

A responsabilidade civil no uso da inteligência artificial nas interações com crianças e adolescentes em plataformas de jogos online

Jéssica de Oliveira Dias¹, Maria Alice de Freitas Figueiredo², Aluísio Santos de Oliveira³, Alexandre Pires Duarte⁴, Marcelo Silva Ângelo Ferreira⁵

Resumo: O presente Trabalho tem como objetivo analisar a responsabilidade civil relacionada ao uso da inteligência artificial (IA) nas interações com crianças e adolescentes em plataformas de jogos online. Com o avanço acelerado das tecnologias digitais e a crescente presença de menores nesses ambientes, observa-se a ampliação de riscos decorrentes da utilização de algoritmos, sistemas de moderação automatizada, avatares interativos, chatbots e mecanismos de recomendação que influenciam diretamente a experiência dos usuários. A ausência de regulamentação específica para o emprego de IA voltada ao público infantojuvenil, aliada à insuficiência de mecanismos de proteção e fiscalização, contribui para a vulnerabilidade desses sujeitos, que já são reconhecidos pelo ordenamento jurídico brasileiro como destinatários de proteção integral. Nesse contexto, o trabalho investiga os limites e as possibilidades da responsabilidade civil das plataformas de jogos online, considerando o dever de segurança, o risco da atividade e a teoria do defeito do serviço. Analisa-se também o papel dos responsáveis legais e do Estado na mitigação de danos, especialmente em casos de exposição a violência, exploração, coleta abusiva de dados pessoais, práticas manipulativas e outros danos digitais. O estudo propõe a necessidade de implementação de princípios contemporâneos como diligência digital, governança algorítmica, educação em IA e adoção de modelos preventivos, tais como safety by

¹ Graduada em Direito pela Fundação Comunitária de Ensino Superior de Itabira –UNIFUNCESI, Brasil, jeh.odiaas@gmail.com.

² Graduada em Direito pela Fundação Comunitária de Ensino Superior de Itabira –UNIFUNCESI, Brasil, mariipoema2@gmail.com

³ Mestre em Direito Privado. Pós-graduação/Especialização em Direito Privado. Docente no Centro Universitário Funcesi/UNIFUNCESI. Auditor Fiscal de Tributos no Município de Itabira-MG. aluisio.santosdeoliveira@gmail.com

⁴ Graduado em Direito pela (UNIFENAS 2004); pós-graduado em MBA – Gestão Empresarial com Ênfase em Gestão de Pessoas (FUNCESI 2011); pós-graduado em Ciências Criminais (Universidade Gama Filho 2009). Docente no Centro Universitário Funcesi/UNIFUNCESI. Mestrando em Direito nas Relações Econômicas e Sociais (Milton Campos). alexandre.duarte@funcesi.br

⁵ Doutor/Mestre em Administração de Empresas, Professor Titular na Fundação Comunitária de Ensino Superior de Itabira – UNIFUNCESI, Faculdade de Minas Gerais, FAMIG, Faculdade de Sabará, Brasil, marcelo.ferreira@funcesi.br, marcelos.bh01@gmail.com, marcelo.ferreira@faculadadesabará.com.br

design e privacy by design. Ao final, busca-se demonstrar que o sistema brasileiro de responsabilidade civil ainda apresenta caráter predominantemente reativo diante dos riscos tecnológicos, sendo imprescindível a modernização de seus instrumentos para assegurar a efetiva proteção de crianças e adolescentes no ambiente virtual. O trabalho, portanto, contribui para o debate jurídico sobre os desafios emergentes da IA e sobre as medidas necessárias para garantir um ambiente digital mais seguro e responsável.

Palavras-chave: responsabilidade civil; inteligência artificial; crianças e adolescentes; jogos online; plataformas digitais.

