

CORRESPONSABILIDAD ESCOLAR ANTE LA VIOLENCIA DIGITAL: DESAFÍOS DE LA LEY 15.211/2025

CORRESPONSABILIDADE ESCOLAR DIANTE DA VIOLÊNCIA DIGITAL: DESAFIOS DA LEI 15.211/2025

Lizeth Nataly Delgado Villota¹
Fernando de Brito Alves²

RESUMEN

El avance tecnológico y la proliferación del ciberacoso han transformado la violencia digital en una vulneración directa del derecho a la educación, lo que evidenció la lentitud e insuficiencia del modelo reactivo propuesto inicialmente en el artículo 19 del Marco Civil de Internet. Ante esta problemática, Brasil ha transitado hacia un paradigma de corresponsabilidad institucional estructurado mediante la Ley 15.211/2025 y el Decreto 12.975/2026. En este contexto normativo, el presente artículo tiene como objetivo analizar los desafíos operativos que asumen los establecimientos educativos para garantizar este derecho. Metodológicamente, la investigación emplea un enfoque cualitativo, sustentado en el método jurídico-dogmático y la revisión documental de normativas internacionales y nacionales. Los hallazgos permiten inferir que las escuelas adquieren un rol de ejecución activa, el cual demanda la articulación de canales interinstitucionales, el mapeo de riesgos, el monitoreo del entorno y la consolidación de programas de alfabetización digital dirigidos a la comunidad educativa.

Palabras clave: Derecho a la educación; ciberacoso; ECA Digital; Corresponsabilidad; Instituciones Educativas.

RESUMO

O avanço tecnológico e a proliferação do ciberassédio transformaram a violência digital em uma violação direta do direito à educação, o que evidenciou a lentidão e a insuficiência do modelo reativo proposto inicialmente no artigo 19 do Marco Civil da Internet. Diante dessa problemática, o Brasil transitou para um paradigma de corresponsabilidade institucional estruturado pela Lei 15.211/2025 e pelo Decreto 12.975/2026. Nesse contexto normativo, o presente artigo tem como objetivo analisar os desafios operacionais assumidos pelos estabelecimentos de ensino para garantir esse direito. Metodologicamente, a pesquisa emprega uma abordagem qualitativa, sustentada no método jurídico-dogmático e na revisão documental de normativas internacionais e nacionais. Os resultados permitem inferir que as escolas adquirem um papel de execução ativa, o qual demanda a articulação de canais interinstitucionais, o mapeamento de riscos, o monitoramento do ambiente e a consolidação de programas de alfabetização digital direcionados à comunidade escolar.

Palavras-chave: Direito à educação; Cyberbullying; ECA Digital; Corresponsabilidade; Instituições de ensino.

INTRODUCCIÓN.

¹ Advogada. E-mail para contato: lizeth.villota@discente.uenp.edu.br

² Doutor em Direito. Professor Associado da Universidade Estadual do Norte do Paraná. LATTES: <http://lattes.cnpq.br/1975997868167667>. ORCID: <https://orcid.org/0000-0001-8917-4717>. E-MAIL para contato: fernandobrito@uenp.edu.br

El derecho y la tecnología avanzan a diferentes velocidades, y en esa asimetría la regulación reactiva suele llegar tarde. En Brasil, si un estudiante sufría acoso en línea, la víctima y la institución educativa dependían de la emisión de una orden judicial para lograr la remoción del contenido lesivo, no obstante, hasta completar el trámite procesal, el daño psicológico y social ya se había propagado entre la comunidad escolar y digital. Este esquema se sustentaba en el artículo 19 del Marco Civil de Internet (Brasil, 2014), una disposición que limitaba la responsabilidad directa de las plataformas y las eximía de actuar de manera autónoma. Este modelo fue objeto de control de constitucionalidad: el Supremo Tribunal Federal, al juzgar el Recurso Extraordinario (RE) 1.037.396, correspondiente al tema 987, que declaró la inconstitucionalidad parcial del artículo 19 (Brasil, 2025b), dicha decisión jurisprudencial estableció el precedente para la transición normativa analizada en la presente investigación.

El escenario normativo en materia digital en Brasil ha experimentado una serie de transformaciones con la vigencia de la Ley n.º 15.211 (Brasil, 2025a) que instituye el *Estatuto da Criança e do Adolescente Digital (ECA Digital)*, y posteriormente el del Decreto n.º 12.975 (Brasil, 2026), instaurando un mandato legal de proactividad y corrección de fallas sistémicas para las empresas tecnológicas. Esta transición incide de forma directa en las garantías educativas; sin embargo, la materialización de este modelo traslada exigencias operativas concurrentes a las instituciones de enseñanza. En la actualidad, el aula no se limita a su infraestructura física y la violencia digital puede generar una vulneración al derecho a la educación afectando el rendimiento académico, el bienestar emocional y se puede consolidar como un factor directo de exclusión escolar. En el caso de que un estudiante padezca acoso continuo a través de una aplicación, plataforma o red social, la vulneración a su derecho a la educación se materializa con la misma severidad que en el espacio presencial.

A partir de este contexto, el presente texto plantea la siguiente pregunta de investigación: ¿Cuáles son los desafíos operativos e institucionales que enfrentan los establecimientos educativos en Brasil para articular la garantía del derecho a la educación con el modelo de corresponsabilidad impuesto mediante la Ley n.º 15.211/2025?

La hipótesis central sostiene que, si bien la transición legislativa reconfigura la protección digital al exigir seguridad desde el diseño a las plataformas corporativas, la garantía efectiva del derecho a la educación frente a la violencia digital exige también un ejercicio de corresponsabilidad, en donde el Estado, por medio de sus instituciones educativas tendrá la misión de organizar su capacidad administrativa y técnica para articular la norma, para lo cual se requiere estructurar canales interinstitucionales, ejecutar capacitaciones, mapeos de riesgos en entornos digitales, adoptar instrumentos de evaluación e implementar procesos de alfabetización digital y control de datos personales dentro de la comunidad escolar.

Esta investigación se desarrolla bajo un enfoque cualitativo, fundamentado en el método jurídico dogmático y estructurado mediante un diseño teórico documental, realizando un examen sistemático de la legislación vigente, su evolución y su aplicabilidad institucional para analizar la ejecución de la norma en el entorno escolar. Se emplea el análisis documental como técnica de recolección de información, aplicado al corpus normativo internacional y nacional, con énfasis en la Ley n.º 15.211/2025 (ECA Digital), el Decreto n.º 12.975/2026, y directrices técnicas de interoperabilidad. A partir de esta revisión, se evalúan los desafíos operativos que asumen los centros educativos para garantizar el derecho a la educación libre de ciberacoso y violencia

digital. La delimitación temporal del corpus documental abarcó el período de 2014 a 2026, desde el Marco Civil de Internet (Ley n.º 12.965/2014) hasta el Decreto n.º 12.975/2026, y la selección de las fuentes normativas, jurisprudenciales e institucionales obedeció a los criterios de (i) vigencia y pertinencia directa con la corresponsabilidad escolar frente a la violencia digital, (ii) jerarquía normativa e institucional del emisor, y (iii) disponibilidad de acceso público a texto íntegro, habiéndose excluido: (i) proyectos normativos aún en tramitación legislativa, por no integrar el derecho vigente; (ii) decisiones jurisprudenciales de instancias no vinculantes, salvo el precedente de repercusión general del Supremo Tribunal Federal; (iii) modelos de derecho comparado no estructurados en torno a obligaciones sistémicas de debida diligencia digital; y (iv) fuentes sin acceso público verificable. La organización del corpus siguió una lógica cronológico-temática, agrupando los instrumentos internacionales, la legislación brasileña y el derecho comparado conforme su incidencia sobre el objeto de estudio.

