

**DA PREVENÇÃO À COMPOSIÇÃO DE DANOS NA
INTIMIDAÇÃO SISTEMÁTICA: UMA ANÁLISE DA
RESPONSABILIDADE CIVIL A PARTIR DO *CYBERBULLYING*
PRATICADO COM O USO DA INTELIGÊNCIA ARTIFICIAL**

**FROM PREVENTION TO DAMAGE MITIGATION IN
SYSTEMATIC INTIMIDATION: AN ANALYSIS OF CIVIL
LIABILITY IN CASES OF *CYBERBULLYING* CARRIED OUT
USING ARTIFICIAL INTELLIGENCE**

**DE LA PREVENCIÓN A LA MITIGACIÓN DE DAÑOS EN LA
INTIMIDACIÓN SISTEMÁTICA: UN ANÁLISIS DE LA
RESPONSABILIDAD CIVIL A PARTIR DEL *CIBERACOSO*
REALIZADO CON EL USO DE INTELIGENCIA ARTIFICIAL**

Cleber Sanfelici Otero¹
João Gabriel Yaegashi²
Rubens Vasconcelos Calixto Neto³
Yago Felipe Bruchez Braga⁴

Resumo

O fenômeno do *cyberbullying* tem se intensificado com o avanço tecnológico, especialmente com o uso de ferramentas de inteligência artificial (IA), ampliando o alcance e impacto das agressões no ambiente escolar. A utilização de IA permite a criação de conteúdos intimidatórios personalizados e a disseminação automática de informações, aumentando o sofrimento das vítimas e dificultando a identificação dos responsáveis. Este artigo tem como objetivo analisar a responsabilidade civil dos provedores de aplicação de internet no contexto do *cyberbullying* escolar, considerando os novos desafios jurídicos trazidos pela participação de sistemas de IA nesse tipo de intimidação sistemática. Trata-se de uma pesquisa bibliográfica e documental, de abordagem dedutiva, que examina legislações, doutrinas e jurisprudências

¹Doutor em Direito Constitucional pela Instituição Toledo de Ensino. Docente do Programa de Pós-Graduação em Ciências Jurídicas da Universidade Cesumar (UNICESUMAR), na linha Direitos da Personalidade e o seu alcance na contemporaneidade. Juiz Federal. Orcid: <https://orcid.org/0000-0001-6035-7835>. Lattes: <http://lattes.cnpq.br/7156277822751107>. E-mail: cleber.otero@unicesumar.edu.br

²Doutorando em Direito pela Universidade Cesumar (UNICESUMAR). Docente do Departamento de Direito Público e Processual da Universidade Estadual de Maringá (UEM). Advogado. Orcid: <https://orcid.org/0000-0002-6341-0942>. Lattes: <http://lattes.cnpq.br/9776553896356663>. E-mail: jgyaegashi@hotmail.com

³Bacharel em Direito pela Universidade Estadual de Maringá (UEM). Advogado. Orcid: <https://orcid.org/0009-0004-0661-9784>. Lattes: <http://lattes.cnpq.br/8880749345512345>. E-mail: rubensvcneto@gmail.com

⁴Graduando em Direito pela Universidade Estadual de Maringá (UEM). Orcid: <https://orcid.org/0009-0003-8441-084X>. Lattes: <http://lattes.cnpq.br/7354241198700823>. E-mail: yagobruchez@gmail.com

relevantes para compreender a aplicabilidade da responsabilidade civil em casos mediados pela tecnologia. As considerações finais destacam que, diante das complexidades trazidas pela IA, é essencial o desenvolvimento de uma abordagem normativa capaz de prevenir e mitigar os danos causados às vítimas, assegurando proteção no ambiente escolar.

Palavras-chave: Direitos da personalidade; Intimidação sistemática; Responsabilidade civil.

Abstract

The phenomenon of cyberbullying has intensified with technological advances, especially with the use of artificial intelligence (AI) tools, expanding the reach and impact of aggression within the school environment. AI enables the creation of personalized intimidating content and the automated dissemination of information, increasing victims' suffering and complicating the identification of those responsible. This article aims to analyze civil liability of internet application providers within the context of school cyberbullying, considering the new legal challenges posed by the involvement of AI systems in this type of systematic intimidation. This is a bibliographic and documentary research, with a deductive approach, which examines relevant legislation, doctrines and jurisprudence to understand the applicability of civil liability in cases mediated by technology. The final considerations emphasize that, given the complexities brought by AI, it is essential to develop a regulatory approach capable of preventing and mitigating the harm caused to victims, ensuring protection within the school environment.

Keywords: Personality rights; Systematic intimidation; Civil liability.

Resumen

El fenómeno del ciberacoso se ha intensificado con los avances tecnológicos, especialmente con el uso de herramientas de inteligencia artificial (IA), ampliando el alcance e impacto de las agresiones en el entorno escolar. La IA permite la creación de contenidos intimidatorios personalizados y la difusión automática de información, aumentando el sufrimiento de las víctimas y dificultando la identificación de los responsables. Este artículo tiene como objetivo analizar la responsabilidad civil de los proveedores de aplicaciones de internet en el contexto del ciberacoso escolar, considerando los nuevos desafíos legales que plantea la participación de sistemas de IA en este tipo de intimidación sistemática. Se trata de una investigación bibliográfica y documental, con enfoque deductivo, que examina la legislación, doctrina y jurisprudencia relevante para comprender la aplicabilidad de la responsabilidad civil en casos mediados por tecnología. Las consideraciones finales destacan que, dadas las complejidades introducidas por la IA, es esencial desarrollar un enfoque normativo capaz de prevenir y mitigar el daño causado a las víctimas, garantizando protección en el entorno escolar.

Palabras clave: Derechos de la personalidad; Intimidación sistemática; Responsabilidad civil.

Introdução

A rápida evolução tecnológica tem impulsionado o surgimento de novas formas de interação social e, com isso, de novos desafios relacionados à segurança e ao bem-estar no ambiente digital. No contexto escolar, o fenômeno do *cyberbullying* tem se intensificado com o uso de ferramentas de inteligência artificial (IA), o que amplia o alcance e a intensidade das agressões, muitas vezes dificultando a identificação e responsabilização dos envolvidos.

Nesse sentido, coloca-se em discussão a responsabilidade dos provedores de internet, redes sociais e plataformas de conteúdo, uma vez que estes precisam adotar políticas eficazes para impedir que conteúdos prejudiciais circulem na rede de modo

desenfreado, a fim de proteger os usuários das consequências advindas da malversação tecnológica. Posto isso, este estudo procurou responder à seguinte problemática: qual a responsabilidade civil dos provedores de aplicação de internet para com o tratamento do *cyberbullying* escolar?

