitativa, analisou-se a intersecção entre a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet, a Lei de Direitos Autorais e a jurisprudência do Supremo Tribunal Federal (STF), notadamente a ADI 6387. Os resultados indicam que a ausência de um Marco Legal da IA federal sancionado obriga as IES e polos da administração pública a adotarem diretrizes de *soft law* interno. O estudo propõe um modelo materializado na implantação de trilhas de auditoria, segregação de dados via servidores locais, certificação notarial digital de autoria e transparência algorítmica em licitações educacionais. Conclui-se que o *compliance* educacional estruturado é o mecanismo decisivo para mitigar riscos de responsabilização civil e assegurar a integridade acadêmica nos ecossistemas digitais.

Palavras-chave: Inteligência Artificial; Governança de Dados; Segurança da Informação; Compliance Educacional; Direito Digital.

ABSTRACT

The rapid adoption of Artificial Intelligence (AI) systems in Higher Education Institutions (HEIs) offering Distance Education (DE) in Brazil has created a gap between technological advancement and legal security. This article investigates the current normative vacuum and proposes a governance framework focused on student data protection, corporate information security, and intellectual property

assurance. Through documentary and bibliographic research with a qualitative approach, the intersection between the General Data Protection Law (LGPD), the Civil Rights Framework for the Internet, the Copyright Law, and the jurisprudence of the Supreme Federal Court (STF), notably ADI 6387, was analyzed. The results indicate that the absence of a sanctioned federal AI Legal Framework obliges HEIs and public administration centers to adopt internal soft law guidelines. The study proposes a model materialized in the implementation of audit trails, data segregation via local servers, digital notarial authorship certification, and algorithmic transparency in educational public bidding. It is concluded that structured educational compliance is the decisive mechanism to mitigate civil liability risks and ensure academic integrity in digital ecosystems.

Keywords: Artificial Intelligence; Data Governance; Information Security; Educational Compliance; Digital Law.

1. INTRODUÇÃO

A arquitetura contemporânea da Educação a Distância (EaD) no Brasil atravessa um ponto de inflexão crítico. O que outrora se configurava como um repositório assíncrono de conteúdos mediados por Ambientes Virtuais de Aprendizagem (AVA), transformou-se em um ecossistema complexo operado por sistemas de Inteligência Artificial (IA). A inserção de algoritmos de *Machine Learning* e Inteligência Artificial Generativa transferiu o protagonismo tecnológico da mera mediação para a automação de processos acadêmicos decisivos, incluindo a curadoria preditiva de materiais, a avaliação automatizada de desempenho, o rastreamento comportamental de usuários e a gestão de evasão discente.

Contudo, essa hiperautomação expõe as Instituições de Ensino Superior (IES), bem como os polos de apoio mantidos pela administração pública municipal e estadual, a vulnerabilidades operacionais e jurídicas sem precedentes. O problema central que orienta esta pesquisa científica formula-se na seguinte questão: Como as instituições provedoras de ensino a distância no Brasil podem estruturar diretrizes regulatórias internas capazes de garantir a segurança jurídica, a integridade da infraestrutura de rede e a proteção incondicional de dados discentes, diante da ausência de uma legislação federal consolidada e específica sobre IA?

O objetivo geral deste estudo é propor um *framework* prático e rigoroso de diretrizes regulatórias institucionais que embase a formulação de políticas de *compliance* educacional. Para atingir tal escopo, definiram-se os seguintes objetivos específicos: a) mapear o arcabouço normativo brasileiro (LGPD, Marco Civil da Internet e Lei de Direitos Autorais) aplicável tangencialmente ao uso de IA no EaD; b) identificar as vulnerabilidades técnico-jurídicas no tratamento massivo de dados acadêmicos; e c) estruturar um modelo de governança tecnológica que harmonize as inovações pedagógicas com as garantias constitucionais vigentes.

A justificativa para o desenvolvimento desta pesquisa assenta-se na necessidade de promover uma ruptura na abordagem predominante da literatura educacional recente. Observa-se que grande parte das publicações sobre IA na educação concentra-se, quase de maneira uníssona, em impactos estritamente metodológicos — debatendo exaustivamente a personalização do ensino versus a perda do pensamento crítico, ou a eficiência da tutoria virtual versus as facilidades do plágio discente (GIRAFFA; KOHLS-SANTOS, 2023; SILVA et al., 2024). Em contrapartida, há uma

escassez crítica de investigações voltadas à camada de infraestrutura, à segurança da informação corporativa e à responsabilidade civil objetiva das instituições.