Fundamentos del derecho a la educación y su desafío con los daños online

La educación se consolida en el marco jurídico internacional como un derecho humano esencial, un pilar para la dignidad y una garantía habilitante que facilita el ejercicio pleno de otras libertades fundamentales, abarcando desde las civiles y políticas hasta las económicas y culturales. Esta prerrogativa universal e inalienable se encuentra establecida en instrumentos como la Declaración Universal de Derechos Humanos (artículo 26) y es vital para la consecución de la paz y el desarrollo sostenible global, tal como lo enfatiza la Agenda 2030 a través del Objetivo de Desarrollo Sostenible número 4 (ODS 4). Dicha visión exige que los Estados garanticen la progresiva accesibilidad y la gratuidad de la enseñanza en sus diversos niveles.

Sin embargo, la materialización de este derecho fundamental se ve afectada por el incremento de conflictividad en los centros educativos, exacerbada por la proliferación del acoso escolar (*bullying*) y su manifestación en la esfera digital, el ciberacoso (*ciberbullying*). Estos comportamientos agresivos y repetitivos, caracterizados por un ineludible desequilibrio de poder entre el agresor y la víctima, se han trasladado al entorno virtual mediante el uso de tecnologías de la información, lo que agrava la vulnerabilidad de las víctimas al extender la intimidación más allá de los límites escolares.

En este contexto, es fundamental comprender que la violencia digital no constituye únicamente un problema de convivencia escolar o de interacción social en línea, sino que configura una forma de vulneración directa del derecho humano a la educación. En efecto, cuando el acoso se despliega en entornos digitales, afecta no solo la integridad emocional de las víctimas, sino también su capacidad real de acceder, permanecer y participar en el proceso educativo en condiciones de dignidad, igualdad y seguridad. De este modo, la violencia digital debe ser analizada desde una perspectiva de derechos humanos, como un fenómeno que compromete estructuralmente el ejercicio efectivo del derecho a la educación en la sociedad contemporánea.

La región de América Latina ha sido identificada como un punto crítico en esta problemática, en el caso de Brasil, las tasas de acoso tradicional y de ciberacoso son motivo de preocupación, en las que se encuentran consecuencias psicopatológicas severas incluyendo ansiedad, depresión, riesgo de suicidio, que menoscaban el desarrollo integral y el rendimiento académico de los estudiantes.

El corpus internacional, la educación como derecho habilitante

Para entender la responsabilidad de regular el espacio virtual, es importante estudiar de dónde surge la obligación original del Estado. Los tratados internacionales no ven la educación como un simple ejercicio de memorización y repetición, sino que se estructura como un derecho habilitante, una base que permite a las personas ejercer otras libertades civiles, políticas, sociales, culturales y económicas de forma efectiva. La agenda 2030 de Naciones Unidas, mediante el ODS 4, establece el compromiso de la comunidad internacional de “garantizar una educación inclusiva, equitativa y de calidad y promover oportunidades de aprendizaje durante toda la vida para todos” (Naciones Unidas, 2021a).

En la revisión de los textos matrices, se encuentra la Declaración Universal de Derechos Humanos, en su artículo 26 se establece que la educación debe orientarse al desarrollo pleno de la personalidad, el respeto por los derechos y libertades fundamentales. Su carácter universal e inclusivo al reconocer que es inalienable de todas las personas, sin distinción, accesible a todos en condiciones de igualdad, el cual a su vez debe promover la comprensión, tolerancia, amistad, paz entre todas las naciones en el marco de los derechos humanos (Organización de las Naciones Unidas, 1948).

El Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC), en sus artículos 13 y 14, reconoce que el derecho a la educación debe orientarse hacia el pleno desarrollo integral del ser humano y exige a los Estados garantizar la gratuidad de la enseñanza primaria y avanzar progresivamente en la accesibilidad de la secundaria y la superior, utilizando todos los recursos disponibles para alcanzarlo (Organización de las Naciones Unidas, 1966).

La normativa aplica también enfoques diferenciados para grupos específicos, como la Convención sobre los Derechos del Niño (artículos 28 y 29) que obliga a centrar el modelo en el desarrollo integral del menor. Exige que la disciplina escolar respete su dignidad y potencie sus aptitudes físicas y mentales hasta el máximo, formando individuos preparados para la vida en sociedad (Organización de las Naciones Unidas, 1989). De manera paralela, la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer - CEDAW (artículo 10), consagra el derecho a la educación de las mujeres en igualdad de condiciones, con un enfoque de acciones concretas para erradicar la discriminación, los estereotipos de género, reducir la deserción femenina y promover acciones afirmativas con el fin de alcanzar la igualdad sustantiva en el ejercicio efectivo de sus derechos, desarrollo y empoderamiento de las mujeres (Organización de las Naciones Unidas, 1979).

A nivel Latinoamericano, el Protocolo Adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales "Protocolo de San Salvador" (artículo 13) ratifica este mandato, obligando a los Estados a garantizar una educación de calidad en todos sus niveles y a mejorar continuamente el sistema educativo para que los estudiantes participen activamente y se puedan desarrollar integralmente y en la sociedad (Organización de Estados Americanos, 1988).

Este cuerpo normativo internacional, establece claras obligaciones jurídicas para los Estados que se han adherido, más allá de la mera declaración de derechos, las cuales son de carácter progresivo e inclusivo, y se deben alinear con el pleno desarrollo de la personalidad humana, el respeto de los derechos y libertades fundamentales, tanto de

manera presencial como con los nuevos desafíos de la virtualidad, en todos los espacios académicos.

La conceptualización del bullying y el ciberbullying.

La conceptualización moderna del acoso escolar (*bullying*) se cimenta en las investigaciones pioneras de Dan Olweus, iniciadas en la década de 1970, después de suicidios de varios estudiantes que reflejó las graves consecuencias del maltrato entre pares (Silva *et al.*, 2025). El trabajo de Olweus (1993) fue central para establecer las bases de la definición: el *bullying* se caracteriza por tener comportamientos agresivos y repetitivos, que se manifiestan como intimidación física o psicológica entre estudiantes, dentro de sus elementos esenciales se encuentra el desequilibrio de poder entre el agresor y la víctima, lo cual se genera cuando un alumno de forma reiterada y prolongada recibe acciones negativas, intencionales ante las cuales tiene dificultad de defenderse, y enfatizó que dicho fenómeno afecta negativamente el ambiente escolar en su totalidad, perjudicando profundamente el desarrollo académico y social de quienes son victimizados (Pinho de Oliveira, 2023).