O objetivo geral deste estudo consiste em analisar a responsabilidade civil dos provedores de aplicação de internet no contexto do *cyberbullying* escolar, considerando os novos desafios jurídicos trazidos pela participação de sistemas de IA nesse tipo de intimidação sistemática. Especificamente, pretende-se: a) analisar a responsabilidade do ambiente escolar frente aos danos provocados pelo uso de IA para *cyberbullying*; b) compreender os impactos da intimidação sistemática no desenvolvimento da personalidade dos jovens; e c) examinar as estratégias de prevenção e reparação de danos no contexto digital, com ênfase na responsabilidade civil.

A justificativa para a elaboração deste estudo reside na crescente relevância do tema diante da integração das tecnologias de IA no cotidiano, inclusive na vida escolar, onde as consequências do *cyberbullying* afetam diretamente o desenvolvimento psicossocial dos estudantes. A responsabilidade civil apresenta-se como um importante instrumento de proteção e reparação para as vítimas, exigindo adaptações para lidar com as especificidades da IA.

A metodologia utilizada baseia-se em uma revisão bibliográfica e documental, por meio da análise de legislação, doutrina e jurisprudência relacionadas ao tema. O método de investigação será o dedutivo, cujo processo de análise utiliza o raciocínio lógico e a dedução para obter uma conclusão a respeito de um determinado assunto. No caso específico deste estudo, discutiremos o caso noticiado pelo portal G1, no qual a Inteligência Artificial (IA) foi utilizada para simular imagens pornográficas de uma professora e colegas de sala em uma escola particular de Cuiabá/MT.

O artigo está estruturado em três seções. A primeira seção abordará a responsabilidade no ambiente escolar, destacando os novos danos resultantes do uso da IA para a prática do *cyberbullying*. A segunda seção explorará a intimidação sistemática e os seus impactos no desenvolvimento da personalidade dos jovens. Por fim, a terceira seção examinará a responsabilidade civil no contexto digital, discutindo as práticas de

prevenção e reparação de danos causados pelo *cyberbullying* com o auxílio da IA. Essa estrutura visa proporcionar uma análise abrangente das questões legais, psicológicas e preventivas envolvidas na temática.

Responsabilidade no ambiente escolar: a aplicação da inteligência artificial para a prática do *cyberbullying*

Em junho do corrente ano de 2024, veiculou-se nos canais de informação um preocupante caso, no qual o uso da IA foi determinante para a prática do *cyberbullying* em uma escola particular de Cuiabá/MT. O caso culminou com a expulsão de quatro alunos em razão do emprego da IA para criar nudes falsos, com a inserção dos rostos das vítimas em corpos alheios, especificamente, de uma professora e colegas de sala, divulgando-se as imagens em grupos de pornografia nas redes sociais. Segundo a Associação SOS Bullying, que acompanhou o caso, as imagens continuaram sendo divulgadas por meio de conversas e publicações *on-line* no mês de agosto, culminando com a exposição de mais de 30 jovens com as imagens falsas (G1, 2024).

A prática do *cyberbullying* não é incomum à realidade escolar brasileira. Em uma pesquisa conduzida pelo instituto Ipsos para identificar os países com maior frequência de casos de *cyberbullying* no mundo, o Brasil ocupou o segundo lugar, ficando atrás apenas da Índia. O estudo apontou que a maioria dos casos envolve a divulgação não consentida de imagens íntimas (Lima, 2019). Essa forma de exposição virtual permite a disseminação de informações da vítima de maneira rápida, contínua e em escala potencialmente ilimitada (Oliveira, Lourenço & Senra, 2015). O que merece especial análise, no presente momento, é a nova ferramenta de criação e desenvolvimento muitas vezes indiscriminadamente disponibilizada para a prática de tais atos, a IA, cuja definição e análise mais aprofundada será realizada na terceira seção.

As relações sociais estão cada vez mais alicerçadas nos ambientes virtuais. O avanço tecnológico tem proporcionado transformações significativas na cultura da

sociedade, impulsionando a expansão dos ciberespaços⁵. Exemplos como o acesso facilitado à educação a distância, a ampliação de redes de solidariedade em plataformas sociais e a inovação em serviços de saúde, como a telemedicina, destacam como a tecnologia tem contribuído para a melhoria da qualidade de vida. Além disso, a conectividade global permite a troca de conhecimentos e o fortalecimento de vínculos familiares e sociais, mesmo à distância. No entanto, apesar dessas conquistas, os ciberespaços também podem ser palco de práticas prejudiciais, especialmente para crianças e adolescentes. Esses ambientes, que oferecem anonimato e ampla disseminação de informações, tornam-se propícios para a perpetração de violências *online*, como o *cyberbullying*, expondo vulnerabilidades e facilitando a realização de atividades ultrajantes. Assim, enquanto a tecnologia avança como uma aliada no desenvolvimento humano, também exige atenção e responsabilidade no uso das plataformas digitais.

Em um curto intervalo de tempo, a sociedade passou a incorporar e aplicar mecanismos de automação em praticamente todos os setores, resultado da chamada revolução das Tecnologias da Informação e Comunicação (TICs). Vale destacar que a “tecnologia” não se restringe aos recursos informáticos, que representam apenas um ramo – embora o mais destacado – desse vasto campo. A tecnologia, por sua vez, é um processo que acompanha o ser humano desde o início de sua existência, sendo um dos fatores que o diferenciam dos demais seres vivos. Ela abrange desde processos de gestão e controle até materiais físicos, variando de ferramentas simples a equipamentos sofisticados, como computadores (Galdino *et al.* 2013). Por outro lado, a “técnica” refere-se ao conjunto de ações humanas sobre a natureza, cujo objetivo é aprimorar instrumentos que satisfaçam suas necessidades. A organização e sistematização dessas ações constituem a “tecnologia”, entendida como o estado da técnica em determinado

⁵ O ciberespaço se caracteriza pela convergência digital consubstanciada na integração de diversos formatos e dispositivos em um mesmo “lugar”, ou seja, trata-se de um espaço conceitual inserido no ambiente das TICs. Assim, dada a continuidade dos avanços tecnológicos, atualmente o ciberespaço não pode ser visto tão somente como um espaço de interconexão de computadores, mas sim em todas as suas variações como tablets, smartphones, laptops, vídeo games, smartvts etc., tornando uma característica desse espaço a multidisciplinariedade (Lehfeld *et al.* 2021, p. 241).

período histórico (Doneda, 2020). Assim, a tecnologia não deve ser vista como um fim em si mesma, mas como um meio que promove o aprimoramento de bens e serviços.