Civil liability in the use of artificial intelligence in interactions with children and adolescents on online gaming platforms

Abstract: This undergraduate thesis aims to analyze civil liability concerning the use of artificial intelligence (AI) in interactions with children and adolescents on online gaming platforms. With the rapid advancement of digital technologies and the growing presence of minors in these environments, there is an increase in risks arising from the use of algorithms, automated moderation systems, interactive avatars, chatbots, and recommendation mechanisms that directly influence users' experiences. The lack of specific regulation governing the use of AI directed at children and adolescents, combined with the insufficiency of protection and monitoring mechanisms, intensifies the vulnerability of these individuals, who are already recognized by the Brazilian legal system as subjects of full protection. In this context, the study investigates the limits and possibilities of civil liability for online gaming platforms, considering their duty of safety, the risk of the activity, and the defect-of-service theory. It also examines the role of legal guardians and the State in mitigating damages, especially in cases involving exposure to violence, exploitation, abusive data collection, manipulative practices, and other digital harms. The research proposes the need to implement contemporary principles such as digital diligence, algorithmic governance, AI education, and preventive models such as safety by design and privacy by design. Ultimately, it seeks to demonstrate that the Brazilian civil liability system still operates in a predominantly reactive manner when confronted with technological risks, making it essential to modernize its instruments in order to ensure effective protection of children and adolescents in virtual environments. Thus, this study contributes to the legal debate on the emerging challenges of AI and on the measures required to promote safer and more responsible digital spaces.

Keywords: civil liability; artificial intelligence; children and adolescents; online games; digital platforms.

1 INTRODUÇÃO

A crescente presença da inteligência artificial (IA) no cotidiano tem transformado radicalmente as interações sociais, sobretudo no ambiente digital. Essa transformação adquire contornos ainda mais delicados quando envolve públicos vulneráveis, como crianças e adolescentes, cujo estágio de desenvolvimento exige proteção prioritária por parte do Estado, da sociedade e da família, conforme estabelece o artigo 227 da Constituição Federal de 1988. Assistentes virtuais, algoritmos de recomendação em redes sociais, jogos online e plataformas de ensino adaptativo são exemplos de sistemas de IA que hoje interagem diretamente com esse público, muitas vezes de forma automatizada e sem mediação humana.

Embora essas tecnologias ofereçam inegáveis benefícios como acesso à informação, lazer e ferramentas educativas também trazem riscos consideráveis, especialmente no que se refere à exposição a conteúdos inadequados, coleta indevida de dados pessoais, indução de comportamentos e até mesmo manipulação emocional. Nesse cenário, torna-se fundamental refletir sobre os limites éticos e jurídicos dessas interações, em especial diante do princípio da proteção integral previsto no Estatuto da Criança e do Adolescente (ECA) e da Lei Geral de Proteção de Dados, LGPD (Lei nº 13.709/2018), que dedica atenção específica ao tratamento de dados de menores de idade (art. 14).

A Convenção sobre os Direitos da Criança das Nações Unidas, internalizada pelo Brasil por meio do Decreto nº 99.710/1990, também destaca o dever dos Estados em assegurar o bem-estar de crianças e adolescentes frente a qualquer ameaça, inclusive as que emergem de contextos digitais. Diante disso, o presente trabalho busca investigar como se estrutura a responsabilidade civil em casos de danos causados por sistemas de IA a crianças e adolescentes, considerando não apenas os marcos normativos já existentes, mas também as lacunas regulatórias que desafiam o direito contemporâneo frente às novas tecnologias. Além disso, pretende-se compreender o funcionamento básico da inteligência artificial, seus principais usos em plataformas digitais voltadas ao público infantojuvenil incluindo redes sociais, jogos e aplicativos de comunicação, como o Discord e os riscos

decorrentes dessas interações. A análise dessas dinâmicas permitirá discutir como essas tecnologias podem tanto contribuir para o desenvolvimento social quanto, mas principalmente, representar ameaças à integridade, à privacidade e ao bem-estar físico e mental de crianças e adolescentes.

2 RELEVÂNCIA DO TEMA: VULNERABILIDADE DAS CRIANÇAS E ADOLESCENTES NO AMBIENTE DIGITAL CONTEMPORÂNEO

O avanço das tecnologias da informação e a consolidação das redes sociais transformaram profundamente as formas de interação social, comunicação e acesso ao conhecimento. Entretanto, o ambiente digital, apesar de oferecer inúmeras oportunidades, também potencializa riscos e vulnerabilidades, especialmente para crianças e adolescentes, cuja formação psíquica e emocional ainda se encontra em desenvolvimento.