Hoy en día, en la era digital, este fenómeno ha evolucionado hacia el ciberacoso (*ciberbullying*), una forma de violencia que utiliza las tecnologías de la información y la comunicación como medio para su ejecución (Antonio Ortega *et al.*, 2024). Por su parte Tokunaga (2010) lo define como un comportamiento intencional y repetitivo, realizado de manera individual o grupal con el fin de causar daño por medios digitales, el cual trasciende las barreras espacio temporales del entorno escolar, lo que permite que la intimidación persista de forma continua y se difunda a una audiencia ilimitada agravando la vulnerabilidad y la incertidumbre de la víctima.

Al extenderse este maltrato a la esfera de la tecnología, el Manual de violencia de género en línea publicado por la OEA (2022) evidencia diferentes tipos de violencia como las siguientes: Creación, difusión, distribución o intercambio digital de fotografías, vídeos o audioclips de naturaleza sexual o íntima sin consentimiento; Acceso, uso, manipulación o intercambio o distribución no autorizados de datos personales; suplantación y robo de identidad; actos que dañan la reputación o credibilidad de una persona; actos que implican la vigilancia y el monitoreo de una persona; ciberhostigamiento; ciberacoso; ciberintimidación; amenazas directas de daño; violencia física facilitada por las tecnologías; abuso, explotación a través de las tecnologías; ataques a grupos, organizaciones o comunidades.

La evolución del acoso escolar hacia el entorno digital no constituye una simple transición de conductas preexistentes, sino una reconfiguración cualitativa del fenómeno, conservando sus elementos de intencionalidad, repetición, desequilibrio de poder, pero que adquieren unas nuevas dimensiones en el ciberespacio, como la supresión de las barreras espaciotemporales, el potencial anonimato del agresor y la amplificación del daño ante audiencias ilimitadas que intensifican significativamente la vulnerabilidad de las víctimas. A ello se le suman las diversas formas de violencia en línea anunciadas por la OEA (2022) que representan un riesgo directo para el buen desarrollo del derecho a la educación de niños y adolescentes.

La violencia digital como violación del derecho a la educación.

La violencia digital constituye una forma contemporánea y creciente de la vulneración de los derechos de la infancia, con impactos directos sobre el derecho a la educación, es por ello que el Comité de los Derechos del Niño de las Naciones Unidas, en su observación General No 25 de 2021, reconoce que el entorno digital representa al mismo tiempo un espacio de oportunidades y de riesgos para la infancia, destacando que los Estados partes tienen la obligación de proteger a los niños frente a las ciberagresiones, amenazas, censura, filtraciones de datos y la vigilancia digital (Naciones Unidas, 2021b). En ese sentido cuando la violencia escolar incide sobre el entorno escolar o sobre los procesos de aprendizaje, compromete no solo el bienestar emocional del estudiante, sino también el ejercicio pleno de su derecho a la educación, consagrado en el artículo 28 de la Convención sobre los Derechos del Niño (Organización de las Naciones Unidas, 1989).

La ciberagresión produce efectos perjudiciales sobre el rendimiento académico y la permanencia escolar de niños y adolescentes, por ello la Declaración Conjunta sobre inteligencia artificial en su numeral cuarto, literal a, sobre seguridad de los niños manifiesta:

Se deben prevenir y abordar todas las formas de violencia contra los niños y explotación infantil cometidas a través de los sistemas, herramientas y plataformas de IA o con su apoyo. Se refiere a la violencia física, sexual y mental, incluida la violencia de género, el ciberacoso, la exposición a contenidos y explotación perjudiciales, el contenido generado por IA que propague discursos de odio, incite a la violencia o promueva el trabajo infantil, la trata de niños, el reclutamiento y utilización de niños, y el asesinato y la mutilación, entre otros, en situaciones de conflicto armado. El contenido perjudicial puede incluir los deepfakes y otros medios engañosos generados por IA, la incitación al odio, el material gráfico violento, contenidos de abusos sexuales infantiles, la mendicidad infantil forzada, la información errónea o desinformación dirigida a los niños y contenidos que promueven las autolesiones, los trastornos alimentarios, el consumo de drogas u otras sustancias nocivas, los juegos de azar u otros discursos dañinos amplificados algorítmicamente (Naciones Unidas et al., 2025).

Esta convergencia de riesgos digitales se manifiesta con particular gravedad en América Latina, una región con altos índices de violencia y conflictos estructurales que permean los centros educativos, en donde los estudiantes experimentan acoso y ciberacoso, conductas que en su manifestación más extrema inciden en las más de 200.000 muertes anuales registradas a nivel global por homicidio o suicidio inducido (Antonio Ortega *et al.*, 2024).

En Brasil, las tasas de acoso escolar tradicional y ciberacoso presentan indicadores elevados, la Pesquisa Internacional sobre Enseñanza y Aprendizaje (Brasil, 2021) reportó que el 28% de los directores de escuelas brasileñas señalaron que la intimidación o el bullying entre los estudiantes es una situación que ocurre semanal o diariamente, un porcentaje que consideran alto, teniendo en cuenta que el promedio en América Latina y 48 países participantes en el estudio es del 13%. Es decir, que la frecuencia con la que los directores brasileños perciben que la violencia entre estudiantes es más del doble del promedio internacional (28% frente al 13%), lo que evidencia que la violencia entre estudiantes es un problema significativo, que afecta la convivencia escolar y bienestar de niños y adolescentes.

Aunado a lo anterior, la *Pesquisa Nacional de Saúde Escolar* (PeNSE) de 2019, conducida por el Instituto Brasileiro de Geografia e Estatística (IBGE), aplicada a estudiantes brasileños de 13 a 17 años, reveló que el 39.1% de los estudiantes

adolescentes admitió haber sufrido ciberacoso, provocación o intimidación (IBGE, 2021). Este alto nivel de violencia en el ambiente escolar genera inseguridad y tensión que perjudica el proceso de enseñanza, aprendizaje y se considera una violación de los derechos humanos, y es un problema estructural puesto que Brasil es considerado el segundo país que registra más casos de ciberacoso, solo superado por la India (Purificação e Cerqueira, 2025).

Un informe publicado en marzo de 2026 por UNICEF revela que uno de cada cinco adolescentes brasileños, entre 12 y 17 años sufrió explotación o abuso sexual, con el fin de atraer, extorsionar, producir, almacenar o difundir material abusivo. Estos actos se materializan en el entorno virtual, presencial, o mediante una combinación de ambos, configurando una forma de violencia facilitada por herramientas digitales, como redes sociales, juegos en línea y plataformas de mensajería; asimismo, este estudio evidenció tres situaciones recurrentes: i) el 14% de los niños y adolescentes entrevistados, recibió contenido sexual no solicitado; ii) en el 49% de los casos, la explotación o abuso fue perpetrada por un individuo conocido por la víctima; y iii) el 34% de los menores no reportó el incidente ni solicitó asistencia (UNICEF *et al.*, 2026).