A integração da telefonia com a computação, iniciada na década de 1980, resultou em uma ampla disseminação da informática ao redor do mundo. Esse avanço foi marcado pela interconexão em redes de conexão e interação, estabelecendo uma nova base material para a execução de atividades em toda a estrutura social (Castells, 2020). Desde então, as TICs têm sido implementadas em uma ampla variedade de atividades, promovendo uma conexão universal que ultrapassa fronteiras e aproxima indivíduos globalmente. No século XXI, a vida cotidiana é amplamente monitorada e influenciada por dispositivos eletrônicos e algoritmos, tornando a onipresença da tecnologia uma das características mais distintivas da sociedade da informação (Wimmer, 2019). Nesse contexto, Sarlet (2021) destaca o impacto significativo das TICs em áreas cruciais da vida contemporânea, como os campos social, econômico, político e cultural, caracterizando o fenômeno conhecido como *ubiquitous computing*, no qual a tecnologia permeia praticamente todas as esferas da existência humana.

As gerações atuais e futuras, diferentemente daqueles que nasceram antes da década de 1990, são consideradas nativas digitais. Isso significa que essas pessoas cresceram em um ambiente amplamente influenciado por recursos tecnológicos, absorvendo-os, compreendendo-os e utilizando-os com naturalidade e preferência, como uma extensão de sua linguagem cotidiana (Prensky, 2001). Essa familiaridade da juventude com a tecnologia no Brasil é evidenciada pela pesquisa “TIC Kids Online Brasil 2019”, conduzida pelo Comitê Gestor da Internet no Brasil (CGI.br), que revelou que 89% das crianças e adolescentes entre 9 e 17 anos têm acesso à internet. Esses jovens utilizam dispositivos diversos, como *smartphones* (95%), televisores (45%), computadores (38%) e videogames (18%) para acessar o ambiente digital (CETIC, 2020). No entanto, a familiaridade com a tecnologia não deve ser confundida com proficiência ou segurança no uso das TICs. Muitas crianças e adolescentes não compreendem plenamente a relação de causa e efeito associada a essas ferramentas, o que os expõe a riscos. O uso acrítico dessas tecnologias é frequentemente comparado ao

aprendizado básico de leitura: dominar o alfabeto confirma a alfabetização, mas não garante uma capacidade crítica de interpretação (Henriques, Pita & Hartung, 2021).

Dada a difusão tecnológica e a sua influência nas relações sociais, importa refletir acerca do seu uso no âmbito escolar e, sobretudo, no que diz respeito à conscientização necessária da eventual malversação desses mesmos recursos pelas pessoas inseridas nesse ambiente, vez que os seus interlocutores, em se tratando de crianças e adolescentes, representam pessoas em especial estágio de desenvolvimento, no qual ocorrem os primeiros traços do desenvolvimento da personalidade (Jung, 2011), carecendo de plena capacidade de compreensão, tampouco defesa, das influências e danos aos quais estão suscetíveis em meio à ubiquidade das TICs (Henriques, Pita & Hartung, 2021).

Dada a progressão tecnológica e o constante emprego de novos recursos para o *cyberbullying*, a intimidação sistemática, enquanto prática ilícita, deve ser considerada uma manifestação dos chamados "novos danos". Esses novos danos surgem das complexidades da sociedade e da ampliação da proteção aos direitos existenciais, sendo distintos dos danos tradicionalmente abordados pelo ordenamento jurídico. Eles resultam de um processo de reconhecimento gradual, uma vez que, em períodos anteriores, eram desconsiderados pela legislação ou, quando pleiteados, sua reparação era negada devido à simplificação das concepções jurídicas da época (Schreiber, 2013). Esses novos danos refletem a proteção dos direitos da personalidade, abrangendo o aspecto existencial, cuja ressarcibilidade tem sido progressivamente acolhida pela doutrina e pela jurisprudência.

No caso da intimidação sistemática, há tempos abordada de forma expressa em programas de combate pela legislação brasileira (Lei nº 13.185, 2015), impende destacar que não se trata de fenômeno superado e tampouco trivial aos olhos do Estado. O evento acima destacado é de especial relevância pois utiliza de novo recurso para a prática do *cyberbullying*, e o faz justamente no mesmo ano em que sancionada a Lei nº 14.811 (2024), para o recrudescimento do tratamento do fenômeno no âmbito educacional.

Frente ao caso preambularmente destacado, há de se analisar a responsabilidade

aplicável aos provedores de aplicação de internet para a prevenção e reparação dos danos derivados desta conduta ilícita, perpassando, necessariamente, pelos impactos ocasionados no desenvolvimento da personalidade das crianças e adolescentes envolvidos no ambiente escolar e, por fim, na responsabilidade civil aplicável a esse contexto.

Intimidação sistemática e os seus impactos no desenvolvimento da personalidade

O avanço das tecnologias e o uso das inteligências artificiais trouxe ao mundo moderno uma nova preocupação ao fenômeno conhecido como *cyberbullying*. A etimologia do termo empregado remete-se ao prefixo “*cyber*”, tratando-se de uma prática ocorrida nos ambientes virtuais, em plataformas de comunicação e informação, e radical “*bullying*”, sem tradução na língua portuguesa, mas compreendido como a perseguição e intimidação sistemática direcionada à vítima. Nesse sentido, “*cyberbullying*”, conforme Smith *et al* (2008), é assim conceituado:

Uma definição correspondente de *cyberbullying* é: ‘Um ato agressivo e intencional realizado por um grupo ou indivíduo, usando formas eletrônicas de contato, repetidamente e ao longo do tempo contra uma vítima que não pode se defender facilmente’ (Smith *et al*, 2008, p. 376, tradução nossa)⁶.

Tal definição, na verdade, foi adaptada ao tradicional conceito de “*bullying*”, qual seja, a conduta agressiva e intencional praticada por um grupo ou indivíduo de forma reiterada e contínua contra uma vítima que não possui os meios necessários à sua defesa (Olweus, 1993). O citado autor, percussor das pesquisas acerca do tema, continua:

Qualquer aluno está sendo intimidado ou vitimizado quando é exposto, repetidamente e ao longo do tempo, a ações negativas por parte de um ou mais outros alunos”, e segue três critérios: “(a) É comportamento agressivo ou “causar dano” intencional (b) que é

⁶ A corresponding definition of cyberbullying is: ‘An aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself’ (Smith *et al*, 2008, p. 376).

realizado “repetidamente e ao longo do tempo” (c) em um relacionamento interpessoal caracterizado por um desequilíbrio de poder” (Olweus, 1993, p. 1173, tradução nossa)⁷.

Os conceitos mencionados foram incorporados à conceituação legal dada pela Lei nº 13.185 (2015), que Institui o Programa de Combate à Intimidação Sistemática (*Bullying*) e o define, em ambas as modalidades, nos seus artigos inaugurais:

[...] § 1º No contexto e para os fins desta Lei, considera-se intimidação sistemática (*bullying*) todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas. [...]