O ineditismo deste artigo, portanto, reside na superação do debate puramente pedagógico, elevando a discussão para o campo do Direito Educacional, do Direito Administrativo e da arquitetura de Tecnologias da Informação (TI).

2. FUNDAMENTAÇÃO TEÓRICA E ANÁLISE JURISPRUDENCIAL

A construção de um modelo de *compliance* para o uso de IA em AVAs exige a compreensão profunda das normativas vigentes e de como os tribunais superiores brasileiros interpretam os conflitos oriundos do processamento de dados.

2.1. A LGPD, a Autodeterminação Informativa e a Jurisprudência do STF

A operacionalização de algoritmos analíticos em plataformas de EaD (o paradigma do *Learning Analytics*) fundamenta-se invariavelmente na extração, cruzamento e armazenamento contínuo de dados pessoais dos estudantes. No ordenamento brasileiro, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD) estabelece os contornos mandatórios para esta prática. A lei impõe que o tratamento de dados pessoais seja ancorado em finalidades legítimas, específicas e informadas de forma explícita ao titular (art. 6º, I e VI). Além disso, a LGPD garante ao usuário, em seu art. 20, o direito fundamental de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem seus interesses, como perfis acadêmicos e avaliações de desempenho.

Para a estruturação de um *compliance* educacional robusto, a análise textual da lei deve ser imperativamente suplementada pela interpretação da Suprema Corte. O Supremo Tribunal Federal (STF), no julgamento paradigmático da Ação Direta de Inconstitucionalidade (ADI) nº 6387, de relatoria da Ministra Rosa Weber, reconheceu de maneira incontestada que a proteção de dados pessoais constitui um direito fundamental autônomo. O acórdão consagrou o princípio da "autodeterminação informativa", que protege o indivíduo contra a instrumentalização e o monitoramento opaco, seja por entidades estatais ou corporações privadas.

Este entendimento jurisprudencial fidedigno (que posteriormente impulsionou a promulgação da Emenda Constitucional nº 115/2022) possui implicações diretas e severas para as IES. A coleta de dados discentes por meio de rastreamento de cliques, tempo de tela, reconhecimento facial em avaliações síncronas (*proctoring*) e análise de sentimentos em fóruns não pode operar sob cláusulas de consentimento genéricas camufladas em Termos de Uso extensos. A ausência de transparência algorítmica configura ofensa a preceitos constitucionais, sujeitando a instituição educacional a ações civis públicas e sanções proibitivas.

2.2. O Marco Civil da Internet e a Guarda de Registros

De forma complementar à LGPD, os Ambientes Virtuais de Aprendizagem são qualificados juridicamente como aplicações de internet, submetendo-se ao Marco Civil da Internet (Lei nº 12.965/2014). O diploma legal estabelece, em seu artigo 15, obrigações estritas sobre a guarda de registros de acesso a aplicações.

Quando uma IES licencia e integra uma IA terceirizada (como APIs de Modelos de Linguagem de Grande Escala - LLMs) ao seu AVA, há o compartilhamento sistêmico de trilhas de navegação. O Marco Civil impõe que a instituição provedora do ambiente assegure que esses registros sejam mantidos em sigilo, em ambiente controlado, e não sejam desviados para o treinamento de redes neurais comerciais de terceiros sem a anuência granular e específica do estudante. Essa exigência legal converte a gestão de infraestrutura de TI em uma peça central de defesa jurídica.

2.3. Direitos Autorais e a Complexidade da Autoria Híbrida

O terceiro eixo de vulnerabilidade regulatória reside na propriedade intelectual e nos direitos autorais da produção acadêmica automatizada. A Lei de Direitos Autorais brasileira (Lei nº 9.610/98) adota uma postura antropocêntrica rigorosa, delimitando em seu artigo 11 que "autor é a pessoa física criadora de obra literária, artística ou científica".

Com a adoção maciça da IA generativa por professores, conteudistas e instrutores técnicos para a estruturação de e-books curriculares, desenvolvimento de códigos-fonte instrucionais e elaboração de simulados avaliativos, a titularidade dessas obras entra em um vácuo interpretativo. Se a obra é concebida primordialmente por algoritmos, não há, à luz da legislação vigente, a atribuição de *copyright* à IES ou ao docente. Pior ainda, caso a IA reproduza fragmentos de textos protegidos que integraram sua base de treinamento original, a instituição de ensino, ao veicular esse material didático no AVA, comete infração de direitos autorais, passível de reparação material. O cenário exige novos instrumentos

contratuais e notariais para aferir a originalidade humana no material submetido.