En consecuencia, la agresión digital entre menores demanda atención institucional prioritaria ante el incremento estadístico de los casos y el derecho a la educación de los niños y adolescentes se ve directamente vulnerado ante la ocurrencia de daños continuos y sistemáticos facilitados por las tecnologías de la información, los cuales comprometen la integridad y seguridad del entorno escolar.

El derecho comparado como antecedente dogmático.

Frente a este escenario, jurisdicciones como la Unión Europea en 2022 empezaron a tomar acción, puesto que durante muchos años predominó la idea de que las plataformas eran intermediarios neutrales, y por medio del Reglamento de Servicios Digitales (DSA) de la Unión Europea y la Ley de Seguridad en Internet (Online Safety Act de 2023) del Reino Unido obligaron a las empresas a asumir su papel de evaluación, transparencia, mitigación de riesgos y un buen funcionamiento de los servicios digitales.

El reglamento de Servicios Digitales (Unión Europea, 2022) en sus considerandos 46, 71 y artículo 28, establece un marco de obligaciones escalonadas de debida diligencia, enfocado en la protección de menores, en donde se prohíbe el perfilamiento publicitario, se exige que el diseño de interfaces sea con el máximo nivel de privacidad y seguridad por defecto, y obliga a redactar las condiciones generales del servicio en un lenguaje comprensible. Respecto al contenido ilícito y al material de abuso y acoso sexual infantil, las plataformas deben establecer canales accesibles de notificación y acción, sistemas de reclamación con revisión humana y vías prioritarias de resolución extrajudicial de litigios. Adicionalmente, a las plataformas de gran tamaño, se les impone un ciclo de evaluación y mitigación de riesgos dirigido a identificar los efectos negativos sobre los derechos fundamentales y la integridad de los usuarios. Asimismo, estas corporaciones están obligadas a someterse a auditorías independientes anuales y a publicar informes de transparencia sobre sus prácticas de moderación de contenido; su incumplimiento puede acarrear sanciones de hasta el 6% del valor de su facturación anual (Unión Europea, 2022, art. 74).

La legislación británica por medio de la Ley de Seguridad en Internet “*Online Safety Act*” (2023), adicionó un “deber de cuidado” vinculante, forzando a las redes sociales, motores de búsqueda, los servicios de mensajería y foros en línea, a implementar verificación de edad y bloquear el acceso de menores a contenido

prioritario como pornografía, promoción del suicidio, autolesión, trastornos alimentarios, consumo de sustancias nocivas, retos peligrosos, o violencia extrema. Asimismo, la exigencia de evaluar riesgos derivados de sus propios servicios para usuarios menores de edad, incluyendo el funcionamiento de sus algoritmos de recomendación.

Asimismo, otorgó funciones de seguridad en internet a la Oficina de Comunicaciones “Ofcom” encargada de supervisar y sancionar a las plataformas digitales que incumplan con multas de hasta 18 millones de libras esterlinas o el 10% de sus ingresos mundiales, aplicándose la cifra que resulte mayor (Reino Unido, 2023) y en los supuestos de mayor gravedad, solicitar a los tribunales británicos ordenar a proveedores de servicios de pago, a anunciantes y a operadores de infraestructura de internet que cesen su relación comercial con la plataforma infractora, privándola de financiación y de accesibilidad en el mercado (Ofcom, 2024). Estas normativas respaldan sus exigencias con autoridades dotadas de poder para imponer multas severas sobre la facturación global de las empresas infractoras.

Paralelamente, la norma tipificó un conjunto de nuevos delitos penales, que recaen sobre los individuos remitentes de comunicaciones lesivas, entre ellos se encuentran el *cyberflashing*, el abuso de imagen íntima, las comunicaciones amenazantes, el *epilepsy trolling*, conducta consistente en la transmisión deliberada de material visual con el propósito de desencadenar convulsiones en personas con epilepsia fotosensible, y la incitación a la autolesión grave (Reino Unido, 2023, art. 171-190).

Esta legislación demuestra que exigir proactividad técnica a los intermediarios es jurídicamente viable, mediante obligaciones de diseño tecnológico, supervisión regulatoria amplia y mecanismos sancionatorios, se establecen marcos integrales en materia de seguridad digital. Ello evidencia una transición desde esquemas de autorregulación corporativa hacia modelos de responsabilidad jurídica para las plataformas frente a los riesgos derivados de su propio funcionamiento. Este avance es un antecedente fundamental para la transformación del sistema brasileño, marcando una ruta para integrar la seguridad del entorno digital como requisito para cumplir las obligaciones de tratados internacionales de protección educativa.

La transformación y actualización de la normatividad brasileña en materia de protección digital a menores de edad.

La protección infantil en Brasil posee una doble connotación normativa, en primer lugar, a partir de la ratificación de la Convención de los Derechos del Niño (Organización de las Naciones Unidas, 1989, art. 19) se instauró la responsabilidad de los Estados Parte de adoptar las medidas legislativas, administrativas y sociales requeridas para proteger a los menores contra toda forma de perjuicio, explotación o abuso de carácter físico o mental, estableciendo que deben contener procedimientos eficaces para su cumplimiento. En segundo lugar, a nivel interno, este mandato se fundamenta en el Estatuto da Criança e do Adolescente (ECA), promulgado mediante la Ley 8.069 (Brasil, 1990). Esta norma impone a la familia, a la sociedad y al poder público el deber solidario de salvaguardar a los menores ante cualquier forma de negligencia, discriminación o violencia, ratificando la responsabilidad del núcleo familiar de proteger al menor, asegurar sus derechos y promover un entorno adecuado.

En consonancia con este marco de protección, el ordenamiento jurídico establece la responsabilidad civil de las instituciones educativas respecto a la integridad física y

moral de los menores mientras se encuentran bajo su custodia, guarda y vigilancia, obligación que es tratada principalmente bajo el régimen de responsabilidad objetiva (Brasil, 2002), lo que exige a los centros de enseñanza responder por los daños ocurridos en su esfera institucional tanto física como virtual, incluyendo programas y canales de comunicación.

La transición hacia el entorno digital amplió el alcance de estas obligaciones mediante la Ley 15.211 (Brasil, 2025), normativa que determina la responsabilidad de las plataformas digitales al imponer un deber objetivo de cuidado, mediante la implementación de controles técnicos, con la obligación de configurar parámetros de privacidad en su nivel más restrictivo por defecto, integrar mecanismos de verificación de edad y habilitar herramientas de supervisión parental. Adicionalmente, los proveedores deben aplicar medidas de mitigación de riesgos destinadas a impedir la exposición algorítmica a contenidos perjudiciales, como violencia, apuestas o autolesiones, y abstenerse de realizar procesos de perfilamiento de datos para la emisión de publicidad dirigida a menores de edad.

A partir de este engranaje normativo, el legislador complementó y desarrolló instrumentos específicos para articular la protección en el entorno escolar.