Art. 2º Caracteriza-se a intimidação sistemática (*bullying*) quando há violência física ou psicológica em atos de intimidação, humilhação ou discriminação e, ainda:

- I - ataques físicos;
- II - insultos pessoais;
- III - comentários sistemáticos e apelidos pejorativos;
- IV - ameaças por quaisquer meios;
- V - grafites depreciativos;
- VI - expressões preconceituosas;
- VII - isolamento social consciente e premeditado;
- VIII – pilhérias.

Parágrafo único. Há intimidação sistemática na rede mundial de computadores (*cyberbullying*), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial (Lei nº 13.185, 2015).

A violência nas escolas pode ocorrer diretamente ou indiretamente. Nesta, incluem-se ações como o *cyberbullying*, rumores, fofocas e exclusão social, ao passo que, naquela, demonstrações físicas ou verbais, como socos, chutes, insultos e ameaças, que tendem a acontecer concomitantemente (Bohn & Hickey, 2010). Deste modo, se, por um lado, são características do “*bullying*” a prática contínua e reiterada de práticas intimidatórias e violentas nos espaços coletivos, de outro norte, soma-se ao “*cyberbullying*” o potencial anonimato, a audiência ilimitada, e a preponderante prática

⁷ Any student is being bullied or victimized when he or she is exposed, repeatedly and over time, to negative actions on the part of one or more other students,” and follows three criteria: “(a) It is aggressive behavior or intentional “harm doing” (b) which is carried out “repeatedly and over time” (c) in an interpersonal relationship characterized by an imbalance of power” (Olweus, 1993, p. 1173).

de assédio sexual e homofóbico com o uso de ferramentas de comunicação social (Shariff, 2009).

A intimidação sistemática virtual, sobretudo no contexto escolar, traz profundos impactos no desenvolvimento das personalidades das crianças e dos adolescentes, afinal, a vítima, que, decorrente do *cyberbullying*, passa a apresentar os sintomas negativos da prática, como ansiedade, depressão, *stress*, medo, frustração, dentre vários outros (Garaigordobil & Oñederra, 2010), tende a tornar-se mais reservada e com baixa autoestima, na medida que, considerando as ações hostis agora sofridas de forma remota, não possui espaço seguro para lidar e evitar com estas agressões, sentindo-se incapaz de encontrar alternativas frente a situação vivida (Yaegashi & Otero, 2023).

Do outro lado, ainda que severas as consequências à formação da personalidade das vítimas, importa destacar que a intimidação sistemática é nociva para todos os atores nas relações escolares, incluindo-se os próprios agressores, que, ao engajarem nessa relação de violência, passam a experimentar uma série de danos psicológicos, sociais e legais, com repercussões a longo prazo para sua formação e desenvolvimento, quais sejam, falta de empatia, problemas com álcool e/ou outras drogas, queda de rendimento acadêmico e comportamento antissocial criminoso (Garaigordobil & Oñederra, 2010).

O *cyberbullying*, com o advento da IA e maior acesso da população, no geral, à Internet, tornou-se questão de fundamental importância no mundo moderno, vez que estes mecanismos contribuem para uma maior facilidade e escala das agressões. Segundo postula Guimarães (2022):

O desenvolvimento e crescente uso dos meios tecnológicos que deixam “pegadas eletrônicas” tornam cada vez mais importantes as garantias contra o tratamento e a utilização abusiva de dados pessoais informatizados. A sua relação de tensão com vários direitos, liberdades e garantias – tais como o desenvolvimento da personalidade, a dignidade da pessoa, a intimidade da vida privada – é inquestionável (Guimarães, 2022, p. 106).

Deste modo, o ambiente digital, em que pese as vantagens já anunciadas, transformou-se ao mesmo tempo em um espaço rico à proliferação duradoura de

práticas abusivas, afetando de forma direta o desenvolvimento da personalidade das crianças e adolescentes. Frente a essa realidade, exige-se uma reflexão acerca do enfrentamento e prevenção do uso indiscriminado dessas tecnologias, o que passa pela necessária compreensão dos impactos que tais violências têm no pleno desenvolvimento das pessoas inseridas no espaço escolar, que são profundamente influenciados na formação de suas personalidades, habilidades e autoestima, gerando consequências a curto e longo prazo, senão permanentes.

O direito ao livre desenvolvimento da personalidade, embora não contido na Constituição, possui previsão expressa no art. 1º da Lei nº 13.709 (2018), Lei Geral de Proteção de Dados Pessoais (LGPD), *in verbis*:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Lei nº 13.709, 2018).

O livre desenvolvimento da personalidade, preambularmente citado, é o instituto que garante a autonomia de constituir uma personalidade plena, com respeito à individualidade e liberta de pressões do meio exterior. Miranda (2013, p. 11178-11179) leciona que “esse direito está contido no rol dos direitos de liberdade e emana um conteúdo positivo, na liberdade de agir, e um conteúdo negativo, na não interferência ou nos impedimentos.”

O *cyberbullying* é uma modalidade de *bullying* e, portanto, culminante em danos de ordem psicológica aos ofendidos. Ainda que prescindida de motivação, a intimidação sistemática tem por causa fatores de ordem social, cultural, psicológico e, não raro, estrutural. Acertadamente, Fante (2005) expõe que a escola não é capaz de plenamente frear a influência de fatores externos sobre seus alunos, de modo que esta passa a ser palco para diversas manifestações de violência. Deste modo, é necessário que agentes externos, como os próprios provedores de aplicação e família, sejam chamados à responsabilidade de cooperar com a prevenção e repressão destas práticas danosas.

Ante o exposto, é fundamental que a intimidação sistemática, sobretudo o *cyberbullying*, seja reconhecida como uma forma de diretamente impactar o desenvolvimento da personalidade de crianças e adolescentes, vítimas ou agressoras, na medida que esta prática mina a formação de sua autoestima, confiança, além de diversos outros malefícios para, frisa-se, ambos. Os desajustes comportamentais e psicológicos, inexoravelmente, afetam e maculam o desenvolvimento saudável esperado dos menores, sendo certo que a exposição contínua à humilhação ou violência interferem na construção de relações interpessoais, resultando, futuramente, em adultos psicologicamente quebrados, com exacerbados impasses no tocante ao estabelecimento de vínculos ou na forma de lidar com adversidades.

Responsabilidade civil no contexto digital: da prevenção à reparação de danos pelo *cyberbullying* praticado com o auxílio da inteligência artificial

O fenômeno do *cyberbullying* emergiu como uma das questões mais urgentes da sociedade contemporânea ao se pensar nas relações escolares, o que se deve ao impulsionamento dado pela revolução digital e pela ampla disseminação das tecnologias da informação. Ao contrário do bullying tradicional, que ocorre em ambientes físicos e, portanto, está sujeito a limitações de tempo e espaço, o *cyberbullying* transcende essas barreiras e ganha proporções globais, perpetuando-se no ciberespaço, ambiente no qual os danos causados podem ser profundos e duradouros, afetando não apenas a saúde mental das vítimas, mas também sua reputação e integridade social.