3. METODOLOGIA

O percurso metodológico adotado caracteriza esta pesquisa como um estudo de natureza aplicada, fundamentado em uma abordagem qualitativa de cunho descritivo. O delineamento baseou-se na técnica de pesquisa documental e revisão bibliográfica crítica.

O universo de análise documental concentrou-se estritamente no arcabouço normativo federal que tangencia o ecossistema tecnológico educacional: a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014), o Código de Defesa do Consumidor (Lei nº 8.078/1990) e a Lei de Direitos Autorais (Lei nº 9.610/98). Adicionalmente, procedeu-se à análise da Nova Lei de Licitações (Lei nº 14.133/2021) aplicável aos entes públicos provedores de educação.

A pesquisa jurisprudencial restringiu-se exclusivamente a precedentes reais, fidedignos e com trânsito em julgado das cortes superiores, com ênfase analítica na ADI 6387 do STF. O método de interpretação consistiu na extração de imperativos legais do ordenamento jurídico (fase hermenêutica) e sua imediata conversão em requisitos sistêmicos, arquiteturais e gerenciais (fase operacional). A síntese desse processo culminou na construção do artefato científico desta pesquisa: o *Framework* de Compliance Educacional, desenhado para suprir as lacunas estruturais das instituições de ensino a distância no Brasil.

4. RESULTADOS E DISCUSSÃO: O FRAMEWORK DE COMPLIANCE EDUCACIONAL

A transposição dos conflitos jurídicos analisados para a realidade administrativa e tecnológica das IES resultou na formulação de um modelo operacional composto por cinco diretrizes essenciais. Cada diretriz propõe uma ação estruturante capaz de mitigar os passivos legais inerentes ao uso da Inteligência Artificial.

4.1. Diretriz I: Arquitetura de Redes, Segurança da Informação e Prevenção de Anomalias

A conformidade com a LGPD e o Marco Civil não se resolve apenas na atualização de políticas de privacidade contratuais; ela demanda reestruturação na infraestrutura de Tecnologia da Informação. A introdução de algoritmos analíticos eleva exponencialmente a superfície de ataque da instituição de ensino.

Para assegurar a integridade do ambiente, a governança ativa pressupõe a implantação de Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS) baseados no reconhecimento de padrões da rede. A aplicação de algoritmos de detecção de anomalias no tráfego de servidores institucionais permite identificar comportamentos desviantes — como um acesso não autorizado extraindo o histórico acadêmico ou os dados sociodemográficos de milhares de alunos. Ao automatizar a identificação e contenção de exfiltrações, a IES materializa o princípio basilar da segurança preconizado pelo art. 6º, VII, da LGPD. Ademais, a infraestrutura do AVA deve operar com trilhas de auditoria (*audit trails*) inalteráveis, registrando quem acessou o dado, qual algoritmo o processou e quando ocorreu o descarte, provendo a base material probatória necessária em caso de auditorias da Autoridade Nacional de Proteção de Dados (ANPD).

4.2. Diretriz II: Segregação de Dados e Servidores de Arquivos Locais

O artigo 12 da LGPD assevera que os dados anonimizados perdem o status de dados pessoais se o processo não puder ser revertido por meios razoáveis. Consequentemente, as IES não podem submeter as métricas de seus alunos diretamente a motores de IA em nuvem terceirizada sem antes aplicar camadas espessas de anonimização.

Esta diretriz preconiza a dissociação física e lógica da Base de Identificação Pessoal (*Personally Identifiable Information* - PII) do repositório (o *Data Lake*) consumido pelas ferramentas de Inteligência Artificial. A implantação de servidores de arquivos locais para consolidação e ofuscação prévia dos dados, gerenciados por protocolos estritos de permissão em diretórios, configura uma medida de altíssima eficácia. Nesse cenário, o algoritmo de IA analisa estritamente variáveis comportamentais despersonalizadas, sendo impedido, por barreira arquitetural, de cruzar o desempenho do aluno com seus marcadores de vulnerabilidade social, localização ou renda. Essa segregação impede a formação de vieses algorítmicos discriminatórios e protege a rede principal da IES contra vazamentos direcionados.

4.3. Diretriz III: Validação Jurídica da Autoria Via Serviços Notariais e Certificação Digital

Para mitigar a insegurança jurídica gerada pela "autoria híbrida" abordada na Lei nº 9.610/98, os métodos convencionais de *software* anti-plágio tornam-se ineficazes. O *framework* integra, nesta diretriz, as garantias oriundas do Direito Processual Civil e dos serviços notariais aplicados ao ambiente digital.