La protección infantil en Brasil tiene su fundamento en el Estatuto da Criança e do Adolescente (ECA), promulgado mediante la Ley 8.069 (Brasil, 1990). Esta norma impuso a la familia, a la sociedad y al poder público el deber solidario de salvaguardar a los menores de cualquier forma de negligencia, discriminación o violencia. A partir de esta premisa, el legislador desarrolló instrumentos específicos para el entorno escolar.

En 2015, la Ley 13.185 instituyó el Programa de Combate a la Intimidación Sistemática en el territorio nacional (Brasil, 2015) la cual proporcionó la definición legal de *bullying*, estipulando que es todo acto de violencia física o psicológica, intencional y repetitiva, que ocurre sin motivación evidente, el cual es practicada por un individuo o un grupo, contra una o más personas, con el objetivo de intimidarlas o agredirlas, causando dolor y angustia, la cual ocurre en una relación de desequilibrio de poder. Esta norma tiene como fin prevenir y cohibir actos de violencia física o psicológica, la exclusión social y discriminación, incluyendo la violencia virtual, abarcando el envío de mensajes intrusivos, la difusión de datos personales o fotografías reales o alteradas con el propósito de causar daño emocional o ejercer coacción psicológica, económica o social. Posteriormente, el sistema sumó obligaciones institucionales: por medio de la Ley No 13.663 de 2018, introdujo una modificación sustancial en la *Lei de Diretrizes e Bases da Educação Nacional* (LDB) y exigió a los establecimientos de enseñanza promover medidas de concientización, prevención y combate a todos los tipos de violencia, y promoción de la cultura de paz (Brasil, 2018a).

A pesar de lo anterior, ante la existencia de una crisis de convivencia escolar, se tuvo que dar una respuesta estatal que avanzó hacia la coerción penal, en 2024 la Ley n° 14.811 modificó el Código Penal, la *Lei dos Crimes Hediondos* y el ECA para establecer medidas concretas de protección en establecimientos educativos (Brasil, 2024b).

Esta legislación incorporó el artículo 146-A en el Código Penal, tipificando las conductas de intimidación sistemática cometidas de forma individual o colectiva, el delito de *ciberbullying* se configuró como una agravación de la conducta base. Si la intimidación se realiza a través de redes sociales, aplicaciones, juegos en línea o cualquier entorno digital, conlleva una pena de reclusión de dos a cuatro años, además del pago de una multa. Adicionalmente, se incrementaron agravantes que impactan otros delitos penales, verbigracia, la pena se incrementa si el crimen es practicado en una institución educativa, y en el contexto de inducción, instigación o auxilio a suicidio o

automutilación a través de medio digitales, la pena se duplica si el autor es líder, coordinador o administrador de un grupo, comunidad o red virtual, o es responsable por esta (Brasil, 2024b).

De forma paralela a la legislación educativa y penal, la *Lei Geral de Proteção de Dados Pessoais* (LGPD) aportó un componente técnico aplicable a las plataformas digitales, en su artículo 14 se determina que el tratamiento de datos personales de niños y adolescentes debe realizarse atendiendo a su interés superior, exige el consentimiento específico de al menos uno de los padres o responsables legales, y prohíbe condicionar la participación de los menores en juegos o aplicaciones a la entrega de información personal que exceda lo estrictamente necesario para la actividad (Brasil, 2018b).

Inicialmente, el Marco Civil de Internet (Ley n° 12.965 de 2014) eximía a las plataformas digitales de responsabilidad por el contenido generados por terceros, condicionando su remoción a la expedición de una orden judicial específica (Brasil, 2014, art. 19). Esta dependencia procesal resulta lenta e ineficaz para la víctima del acoso, frente a la velocidad de difusión de la violencia digital. En el entorno escolar, las amenazas se manifiestan principalmente en redes sociales, donde los algoritmos de recomendación favorecen la circulación de contenidos sensacionalistas e irreales (Santos *et al.*, 2025). Dicha exposición se agrava por el déficit de alfabetización digital de los estudiantes para distinguir información verdadera de la falsa, generando como resultado una asimetría entre la inmediatez del daño y la lentitud del mecanismo de protección.

Dicha limitación evidenció la necesidad de abandonar un modelo reactivo y transitar hacia obligaciones sistémicas implementadas mediante el actual *Estatuto da Criança e do Adolescente Digital* (ECA Digital) (Brasil, 2025a) y el Decreto n.º 12.975 (Brasil, 2026), este sistema modificó su enfoque puesto que pasó de concentrarse exclusivamente en la represión del daño para exigir infraestructura preventiva a las corporaciones.

La ley n° 15.211/2025 (ECA Digital) adaptó las garantías del Estatuto da Criança e do Adolescente a la actualidad del entorno digital, introduciendo el principio de los derechos desde el diseño y la protección por defecto, estableciendo un deber de cuidado para los proveedores de productos y servicios digitales, y exige que sus servicios se ajusten al desarrollo biopsicosocial de los usuarios, obligando a una configuración predeterminada de controles de privacidad, filtros de seguridad y límites de tiempo de uso desde el primer acceso (Brasil, 2025a, art. 5).

La norma determina la gestión proactiva de riesgos vinculados a algoritmos de recomendación, prohíbe prácticas de diseño adictivo como la reproducción automática, las recompensas por tiempo de uso, las notificaciones insistentes y las cajas de oferta o *loot boxes*, asimismo una prohibición absoluta de monetización de imágenes erotizadas o sexualmente sugestivas de menores (Brasil, 2025a, art. 6 y 8).

En el ámbito comercial y de procesamiento de datos, se prohíbe el perfilamiento de menores para el direccionamiento de publicidad (Brasil, 2025a, arts. 22 y 26). Las plataformas deben adoptar medidas para impedir el acceso de productos inadecuados como apuestas, alcohol, tabaco y para el contenido de adultos, la norma exige la implementación de sistemas de verificación etaria, invalidando la autodeclaración de edad (Brasil, 2025a, art. 6, IV). Adicionalmente, la ley modifica la administración de perfiles de usuarios menores de 16 años en redes sociales, los cuales deben estar vinculados a sus padres o tutores legales (Brasil, 2025a, art. 24), ello permite la supervisión de tiempo de uso, la restricción de contactos, sistemas de recomendación personalizados y aplicaciones inadecuadas según la madurez o edad del menor.

Aunado a lo anterior, el marco de gobernanza y transparencia supervisado por la Autoridad Nacional de Protección de Datos (ANPD), que actúa como agencia reguladora autónoma y exige a las plataformas la elaboración de mapeos de riesgos, informes de impacto a la protección de datos específicos, y a las plataformas con más de un millón de usuarios infantojuveniles tienen la obligación de publicar informes periódicos detallados sobre moderación de contenido y evaluación de riesgos, además, garantiza el acceso controlado y gratuito de los datos tecnológicos para investigadores independientes con fines académicos, científicos o periodísticos, vedando investigación con fines comerciales (Brasil, 2025a, arts. 8 y 31).