Este cenário exige uma resposta eficaz, que passe necessariamente pela adaptação do sistema jurídico a uma realidade na qual as interações digitais desempenham um papel central na vida das pessoas. A responsabilidade civil, nesse contexto, não pode ser vista apenas como uma ferramenta para reparar danos após sua ocorrência, mas também como um mecanismo preventivo que visa evitar que estes ocorram em primeiro lugar. O conceito de *answerability*, ou explicabilidade, surge como uma das peças-chave dessa discussão. Como destacado por Rosenvald e Faleiros Júnior (2023), a explicabilidade não se limita a saber qual tecnologia ou IA está sendo utilizada, mas envolve uma obrigação mais ampla de fornecer explicações claras e

justificativas para as decisões e ações tomadas por sistemas algorítmicos, especialmente quando essas ações afetam os direitos fundamentais das pessoas.

A explicabilidade tem um papel central na responsabilização de provedores de serviços digitais, como plataformas de redes sociais, que, por meio de seus algoritmos, gerenciam e amplificam o conteúdo que circula em seus espaços. Se esses sistemas não são suficientemente transparentes e auditáveis, torna-se impossível responsabilizar aqueles que projetam ou controlam essas tecnologias, deixando as vítimas de *cyberbullying* à mercê de um sistema que pode amplificar e perpetuar suas agressões sem qualquer controle. Esse vácuo de responsabilidade é o que torna a discussão sobre *answerability* tão urgente. Pasquale (2017), um dos principais defensores do conceito de explicabilidade, propôs que a responsabilidade não deve ser apenas sobre o ato concreto, mas também sobre o fornecimento claro das razões para a sua prática. Em sua obra, defende-se a necessidade de estabelecer uma relação mais transparente entre os operadores de IA e os usuários, especialmente para garantir que os sistemas algorítmicos não ajam de maneira imprevista ou prejudicial aos indivíduos.

O papel da responsabilidade civil, portanto, vai além da compensação de danos; ela deve atuar de maneira preventiva e precaucional, antecipando os riscos e buscando mitigar as consequências antes que elas se materializem. A função preventiva da responsabilidade civil está relacionada ao dever de os provedores de serviços digitais adotarem políticas eficazes para impedir que conteúdos prejudiciais (Rosenvald & Faleiros Júnior, 2023), como aqueles que fomentam o ódio e o *bullying*, sejam disseminados em suas plataformas. Ao mesmo tempo, a função precaucional entra em cena quando o risco não é totalmente previsível, mas as tecnologias em questão apresentam potencial para causar danos significativos (Barbosa, 2006). Nesse sentido, a responsabilidade civil deve ser capaz de agir mesmo diante de incertezas, implementando mecanismos que reduzam ao máximo a possibilidade de dano.

A responsabilidade dos provedores de serviços de internet e redes sociais se estende à necessidade de regular o conteúdo disseminado por meio de seus algoritmos. Eles não podem ser considerados apenas intermediários passivos. De acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Regulamentação Geral de Proteção de

Dados (GDPR) da União Europeia, as plataformas digitais devem garantir não apenas a proteção dos dados pessoais, mas também a transparência sobre como esses dados são usados para decisões automatizadas. O direito à explicação (*right to an explanation*), que assegura ao usuário o direito de contestar decisões baseadas exclusivamente em processamento automatizado, é uma das principais ferramentas para garantir que as decisões algorítmicas possam ser auditadas e justificadas.

A moderação de conteúdo, especialmente em plataformas de redes sociais, é uma das formas mais claras de aplicação dessa responsabilidade. As redes sociais, por exemplo, têm o poder de amplificar conteúdos negativos, como discursos de ódio, informações falsas e, claro, casos de *cyberbullying*. O algoritmo dessas plataformas tende a priorizar conteúdos que gerem mais engajamento, o que frequentemente inclui publicações polarizadoras e provocativas. Portanto, é fundamental que os desenvolvedores e operadores dessas plataformas assumam uma responsabilidade ativa em impedir que seus sistemas alimentem ou amplifiquem comportamentos prejudiciais.

A supervisão humana e a transparência são elementos cruciais para garantir que os algoritmos não contribuam para o agravamento de problemas como o *cyberbullying*. O modelo de supervisão implica que decisões automatizadas não sejam tomadas sem a possibilidade de revisão humana. Isso garante que, em casos de impactos significativos sobre os direitos dos indivíduos, as plataformas possam fornecer explicações e justificativas adequadas. Como Coeckelbergh (2020) sugere, a responsabilidade não se resume a agir corretamente, mas também em poder dar razões para essas ações. Isso implica que, ao lidar com tecnologias que afetam diretamente as vidas das pessoas, especialmente na internet, os desenvolvedores de IA e as plataformas digitais devem ser capazes de fornecer uma justificativa robusta para suas decisões, demonstrando que estas não apenas são funcionais, mas também éticas e responsáveis.

Em termos legais, diferentemente de outros prestadores de serviços no Brasil, os provedores de aplicação de internet não possuem responsabilidade objetiva pelos danos decorrentes de conteúdos gerados por terceiros em suas plataformas, conforme se extrai do art. 18 do Marco Civil da Internet – MCI (Lei nº 12.965, 2014). Sua responsabilidade é apenas culposa e ocorre quando, após notificação por ordem judicial específica, não

adotarem as providências necessárias para, dentro dos limites técnicos de seu serviço e no prazo estipulado, tornar indisponível o conteúdo considerado infringente, nos termos do art. 19, MCI. Embora a possibilidade de retirada de conteúdo danoso constitua uma importante medida inibitória, a forma como é regulamentada pelo ordenamento jurídico suscita questionamentos quanto à sua constitucionalidade, pois desobriga os provedores, dentro de suas capacidades técnicas, de responderem civilmente por falhas na segurança e eficiência no controle e compartilhamento prévio do conteúdo em suas plataformas.

No modelo vigente, com exceção de conteúdos que envolvam cenas de nudez ou atos sexuais de caráter privado, para os quais é permitida a responsabilidade subsidiária caso o provedor não os remova de forma diligente após uma mera notificação extrajudicial - conforme disciplina o art. 21, MCI -, os demais conteúdos disponíveis na rede, mesmo aqueles que atentem contra a personalidade, como no caso do *cyberbullying*, só poderão ser removidos, sob pena de responsabilização, mediante ordem judicial que identifique especificamente a URL do conteúdo a ser excluído. Essa exigência não se aplica a conteúdos similares, ainda que possuam teor idêntico.