Segundo Lemos (2021), a infância e a adolescência são fases marcadas por intensa construção identitária e social, o que torna seus sujeitos mais suscetíveis à influência e à exposição digital. Essa vulnerabilidade é ampliada pela lógica de funcionamento das plataformas, que coletam e exploram dados pessoais de forma muitas vezes invisível ao usuário comum, inclusive de menores de idade. Nesse contexto, a hiper vulnerabilidade digital surge como um desafio à proteção integral prevista no artigo 227 da Constituição Federal, que impõe à família, à sociedade e ao Estado o dever de assegurar, com absoluta prioridade, os direitos das crianças e dos adolescentes.

De acordo com Doneda (2019), a coleta e o tratamento de dados de crianças e adolescentes exigem especial atenção, pois envolvem informações sensíveis capazes de afetar sua dignidade e liberdade futura. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) reforça essa proteção, ao estabelecer que o tratamento de dados de menores deve ocorrer sempre em seu melhor interesse, conforme disposto no artigo 14. Ainda assim, a falta de conscientização dos próprios responsáveis e a ausência de uma cultura digital protetiva tornam o público infantojuvenil um dos mais expostos aos danos digitais, como o *cyberbullying*, o *grooming* (aliciamento online) e a superexposição por *sharenting*.

Para Teixeira (2019), a vulnerabilidade digital da criança não decorre apenas da sua condição etária, mas da assimetria informacional entre o usuário e as grandes plataformas tecnológicas, que detêm o controle dos dados e dos algoritmos que modulam a experiência online. Assim, a vulnerabilidade no ambiente digital contemporâneo assume um caráter estrutural e coletivo, demandando não apenas a atuação estatal, mas também responsabilidade parental e social na mediação do uso da internet.

Por fim, Tavares (2020) ressalta que a exposição excessiva de crianças nas redes sociais — prática conhecida como *sharenting* revela o quanto os próprios adultos podem contribuir, ainda que de forma não intencional, para a violação dos direitos de personalidade dos menores. Dessa forma, a discussão sobre vulnerabilidade digital infantil torna-se indispensável para o fortalecimento de políticas públicas, práticas educativas e instrumentos jurídicos que assegurem uma cidadania digital responsável e protetiva.

Portanto, discutir a vulnerabilidade das crianças e adolescentes no ambiente digital contemporâneo é fundamental não apenas sob o ponto de vista tecnológico, mas sobretudo ético e jurídico, uma vez que envolve a concretização de direitos fundamentais e a necessidade de adaptação das normas de proteção à nova realidade social imposta pela era digital.

2.1 Objetivos e justificativa do estudo

O presente estudo tem como objetivo geral analisar os impactos jurídicos decorrentes da utilização de sistemas de inteligência artificial (IA) nas plataformas de jogos online, especialmente no que se refere à responsabilidade civil em situações que envolvem crianças e adolescentes. Busca-se compreender de que forma a aplicação da IA em mecanismos de moderação de conteúdo, personalização de experiências e coleta de dados influencia a ocorrência de danos à privacidade, à imagem e ao desenvolvimento psíquico e social de usuários em condição de vulnerabilidade.

A justificativa do estudo repousa na constatação de que o uso crescente de inteligência artificial em plataformas de jogos tem transformado profundamente as