Finalmente, el Decreto No 12.975 /2026 presenta una innovación legislativa, puesto que supera la regla general del Marco Civil da Internet de esperar por una orden judicial: si un contenido se configura como un delito penal evidente, como el *ciberbullying* tipificado en la ley 14.811 (Brasil, 2024b), la incitación al suicidio o la explotación sexual infantil, la plataforma tiene la obligación legal de removerlo o bloquearlo en un plazo de hasta 24 horas tras recibir una notificación válida, adicionalmente, el decreto introduce la responsabilidad por falla sistémica, si el algoritmo de una plataforma prioriza contenido ilícito, la empresa asume la responsabilidad administrativa civil por los daños (Brasil, 2026).

Estas disposiciones legales entregan herramientas operativas a las instituciones educativas. El modelo anterior creaba un vacío de protección, limitando la responsabilidad corporativa y dejando a las víctimas vulnerables frente a la lentitud judicial, con el nuevo marco, la infraestructura escolar se conecta con la regulación digital. Un caso de violencia detectado por el *Sistema Nacional de Acompanhamento e Combate à Violência nas Escolas* SNAVE (Brasil, 2024a), se traduce en una notificación a la plataforma, con la eliminación del contenido hasta en 24 horas se frena la exhibición pública del menor, detiene el daño psicológico continuo y reduce el riesgo de deserción escolar. Al exigir entornos digitales transparentes desde su programación, el ordenamiento jurídico reconoce que la tecnología es inseparable del ordenamiento jurídico y que debe operar bajo parámetros de seguridad eficaces.

Desafíos de ejecución del ECA digital en el espacio escolar.

La implementación del ECA Digital exige una reestructuración de procesos y responsabilidades en el ámbito educativo y familiar, las instituciones educativas requieren establecer canales interinstitucionales de prevención, atención y denuncia articulados con los órganos de control y el sistema de justicia. Asimismo, deben garantizar la formación y capacitación de su personal docente, administrativo, estudiantes y tutores legales, mediante la elaboración de protocolos claros y rutas de actuación (Santos *et al.*, 2026).

Entre los principales desafíos operativos para los centros educativos se encuentra la falta de control del diseño de las plataformas académicas y de redes sociales utilizadas por la comunidad escolar, incluidas herramientas informales como WhatsApp. Para mitigar esta vulnerabilidad, las escuelas pueden implementar un mapeo de datos los entornos digitales bajo su influencia, evaluándolos según la clasificación de riesgos del proyecto europeo *EU Kids Online* (Livingstone e Staksrud, 2014): contenido (adecuación de la información consumida según la edad), contacto (interacción con terceros y riesgo de acoso) conducta (fomento de ciberacoso, discurso de odio o retos peligrosos), contrato (términos de uso al ingresar a la plataforma) y comercio (recopilación y finalidad del tratamiento de datos personales) Este diagnóstico permite

estructurar medidas institucionales de prevención, capacitación y rutas de atención. Conviene precisar, en todo caso, los límites de esta responsabilidad institucional: al Estado corresponde el diseño y la actualización del marco normativo y la fiscalización de su cumplimiento por medio de la ANPD; a las plataformas digitales corresponde el deber de cuidado, la seguridad desde el diseño y la remoción de contenido ilícito en los plazos legales; a las familias corresponde la supervisión y el acompañamiento del uso que los menores hacen de los entornos digitales; y a las instituciones educativas corresponde, dentro de su ámbito de gobernanza, la prevención, la capacitación de su comunidad y la articulación con los demás actores, sin que ello implique el control integral de plataformas cuyo diseño no está bajo su administración.

La adopción de herramientas digitales en la educación exige un proceso de evaluación que puede ser guiado mediante la metodología *Child Rights Impact Assessment* (CRIA) que opera como un mecanismo de interoperabilidad y una herramienta de justicia de datos entre los proveedores tecnológicos y las instituciones educativas. En el ámbito corporativo, exige que las empresas desarrollen el software integrando limitaciones de extracción de datos y controles de riesgo desde la fase inicial (Mukherjee, Pothong e Livingstone, 2021). Por su parte, los centros educativos sumen el deber de utilizar esta matriz como filtro de auditoría empírica previo a su implementación pedagógica, con el objetivo de consolidar estándares operativos de seguridad (UNICEF, 2024). Finalmente, los centros académicos deben asegurar que las herramientas contratadas operen bajo el principio de privacidad por defecto, excluyendo algoritmos de retención o patrones adictivos (Brasil, 2025a).

En el mismo sentido, los centros educativos deben mitigar los riesgos asociados a la manipulación de contenidos generados mediante inteligencia artificial, para ello la captura y difusión de la imagen de los estudiantes requiere un documento de autorización específico, detallado e independiente del contrato general de matrícula. Este instrumento debe precisar si la finalidad es pedagógica, comercial o publicitaria. Como medida preventiva se sugiere priorizar registros fotográficos en contextos colectivos o a distancia, reduciendo el riesgo que la imagen individual de un menor sea extraída, descontextualizada o adulterada. Asimismo, la política institucional debe prohibir expresamente el uso de imágenes de los alumnos en las redes sociales particulares del cuerpo docente. La autorización concedida por los tutores legales se otorga de manera exclusiva a la institución educativa en su calidad de persona jurídica, excluyendo a los profesores como personas naturales, ello en estricta observancia de los artículos 17 y 18 del ECA Digital, relativos a la protección de la identidad y dignidad del menor (Brasil, 2025a).

Para coordinar la implementación de estas directrices, las instituciones deben estructurar un proceso continuo de capacitación y alfabetización digital dirigido a docentes, personal administrativo, estudiantes y tutores legales (Brasil, 2025a). Esta formación segmentada por grupos responde al mandato del artículo 70, inciso III de la Ley 8.069 de 1990, que exige la capacitación constante de los agentes educativos para prevenir e identificar la violencia (Brasil, 1990). Los programas deben instruir sobre los deberes de cuidado, las rutas de atención ante vulneraciones y los protocolos para el uso de canales de denuncia integrados por el *Conselho Tutelar*, el Ministerio Público y la *Autoridade Nacional de Proteção de Dados* (ANPD) en casos de actos tipificados como delito (Brasil, 2025a). Concurridamente, las escuelas deben designar delegados para la supervisión y respuesta ante incidentes cibernéticos, estableciendo reglas de cumplimiento normativo en plataformas de comunicación institucional y comunitaria, como por ejemplo WhatsApp, aunque no constituye un canal institucional, su uso

generalizado entre docentes y padres de familia exige la fijación de reglas mínimas para mitigar la exposición, prevenir el acoso y asegurar el respeto mutuo; Finalmente, la capacitación a las familias o tutores legales, deben incluir directrices de supervisión y control parental, restricción de acceso por edades y limitación de exposición pública de la rutina de los menores, consolidando así la aplicación de la norma en el entorno digital (Carvalho e Pereira, 2025).