A constitucionalidade do art. 19, MCI é atualmente contestada, dada a fragilização de proteção que confere aos usuários das redes, no Tema nº 987 do Supremo Tribunal Federal. Ainda assim, a jurisprudência, dos tribunais têm caminhado para abrandar as hipóteses de responsabilidade para a tutela de grupos especialmente vulneráveis, como é o caso das crianças e adolescentes sujeitas às interações digitais. Nesse sentido, o Superior Tribunal de Justiça, atendendo ao *princípio do melhor interesse da criança e do adolescente*, reconhece que este grupo deve contar com proteção integral e prioridade de atendimento. O Estatuto da Criança e do Adolescente (ECA) (Lei nº 8.069, 1990), como um sistema de proteção especialíssimo, prevalece sobre a legislação que regula os serviços de informação prestados por provedores de internet. Assim, a omissão do provedor em remover o conteúdo, mesmo após notificação extrajudicial, configura uma conduta reprovável e passível de indenização:

DIREITO CIVIL, INFANTOJUVENIL E TELEMÁTICO. PROVEDOR DE APLICAÇÃO. REDE SOCIAL. DANOS MORAIS E À IMAGEM. PUBLICAÇÃO OFENSIVA. CONTEÚDO ENVOLVENDO MENOR DE IDADE. RETIRADA.

ORDEM JUDICIAL. DESNECESSIDADE. PROTEÇÃO INTEGRAL. DEVER DE TODA A SOCIEDADE. OMISSÃO RELEVANTE. RESPONSABILIDADE CIVIL CONFIGURADA. 1. O Estatuto da Criança e do Adolescente (art. 18) e a Constituição Federal (art. 227) impõem, como dever de toda a sociedade, zelar pela dignidade da criança e do adolescente, colocando-os a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão, com a finalidade, inclusive, de evitar qualquer tipo de tratamento vexatório ou constrangedor. 1.1. As leis protetivas do direito da infância e da adolescência possuem natureza especialíssima, pertencendo à categoria de diploma legal que se propaga por todas as demais normas, com a função de proteger sujeitos específicos, ainda que também estejam sob a tutela de outras leis especiais. 1.2. Para atender ao princípio da proteção integral consagrado no direito infanto-juvenil, é dever do provedor de aplicação na rede mundial de computadores (Internet) proceder à retirada de conteúdo envolvendo menor de idade – relacionado à acusação de que seu genitor havia praticado crimes de natureza sexual – logo após ser formalmente comunicado da publicação ofensiva, independentemente de ordem judicial. 2. O provedor de aplicação que, após notificado, nega-se a excluir publicação ofensiva envolvendo menor de idade, deve ser responsabilizado civilmente, cabendo impor-lhe o pagamento de indenização pelos danos morais causados à vítima da ofensa. 2.1. A responsabilidade civil, em tal circunstância, deve ser analisada sob o enfoque da relevante omissão de sua conduta, pois deixou de adotar providências que, indubitavelmente sob seu alcance, minimizariam os efeitos do ato danoso praticado por terceiro, o que era seu dever. 2.2. Nesses termos, afigura-se insuficiente a aplicação isolada do art. 19 da Lei Federal n. 12.965/2014, o qual, interpretado à luz do art. 5º, X, da Constituição Federal, não impede a responsabilização do provedor de serviços por outras formas de atos ilícitos, que não se limitam ao descumprimento da ordem judicial a que se refere o dispositivo da lei especial. 3. Recurso especial a que se nega provimento (STJ, 2022).

A decisão em análise representa um alento para as vítimas de *cyberbullying* escolar, especialmente por serem, em sua maioria, hipervulneráveis, devendo contar com a diligência e cautela das plataformas para prevenir e conter danos à sua personalidade. A falha em retirar o conteúdo prejudicial pode resultar em danos irreparáveis, tornando inadmissível que o provedor, que possui a obrigação de assegurar a qualidade e segurança de seus serviços e proteger seus usuários (particularmente os menores), deixe de adotar as medidas ao seu alcance para mitigar os efeitos do ato lesivo (Yaegashi & Otero, 2023).

A responsabilidade dos provedores não se limita a prevenir danos individuais, mas deve abranger uma dimensão mais ampla: a proteção da sociedade como um todo. Se uma plataforma digital ou um algoritmo contribui para o aumento do *cyberbullying* ou para a disseminação de conteúdo prejudicial, sua responsabilidade vai além de

reparar os danos causados à vítima imediata. Ela estende-se à proteção da integridade social, garantindo que o ambiente digital não seja um local onde abusos possam ser sistematicamente alimentados e espalhados. A supervisão mútua desempenha um papel complementar aos métodos regulatórios de governança (*accountability*), ao possibilitar verificações e controles em um processo, mesmo nos casos em que o comportamento desejado não possa ser previamente definido como uma regra. Ainda que posteriormente ao fato, uma entidade supervisora pode diferenciar comportamentos aceitáveis de inaceitáveis dentro da comunidade digital, levando em conta as particularidades das circunstâncias específicas do caso (Kroll, 2020). Desse modo, a responsabilidade deve ser encarada de forma preventiva e colaborativa, envolvendo tanto os operadores dos sistemas quanto a sociedade como um todo, para garantir que os avanços tecnológicos não sejam usados de forma irresponsável, mas sim para promover um ambiente *on-line* mais seguro e inclusivo.

A função preventiva – ou princípio da prevenção – da responsabilidade civil deve ser robustecida pela implementação de práticas que minimizem riscos antes que danos ocorram. Além disso, a função precaucional exige que se atue proativamente para mitigar danos potenciais, considerando que a natureza da tecnologia é muitas vezes imprevisível e cheia de incertezas. Nesse sentido, provedores de serviços digitais e desenvolvedores de IA devem adotar uma postura ética que leve em consideração as consequências de longo prazo de suas inovações, implementando não apenas medidas de segurança, mas também sistemas de revisão e explicação adequados (Rosensvald; Faleiros Júnior, 2023). Portanto, a responsabilidade dos provedores de internet, redes sociais e plataformas de conteúdo é fundamental para o futuro das tecnologias digitais. Não apenas para proteger os usuários de danos imediatos, como também para garantir que essas tecnologias não alimentem ou perpetuem comportamentos destrutivos, como o *cyberbullying* e o discurso de ódio. Por oportuno, destaca-se que a responsabilização dos provedores de aplicação de IA não inibe a responsabilidade individual dos praticantes de *bullying* e *cyberbullying*. Inclusive a aplicação da função precaucional da responsabilidade civil também se estende a estes, pois, por meio das plataformas

digitais, é possível denunciar conteúdos danosos pela própria comunidade e, ainda, identificar o causador do dano, viabilizando a reparação às vítimas.