Com fulcro no Código de Processo Civil (Lei nº 13.105/2015, art. 384), que disciplina a validade de instrumentos comprobatórios de fatos, a IES deve instituir mecanismos de certificação autoral na origem. Quando um docente ou especialista conteudista submeter uma matriz instrucional, um projeto de desenvolvimento de sistemas ou qualquer material didático, ele deve realizar uma assinatura digital qualificada (Padrão ICP-Brasil). Esta certificação gera um *timestamp* (carimbo de tempo) criptográfico inquestionável, cristalizando o instante em que a obra humana foi entregue à instituição. O rigor desta medida probatória exime a instituição de responsabilidade civil em ações de quebra de *copyright*, pois transfere categoricamente o ônus da prova da autoria — e as consequências pela omissão do uso indevido de IA — exclusivamente para os registros irrefutáveis do autor do material.

4.4. Diretriz IV: Contratação de Tecnologias Educacionais por Entes Públicos e o Direito Administrativo

O modelo de *compliance* adquire urgência particular nas esferas da prestação educacional ligadas à administração pública, a exemplo dos polos da Universidade Aberta do Brasil (UAB) geridos por prefeituras municipais e centros de ensino técnico estaduais. Nestes ambientes virtuais geridos pelo Estado, a IA adentra o Direito Administrativo.

A aquisição de sistemas de IA para avaliação ou curadoria no âmbito municipal deve, obrigatoriamente, obedecer aos ditames da Nova Lei de Licitações (Lei nº 14.133/2021). Os Termos de Referência não podem limitar-se a exigir *softwares* com alto poder de acerto; eles devem incluir cláusulas excludentes que imponham a "Transparência Algorítmica" (*Explainable AI*). Um gestor público

municipal que licencia um algoritmo do tipo "caixa-preta", onde nem o instrutor nem o discente compreendem os critérios que levaram à aprovação ou reprovação automática em um curso técnico, fere brutalmente os princípios da publicidade e da impessoalidade (art. 37, *caput*, da CF/88). Adicionalmente, negligenciar a segurança dos servidores e permitir o vazamento de dados de alunos da rede pública para treinamento de *big techs* atrai a responsabilidade objetiva do município e configura risco de responsabilização por improbidade administrativa (Lei nº 8.429/1992) para o servidor que autorizou o contrato.

4.5. Diretriz V: A Responsabilidade Civil Objetiva e a Governança Ativa

A consolidação do *framework* conclui-se com o mapeamento preciso da responsabilidade civil das IES. No âmbito das instituições privadas, a relação mantida com o estudante de EaD é regulada pelas normas consumeristas, operando sob a égide da responsabilidade civil objetiva, expressa no art. 14 do Código de Defesa do Consumidor (Lei nº 8.078/1990). Isso implica que, se um algoritmo de monitoramento e avaliação (ex.: sistemas de *proctoring* automatizado) apresentar falsos positivos, cancelando a prova de um aluno injustamente ou expondo seu histórico, a instituição responderá integralmente pelos danos materiais e morais causados, independentemente de demonstração de dolo ou culpa. A IES não poderá utilizar o argumento de "falha no código da empresa fornecedora" para se esquivar de suas obrigações primárias perante o discente.

Para as instituições de ensino estatais, vigora o mesmo regime objetivo, porém ancorado na Teoria do Risco Administrativo (§ 6º do

art. 37 da Constituição Federal). Diante deste panorama rigoroso, as diretorias e reitorias não podem delegar as decisões tecnológicas exclusivamente às equipes de desenvolvimento. É mandatório instituir um Comitê Permanente de Governança de TI e Ética Educacional, encarregado de homologar cada nova integração de Inteligência Artificial ao AVA, testando os limites de privacidade, rastreabilidade e isenção de vieses algorítmicos.

5. CONSIDERAÇÕES FINAIS

O ecossistema da Educação a Distância no Brasil assumiu a vanguarda da adoção de ferramentas baseadas em Inteligência Artificial. Contudo, o adensamento teórico, normativo e técnico conduzido por este estudo evidenciou que a hiperautomação pedagógica opera atualmente em descompasso severo com a segurança jurídica e a robustez arquitetural. Na ausência de um Marco Regulatório da Inteligência Artificial sancionado pelo Congresso Nacional, a inércia institucional das IES representa um passivo financeiro inaceitável para o setor privado e uma exposição perigosa ao risco de improbidade para os gestores da administração pública.