Por consiguiente, la transmisión de las directrices institucionales debe ejecutarse de forma clara, concisa y adaptada a cada estamento de la comunidad educativa, asegurando su efectiva aplicación práctica. Estos principios legales, de ética y formación humana, se fundamenta en un mandato de corresponsabilidad que inicia en el entorno familiar y se refuerza en la institución educativa, bajo este esquema de corresponsabilidad, el Estado, las plataformas tecnológicas, los tutores legales y los estudiantes asumen deberes concurrentes y complementarios para atenuar riesgos y delitos asociados al entorno digital y a la inteligencia artificial. La finalidad de este esquema tripartito es consolidar un sistema de protección integral que preserve el ejercicio del derecho a la educación y establezca las bases necesarias para evitar la vulneración de cualquier otro derecho de los estudiantes (Brasil, 2025a).

Consideraciones finales

La violencia digital y el ciberacoso exceden los problemas convencionales de convivencia para constituirse como vulneraciones directas al derecho a la educación, en respuesta a esta flagrante problemática, la transición normativa materializada en el ECA Digital y en el Decreto 12.975/2026 reconfigura el modelo de protección, puesto que se abandona la dependencia del proceso judicial para la remoción de contenidos lesivos y exige a las plataformas tecnológicas obligaciones proactivas de diseño, mitigación de fallas en el sistema y la eliminación de material ilícito en un plazo de hasta 24 horas, lo cual detiene el daño psicológico y reduce el riesgo de exclusión escolar.

La implementación de este marco legal traslada también una parte de exigencias operativas y administrativas a las instituciones educativas, las cuales tienen la misión de organizar su capacidad técnica para articular la norma, y ejercer control sobre los entornos digitales, dentro de lo cual deben iniciar con un mapeo de riesgos que evalúe de manera exhaustiva el contenido, el contacto, la conducta, el contrato y el comercio dentro de las plataformas utilizadas por la comunidad escolar, asimismo se requiere la adopción de instrumentos de auditoría para estandarizar criterios y comprobar las barreras de seguridad antes de implementar herramientas digitales de apoyo pedagógico.

En el ámbito del tratamiento de datos personales y la exposición a riesgos contemporáneos derivados de la inteligencia artificial, las escuelas asumen la obligación de gestionar la información de los estudiantes bajo el principio legal de privacidad, para lo cual el uso de imagen de un alumno, deberá tener autorizaciones específicas, detalladas e independientes al contrato general de matrícula, ello con el fin de prevenir la extracción, descontextualización o adulteración de la identidad del alumno por medios tecnológicos.

Finalmente, la eficacia del ECA Digital demanda un ejercicio estructurado de corresponsabilidad entre el Estado, las plataformas tecnológicas, las instituciones educativas y las familias, asimismo requiere la creación de canales interinstitucionales de prevención y atención, la designación de delegados para la supervisión de incidentes cibernéticos y la integración en el currículo de programas de alfabetización digital, esta

articulação permitirá estruturar um sistema que assegure el ejercicio del derecho a la educación libre de violencia digital y provee las bases para evitar la vulneración de otras garantías de los menores.

Los hallazgos confirman, así, la hipótesis planteada en la introducción: la seguridad desde el diseño exigida a las plataformas es condición necesaria, pero no suficiente, de la protección del derecho a la educación; su eficacia depende de la capacidad administrativa y técnica que las instituciones de enseñanza logren organizar. Conviene reconocer, como límite de esta investigación, su carácter jurídico-dogmático y documental: no se midió empíricamente la capacidad instalada de las escuelas brasileñas para asumir tales cargas, en consideración a la reciente promulgación de la normativa. De ahí se desprende una agenda futura de estudios empíricos sobre la implementación del ECA Digital en las redes públicas y privadas de enseñanza, sobre la actuación fiscalizadora y sancionatoria de la ANPD y sobre la efectividad del plazo de remoción de veinticuatro horas como mecanismo de tutela del derecho a la educación.

REFERÊNCIAS BIBLIOGRÁFICAS

ANTONIO ORTEGA, Vanessa; TABORDA SERNA, Sergio Mauricio; PARRA BERMEJO, Jesús David. Cyberbullying: la nueva frontera de la violencia en Colombia. *Estudios y Perspectivas Revista Científica y Académica*, Ciudad de México, v. 4, n. 3, p. 3074-3114, 2024. DOI: 10.61384/r.c.a.v4i3.598. Disponível em: <https://estudiosyperspectivas.org/index.php/EstudiosyPerspectivas/article/view/598>. Acesso em: 12 jun. 2026.

BRASIL. Decreto nº 12.006, de 18 de abril de 2024a. Institui o Sistema Nacional de Acompanhamento e Combate à Violência nas Escolas e regulamenta a Lei nº 14.643, de 2 de agosto de 2023. *Diário Oficial da União*: seção 1, Brasília, DF, p. 3, 19 abr. 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/D12006.htm. Acesso em: 6 nov. 2025.

BRASIL. Decreto nº 12.975, de 20 de maio de 2026. Altera o Decreto nº 8.771, de 11 de maio de 2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014. *Diário Oficial da União*, Brasília, DF, 21 maio 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12975.htm. Acesso em: 26 maio 2026.

BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. *Relatório nacional: pesquisa internacional sobre ensino e aprendizagem: Talis 2018: segunda parte*. Brasília, DF: Inep, 2021. Disponível em: https://download.inep.gov.br/publicacoes/institucionais/estatisticas_e_indicadores/relatorio_nacional_pesquisa_internacional_sobre_ensino_e_aprendizagem_talis_2018_segunda_parte.pdf. Acesso em: 13 jul. 2026.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, p. 13563, 16 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 6 nov. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 set. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e

deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 mar. 2026.

BRASIL. Lei nº 13.185, de 6 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 9 nov. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 11 fev. 2026.

BRASIL. Lei nº 13.663, de 14 de maio de 2018a. Altera o art. 12 da Lei nº 9.394, de 20 de dezembro de 1996, para incluir a promoção de medidas de conscientização, de prevenção e de combate a todos os tipos de violência e a promoção da cultura de paz entre as incumbências dos estabelecimentos de ensino. *Diário Oficial da União*: seção 1, Brasília, DF, p. 2, 15 maio 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13663.htm. Acesso em: 6 nov. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018b. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 ago. 2026.

BRASIL. Lei nº 14.811, de 12 de janeiro de 2024b. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, institui a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), y 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos). *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 15 jan. 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm. Acesso em: 10 out. 2025.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025a. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). *Diário Oficial da União*, Brasília, DF, 18 set. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 11 mar. 2026.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 1.037.396/SC*. Relator: Ministro Dias Toffoli. Brasília, DF, 26 jun. 2025b. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em: 12 jun. 2026.

CARVALHO, Célia Regina de; PEREIRA, Talita Prado. A proteção dos direitos das crianças no ambiente digital: análise de postagens em redes sociais. *Revista Carioca de Ciência, Tecnologia e Educação*, Rio de Janeiro, v. 10, n. 2, p. 72-89, 2025. Disponível em: <https://recite.unicarioca.edu.br/rccte/index.php/rccte/article/view/356>. Acesso em: 14 mar. 2026.