O papel dos provedores de plataformas digitais é, no caso, mais significativo quando analisamos o impacto coletivo de suas ações. As plataformas são, em muitos casos, os principais veículos de disseminação de informações na sociedade moderna. Elas têm o poder de moldar a percepção pública, criar tendências, e até mesmo influenciar o comportamento social e político. Quando seus algoritmos priorizam o compartilhamento de conteúdos que promovem o ódio ou que incentivam práticas prejudiciais como o *cyberbullying*, os danos não são apenas individuais; eles se estendem à coletividade, afetando a convivência social e, em última análise, a estrutura da própria sociedade. Portanto, as plataformas têm um dever ético para com a sociedade em geral, e essa responsabilidade se reflete na maneira como elas projetam seus sistemas algorítmicos e políticas de moderação.

Por fim, a responsabilidade dos provedores de serviços digitais também envolve uma responsabilidade social, que vai além da sua obrigação legal de proteger os dados dos usuários ou de impedir danos diretos. As plataformas digitais têm um impacto profundo nas dinâmicas sociais e culturais, e devem, portanto, assumir uma postura proativa na criação de ambientes digitais que respeitem a dignidade de todos os usuários, especialmente aqueles mais vulneráveis. Isso inclui a implementação de políticas educacionais sobre segurança *on-line*, a promoção de comportamentos respeitosos e inclusivos, e a colaboração com organizações que trabalham para prevenir o *cyberbullying* e outros danos no ambiente digital.

A função preventiva (princípio da prevenção) da responsabilidade civil, juntamente com a função precaucional, deve ser vista como um sistema integrado que visa não apenas reparar danos, mas prevenir que eles ocorram em primeiro lugar. Isso exige uma abordagem multidisciplinar, que combine direito, ética, tecnologia e políticas públicas, com o objetivo de garantir que o desenvolvimento e o uso de tecnologias digitais não coloquem em risco os direitos fundamentais dos indivíduos. Em última análise, a responsabilidade dos provedores deve ser orientada pela premissa de que, ao criar e operar plataformas digitais, eles têm a obrigação de proteger não apenas os

interesses comerciais, mas também o bem-estar dos indivíduos e da sociedade, a prevenir, assim, a dissipação do *bullying* e deste em sua forma digital.

Considerações finais

Este artigo teve como objetivo analisar a responsabilidade civil dos provedores de aplicação de internet no contexto do *cyberbullying* escolar, considerando os novos desafios jurídicos trazidos pela participação de sistemas de IA nesse tipo de intimidação sistemática.

O foco central recaiu sobre os direitos da personalidade das vítimas, especialmente crianças e adolescentes, e a necessidade de que a responsabilidade civil seja concebida como um instrumento preventivo para proteger e garantir a integridade psicossocial no ambiente digital.

Os direitos da personalidade, enquanto pilares essenciais da dignidade humana, exigem proteção especial no contexto escolar, no qual crianças e adolescentes encontram-se em pleno desenvolvimento psicossocial. A utilização de IA para a prática de *cyberbullying* agrava a vulnerabilidade desse grupo, ampliando os danos e dificultando a reparação. Assim, torna-se imperativo que a responsabilidade civil atue não apenas na reparação de danos, mas também como uma ferramenta preventiva capaz de evitar a violação desses direitos fundamentais.

A análise revelou que o modelo atual de responsabilidade culposa, dependente de notificações judiciais específicas para a remoção de conteúdos, é insuficiente diante da rapidez e do alcance das agressões mediadas por IA. A responsabilidade civil, sob uma perspectiva preventiva, deve ser estruturada para antecipar e mitigar os riscos antes que danos irreparáveis ocorram. Isso implica exigir dos provedores de internet a implementação de mecanismos de controle, como algoritmos mais transparentes e sistemas proativos de detecção de conteúdos prejudiciais, respeitando os direitos da personalidade e promovendo um ambiente digital mais seguro.

O princípio da prevenção ganha destaque nesse contexto, impondo aos provedores o dever de adotar medidas eficazes que reduzam a probabilidade de violações. Além disso, o princípio da precaução deve orientar a atuação dos provedores

em situações de incerteza tecnológica, como o uso de sistemas de IA com potenciais riscos desconhecidos. A responsabilização preventiva não deve ser vista como um ônus, mas como um imperativo ético e jurídico para proteger os direitos da personalidade das vítimas e resguardar a integridade do ambiente escolar e digital.

Nesse cenário, o papel dos provedores transcende a simples moderação de conteúdos. Sua atuação deve estar pautada por uma responsabilidade social ampla, promovendo a conscientização e a educação digital para prevenir práticas lesivas. Programas de capacitação para o uso ético e seguro das tecnologias, aliados a uma regulamentação jurídica mais robusta, são essenciais para proteger a dignidade e o desenvolvimento saudável de crianças e adolescentes no ambiente digital.

Conclui-se que a responsabilidade civil, sob uma perspectiva preventiva, é um instrumento indispensável para assegurar a proteção dos direitos da personalidade e a integridade psicossocial no ambiente escolar e digital. A prevenção deve ser o eixo central de uma abordagem normativa que busque não apenas reparar danos, mas também evitar que ocorram, garantindo que a tecnologia seja utilizada de maneira ética e segura, promovendo um ambiente digital que respeite e valorize a dignidade humana em todas as suas dimensões.

Referências

- Barbosa, M. M. (2006). *Liberdade vs. responsabilidade: a precaução como fundamento da imputação delitual?* Coimbra: Almedina.
- Bohn, C., & Hickey, M. (2010). Bullying and social status during school transitions. In S. R. Jimerson, S. M. Swearer, & D. L. Espelage (Eds.). *Handbook of Bullying in Schools: An International Perspective*. (pp. 199-202). New York: Routledge.
- Castells, M. (2020). *A sociedade em rede*. Tradução: Roneide Venancio Majer. 22. ed. São Paulo: Paz e Terra.
- Coeckelbergh, M. (2020). Artificial intelligence, responsibility attribution, and a relational justification of explainability. *Science and Engineering Ethics, Cham*, v. 26, p. 2051-2068. Recuperado de: <https://doi.org/10.1007/s11948-019-00146-8>
- Doneda, D. (2020). *Da privacidade à proteção de dados pessoais: fundamentos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil. E-book.