O *framework* proposto — consubstanciado na adoção de auditoria de redes, segregação de servidores locais, certificação notarial digital e editais licitatórios ancorados em transparência algorítmica — fornece um roteiro pragmático e tecnicamente sólido para reitores, gestores públicos e profissionais de TI educacional.

Diferentemente dos estudos que centralizam a análise na interação sala de aula versus *chatbots*, esta pesquisa demonstra que o real desafio sistêmico da IA no EaD se localiza nos bastidores da

governança. Conclui-se, portanto, que a implementação de um *compliance* educacional estruturado é a via metodológica e administrativa indispensável para assegurar que a evolução tecnológica mantenha-se estritamente subordinada ao preceito da autodeterminação informativa, à segurança de redes operacionais e à integridade dos direitos constitucionais dos discentes brasileiros.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988.

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF, 2022.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF, 2014.

BRASIL. *Lei nº 13.105, de 16 de março de 2015*. Código de Processo Civil. Brasília, DF, 2015.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

BRASIL. *Lei nº 14.133, de 1º de abril de 2021*. Lei de Licitações e Contratos Administrativos. Brasília, DF, 2021.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF, 1990.

BRASIL. *Lei nº 8.429, de 2 de junho de 1992*. Dispõe sobre as sanções aplicáveis em virtude da prática de atos de improbidade administrativa. Brasília, DF, 1992.

BRASIL. *Lei nº 9.610, de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, DF, 1998.

BRASIL. Supremo Tribunal Federal (Plenário). *Ação Direta de Inconstitucionalidade (ADI) nº 6387*. Relatora: Ministra Rosa Weber. Julgamento em: 07/05/2020. Publicação: DJe 12/11/2020. Brasília, DF.

GIRAFFA, L.; KOHLS-SANTOS, P. Inteligência Artificial e Educação: conceitos, aplicações e implicações no fazer docente. *Educ. Anál.*, Londrina, v. 8, n. 1, p. 116-134, 2023.

SILVA, W. M. da et al. Conhecendo o CHATGPT e seus impactos na educação. *Revista Foco*, v. 17, n. 9, p. e5794, 2024.

¹ Especialista em Segurança da Informação (Faculdade Focus). Formação Pedagógica em Informática (Uniasselvi). Instrutor de TI (SENAC PE). ORCID: <https://orcid.org/0009-0008-6740-4604>. E-mail: [acesse o artigo original para visualizar o e-mail](#).

² Bacharel em Sistemas de Informação (Universidade Federal do Piauí – UFPI). Especialista em Novas Tecnologias na Educação (Escola Superior Aberta do Brasil – ESAB). Professora vinculada à Secretaria de Educação do Estado do Piauí. E-mail: [acesse o artigo original para visualizar o e-mail](#)

³ Especialista em Gestão Empresarial (Fundação Getúlio Vargas – FGV – RJ/SP). Administradora e Professora Substituta de Ensino Básico, Técnico e Tecnológico (Instituto Federal do Piauí – IFPI). ORCID: <https://orcid.org/0009-0009-9636-8398>. E-mail: [acesse o artigo original para visualizar o e-mail](#).

⁴ Bacharel em Sistemas de Informação (Universidade Federal do Piauí – UFPI). Especialista em Docência do Ensino Superior (Instituto de Ensino Superior Múltiplo – IESM) e em Educação a Distância: Gestão e Tutoria (Centro Universitário Leonardo da Vinci – UNIASSELVI). Professora vinculada à Secretaria de Educação do Estado do Piauí, Gestora de Polo do Centro Universitário Leonardo da Vinci (UNIASSELVI) e Tutora da Universidade Federal do Piauí (UFPI), vinculada ao Centro de Educação a Distância – Licenciatura em Computação. ORCID: <https://orcid.org/0000-0003-3900-4124>. E-mail: [acesse o artigo original para visualizar o e-mail](#).

⁵ Especialista em Sistemas de Telecomunicações (ESAB). Especialista em Inteligência Artificial (Faculdade Rio Grande). Bacharel em Sistemas de Informação (Universidade Federal do Piauí – UFPI). Professor Substituto da Universidade Federal do Piauí (UFPI – Campus de Picos) e Professor da SEDUC-PI. ORCID: <https://orcid.org/0009-0009-4832-5406>. E-mail: [acesse o artigo original para visualizar o e-mail](#).