FONDO DE LAS NACIONES UNIDAS PARA LA INFANCIA (UNICEF). *Developing global guidance for child rights impact assessments in relation to the digital environment*. Nueva York: UNICEF, 2024. Disponível em: <https://www.unicef.org/media/156046/file/Child%20Rights%20Impact%20Assessments%20in%20Relation%20to%20the%20Digital%20Environment.pdf>. Acesso em: 14 jul. 2026.

FONDO DE LAS NACIONES UNIDAS PARA LA INFANCIA (UNICEF) et al. *Disrupting Harm in Brazil: enfrentando a violência sexual contra crianças facilitada pela tecnologia*. [S. l.]: UNICEF,

2026. Disponível em: <https://www.unicef.org/brazil/relatorios/disrupting-harm-brazil-2026>. Acesso em: 14 jul. 2026.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). *Pesquisa nacional de saúde do escolar: 2019*. Rio de Janeiro: IBGE, 2021. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101852.pdf>. Acesso em: 13 ago. 2026.

LIVINGSTONE, Sonia; HADDON, Leslie. *EU Kids Online: final report*. London: LSE, 2009. Disponível em: https://eucpn.org/sites/default/files/document/files/5.eu_kids_online_final_report.pdf. Acesso em: 20 jul. 2026.

MUKHERJEE, S.; POTHONG, K.; LIVINGSTONE, S. *Child rights impact assessment: a tool to realise child rights in the digital environment*. London: Digital Futures Commission, 2021. Disponível em: https://eprints.lse.ac.uk/119727/1/Livingstone_child_rights_impact_assessment_published.pdf. Acesso em: 21 jul. 2026.

OFCOM. *Online Nation 2024 Report*. Londres: Ofcom, 2024. Disponível em: <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-nation/2024/online-nation-2024-report.pdf?v=386238>. Acesso em: 16 jul. 2026.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. *Protocolo Adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales "Protocolo de San Salvador"*. San Salvador: OEA, 1988. Disponível em: <https://www.oas.org/juridico/spanish/tratados/a-52.html>. Acesso em: 9 out. 2025.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Comité de los Derechos del Niño. *Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital*. Ginebra: ONU, 2021b. Disponível em: <https://www.ohchr.org/es/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>. Acesso em: 11 ago. 2026.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Comité de los Derechos del Niño; UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *Declaración conjunta sobre inteligencia artificial y los derechos del niño*. [S. l.]: ONU; UIT, 2025. Disponível em: <https://www.ohchr.org/sites/default/files/documents/hrbodies/crc/activities/2025-11-joint-stm-itu-crc-s.pdf>. Acesso em: 1 jun. 2026.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Convención sobre la eliminación de todas las formas de discriminación contra la mujer*. Nueva York: ONU, 1979. Disponível em: <https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women>. Acesso em: 9 out. 2025.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Convención sobre los Derechos del Niño*. Nueva York: ONU, 1989. Disponível em: <https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-rights-child>. Acesso em: 9 out. 2025.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. *La Declaración Universal de los Derechos Humanos*. [S. l.]: ONU, 10 dez. 1948. Disponível em: <https://www.un.org/es/about-us/universal-declaration-of-human-rights>. Acesso em: 12 nov. 2025.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. *ODS Objetivo 4: Garantizar una educación inclusiva, equitativa y de calidad y promover oportunidades de aprendizaje durante toda la vida para todos*. Nueva York: ONU, 2021a. Disponível em:

<https://www.un.org/sustainabledevelopment/es/education/>. Acesso em: 4 mai. 2026.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Pacto Internacional de Derechos Económicos, Sociales y Culturales*. Nueva York: ONU, 1966. Disponível em: <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>. Acesso em: 9 out. 2025.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Comité Interamericano contra el Terrorismo (CICTE). *La violencia de género en línea contra las mujeres y niñas: guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*. Washington, D.C.: OEA, 2022. Disponível em: <https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf>. Acesso em: 11 mar. 2026.

PINHO DE OLIVEIRA, María Fátima. Del Bullying al Cyberbullying: una mirada reflexiva. *Ciencia e Interculturalidad*, [S. l.], v. 33, n. 2, p. 132-148, 2023. DOI: 10.5377/rci.v33i2.17719. Disponível em: <https://www.camjol.info/index.php/RCI/article/view/17719>. Acesso em: 12 jul. 2026.

PURIFICAÇÃO, Ana Cristina Silva da; CERQUEIRA, Fernanda Maria Costa. Bullying e cyberbullying à luz do artigo 146-A no Código Penal Brasileiro. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, [S. l.], v. 11, n. 3, p. 1883-1906, 2025. DOI: 10.51891/rease.v11i3.18520. Disponível em: <https://periodicorease.pro.br/rease/article/view/18520>. Acesso em: 13 jul. 2026.

REINO UNIDO. *Online Safety Act 2023*. 2023 c. 50. Londres: The National Archives, 2023. Disponível em: <https://www.legislation.gov.uk/ukpga/2023/50/contents>. Acesso em: 11 mar. 2026.

SANTOS, Emilly Victória Batista dos et al. Proteção de crianças e adolescentes no ambiente digital: desafios e limites do Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025). *Revista Tópicos*, Rio de Janeiro, v. 4, n. 31, p. 1-28, 2026. DOI: 10.70773/revistatopicos/773301671. Disponível em: <https://revistatopicos.com.br/artigos/protecao-de-criancas-e-adolescentes-no-ambiente-digital-desafios-e-limites-do-estatuto-digital-da-crianca-e-do-adolescente-lei-n-15-211-2025>. Acesso em: 12 jul. 2026.

SANTOS, José Leonardo Diniz de Melo et al. O impacto das fake news no cyberbullying escolar: a desinformação como ferramenta de violência digital na educação. In: *Open Science Research XVIII*. [S. l.]: Editora Científica Digital, 2025. cap. 35, p. 506-517. DOI: 10.37885/250218825. Disponível em: <https://downloads.editoracientifica.com.br/articles/250218825.pdf>. Acesso em: 13 jun. 2026.

SILVA, Elane Moraes da et al. Bullying escolar e o sistema legal brasileiro: uma história de desafios e avanços legislativos. *Research, Society and Development*, [S. l.], v. 14, n. 1, p. e0614147925, 2025. DOI: 10.33448/rsd-v14i1.47925. Disponível em: https://www.researchgate.net/publication/387784939_Bullying_escolar_e_o_sistema_legal_brasileiro_Uma_historia_de_desafios_e_avancos_legislativos. Acesso em: 12 jun. 2026.

TOKUNAGA, Robert S. Following you home from school: a critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, [S. l.], v. 26, n. 3, p. 277-287, 2010. DOI: 10.1016/j.chb.2009.11.014. Disponível em: <https://www.sciencedirect.com/science/article/pii/S074756320900185X>. Acesso em: 12 jun. 2026.

UNIÓN EUROPEA. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). *Diario Oficial de la Unión Europea*, [S. l.], L 277, p. 1-102, 27 oct. 2022. Disponível em: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81573>. Acesso em: 12 jul. 2026.

Data de Recebimento: (O editor preenche a data).

Data de Aprovação: (O editor preenche a data).