- Fante, C. (2005). *Fenômeno Bullying: como prevenir a violência nas escolas e educar para a paz*. Campinas, SP: Ed. Versus.
- G1. (2024, 25 de setembro). Alunos são expulsos após usar inteligência artificial para criar nudes falsos de professora e colegas em escola particular de Cuiabá. G1. Recuperado de: <https://g1.globo.com/mt/mato-grosso/noticia/2024/09/25/alunos-sao-expulsos-apos-usar-inteligencia-artificial-para-criar-nudes-falsos-de-professora-e-colegas-em-escola-particular-de-cuiaba.ghtml>
- Galdino, J. C. S *et al.* (Orgs). (2013). *Curso de Informática Avançada*. Natal: IFRN Editora.
- Garaigordobil, M. & Oñederra, J. A. (2010). *La violencia entre iguales: Revisión teórica y estrategias de intervención* [Peer harassment: Theoretical review and intervention strategies]. Madrid: Pirámide.
- Guimarães, J. A. S. A. (2022). O direito ao esquecimento como ferramenta de defesa nas novas tecnologias. In: C. Colombo, W. Engelmann & J. L. M. Faleiros Júnior (Coords.). *Tutela jurídica do corpo eletrônico: novos desafios ao direito digital* (pp. 101-122). Indaiatuba, SP: Foco.
- Henriques, I., Pita, M. & Hartung, P. (2021). A proteção de dados pessoais de crianças e adolescentes. In: L. S. Mendes, D. Doneda, Sarlet, I. W. & Rodrigues Junior, O. L. (Coords.). *Tratado de Proteção de Dados Pessoais* (pp. 199-225). Rio de Janeiro: Forense.
- Jung, C. G. (2011). *O desenvolvimento da personalidade*. Petrópolis: Vozes.
- Lehfeld, L. S. et al. (2021). A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. *Revista Eletrônica Pesquiseduca*, Santos, 29(13), 236-255. Recuperado de: <https://periodicos.unisantos.br/pesquiseduca/article/view/1029/902>
- Lei nº 8.069, de 13 de julho de 1990. (1990). *Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências*. Brasília, DF. Recuperado de: https://www.planalto.gov.br/ccivil_03/leis/18069.htm
- Lei nº 12.965, de 23 de abril de 2014. (2014). *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Brasília, DF: Presidência da República, 2014. Recuperado de: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm#:~:text=L12965&text=Estabelece%20princ%C3%ADpios%2C%20garantias%2C%20direitos%20e,uso%20da%20Internet%20no%20Brasil.&text=Art.,Munic%C3%ADpios%20em%20rela%C3%A7%C3%A3o%20C3%A0%20mat%C3%A9ria
- Lei nº 13.185, de 6 de novembro de 2015. (2015). *Institui o Programa de Combate à Intimidação Sistemática (Bullying)*. Brasília, DF: Presidência da República. Recuperado de: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm

- Lei nº 13.709, de 14 de agosto de 2018. (2018). *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF. Recuperado de: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
- Lei nº 14.811, de 12 de janeiro de 2024. (2024). *Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê 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 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente)*. Brasília, DF: Presidência da República. Recuperado de: <https://www2.camara.leg.br/legin/fed/lei/2024/lei-14811-12-janeiro-2024-795244-publicacaooriginal-170834-pl.html>
- Kroll, J. A. (2020). Accountability in Computer Systems. In: M. Dubber, F. Fasquale, & S. Das (Ed.). *The Oxford Handbook of the Ethics of Artificial Intelligence*. Oxford: Oxford University Press.
- Lima, A. P. M. C. (2019). Cyberbullying: agressão virtual, consequências reais e desdobramentos jurídicos. In: A. P. M. C. Lima, C. B. Hissa & P. M. Saldanha (Orgs.). *Direito digital: debates contemporâneos* (pp. 211-222). São Paulo: Revista dos Tribunais.
- Miranda, F. A. (2013). O direito fundamental ao livre desenvolvimento da personalidade. *Revista do Instituto do Direito Brasileiro*, Lisboa, v. 2, n. 10.
- Oliveira, J. C. C., Lourenço, L. M. & Senra, L. X. (2015). A produção científica sobre o cyberbullying: uma revisão bibliométrica. *Psicologia em Pesquisa*, Juiz de Fora, v.9, n.1, p. 31-39. Recuperado de: <http://pepsic.bvsalud.org/pdf/psipesq/v9n1/v9n1a05.pdf>
- Olweus, D. (1993). *Bullying at school: What we know and what we can do*. Oxford: Blackwell.
- Pasquale, F. (2017). Toward a fourth law of robotics: Preserving attribution, responsibility, and explainability in an algorithmic society. *University of Maryland Legal Studies Research Papers*, Baltimore, n. 21, p. 1-13. Recuperado de: <http://ssrn.com/abstract=3002546>
- Prensky, M. (2001). Digital Natives, Digital Immigrants. In: PRENSKY, Marc. *On the Horizon*. NCB University Press, Bingley, v. 9, n. 5, p. 460-466, October. Recuperado de: https://www.emerald.com/insight/content/doi/10.1108/10748120110424816/full/html?utm_source=TrendMD&utm_medium=cpc&utm_campaign=On_the_Horizon_TrendMD_0&WT.mc_id=Emerald_TrendMD_0
- Rosenvald, N. & Faleiros Júnior, J. L. M. (2023). Answerability e seus reflexos para a responsabilização civil. *Revista IBERC*, Belo Horizonte, v. 6, n. 3, p. IV-X. Recuperado de: <https://revistaiberc.responsabilidadecivil.org/iberc/article/view/284>

- Sarlet, I. W. (2021). Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: L. S. Mendes, D. Doneda, I. W. Sarlet, & Rodrigues Junior, O. L. (Coords.). *Tratado de Proteção de Dados Pessoais* (p. 21-59). Rio de Janeiro: Forense.
- Schreiber, A. (2013). *Novos paradigmas da responsabilidade civil*. São Paulo: Atlas.
- Shariff, S. (2009). *Confronting Cyber-bullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences*. New York: Cambridge University Press.
- Smith, P. *et al.* (2008). Cyberbullying: its nature an impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376-385. doi:10.1111/j.1469-7610.2007.01846.x
- Superior Tribunal de Justiça - STJ (4ª Turma). (2022). *Recurso Especial nº 1783269/MG*. Relator: Ministro Antonio Carlos Ferreira, julgado em 14/12/2021, DJe 18/02/2022. Recuperado de: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%201783269>
- TIC Kids Online Brasil 2019 (2020). *CETIC - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação*, 2020. Recuperado de: https://cetic.br/media/analises/tic_kids_online_brasil_2019_coletiva_imprensa.pdf
- Wimmer, M. (2019). Inteligência artificial, algoritmos e o direito: um panorama dos principais desafios. In: In: A. P. M. C. Lima, C. B. Hissa & P. M. Saldanha. (Orgs.). *Direito digital: debates contemporâneos* (pp. 15-30). São Paulo: Revista dos Tribunais.
- Yaegashi, J. G. & Otero, C. S. (2023). *Bullying e Cyberbullying Escolar: Responsabilidade Civil Como Instrumento de Tutela da Personalidade*. Curitiba: Juruá Editora.

Recebido: 01/12/2024
Aceito: 29/01/2025
Publicado: 20/04/2025

NOTA:

Os autores foram responsáveis pela concepção do artigo, pela análise e interpretação dos dados, pela redação e revisão crítica do conteúdo do manuscrito e, ainda, pela aprovação da versão final publicada.