dinâmicas de socialização e entretenimento infantojuvenil, ao mesmo tempo em que aumenta os riscos jurídicos e éticos relacionados à coleta de dados, manipulação algorítmica e exposição de conteúdos inadequados. A relevância social e jurídica deste trabalho decorre do fato de que crianças e adolescentes constituem público prioritário de proteção segundo o artigo 227 da Constituição Federal e o Estatuto da Criança e do Adolescente (ECA), que impõem à família, à sociedade e ao Estado o dever de garantir-lhes direitos fundamentais de forma integral. Nesse contexto, a utilização de IA por plataformas de jogos online cria um ambiente inseguro de comunicação e lazer em que a linha entre o entretenimento e a exposição de dados é cada vez mais tênue. Assim, este estudo se justifica por sua contribuição para o debate sobre a adequação das normas de responsabilidade civil e proteção de dados pessoais frente às novas tecnologias inteligentes, propondo uma reflexão crítica sobre os limites éticos e jurídicos da IA na mediação das interações entre crianças, adolescentes e plataformas digitais. Ao problematizar essa relação, busca-se fortalecer o entendimento de que a inovação tecnológica deve ocorrer de forma compatível com os direitos da personalidade, a dignidade da pessoa humana e o melhor interesse da criança, pilares fundamentais do ordenamento jurídico brasileiro

2.2 Relevância do tema: vulnerabilidade das crianças e adolescentes no ambiente digital contemporâneo

O avanço das tecnologias da informação e a consolidação das redes sociais transformaram profundamente as formas de interação social, comunicação e acesso ao conhecimento. Entretanto, o ambiente digital, apesar de oferecer inúmeras oportunidades, também potencializa riscos e vulnerabilidades, especialmente para crianças e adolescentes, cuja formação psíquica e emocional ainda se encontra em desenvolvimento.

Segundo Lemos (2021), a infância e a adolescência são fases marcadas por intensa construção identitária e social, o que torna seus sujeitos mais suscetíveis à influência e à exposição digital. Essa vulnerabilidade é ampliada pela lógica de funcionamento das plataformas, que coletam e exploram dados pessoais de forma muitas vezes invisível ao usuário comum, inclusive de menores de idade. Nesse

contexto, a hipervulnerabilidade digital surge como um desafio à proteção integral prevista no artigo 227 da Constituição Federal, que impõe à família, à sociedade e ao Estado o dever de assegurar, com absoluta prioridade, os direitos das crianças e dos adolescentes.

De acordo com Doneda (2019), a coleta e o tratamento de dados de crianças e adolescentes exigem especial atenção, pois envolvem informações sensíveis capazes de afetar sua dignidade e liberdade futura. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) reforça essa proteção, ao estabelecer que o tratamento de dados de menores deve ocorrer sempre em seu melhor interesse, conforme disposto no artigo 14. Ainda assim, a falta de conscientização dos próprios responsáveis e a ausência de uma cultura digital protetiva tornam o público infantojuvenil um dos mais expostos aos danos digitais, como o *cyberbullying*, o *grooming* (aliciamento online) e a superexposição por *sharenting*.

Para Teixeira (2019), a vulnerabilidade digital da criança não decorre apenas da sua condição etária, mas da assimetria informacional entre o usuário e as grandes plataformas tecnológicas, que detêm o controle dos dados e dos algoritmos que modulam a experiência online. Assim, a vulnerabilidade no ambiente digital contemporâneo assume um caráter estrutural e coletivo, demandando não apenas a atuação estatal, mas também responsabilidade parental e social na mediação do uso da internet.

Por fim, Tavares (2020) ressalta que a exposição excessiva de crianças nas redes sociais pratica conhecida como *sharenting* revela o quanto os próprios adultos podem contribuir, ainda que de forma não intencional, para a violação dos direitos de personalidade dos menores. Dessa forma, a discussão sobre vulnerabilidade digital infantil torna-se indispensável para o fortalecimento de políticas públicas, práticas educativas e instrumentos jurídicos que assegurem uma cidadania digital responsável e protetiva.

Portanto, discutir a vulnerabilidade das crianças e adolescentes no ambiente digital contemporâneo é fundamental não apenas sob o ponto de vista tecnológico, mas sobretudo ético e jurídico, uma vez que envolve a concretização de direitos

fundamentais e a necessidade de adaptação das normas de proteção à nova realidade social imposta pela era digital.

3 INTELIGÊNCIA ARTIFICIAL

A expansão das tecnologias digitais tem sido fortemente impulsionada pelo desenvolvimento da Inteligência Artificial (IA), que se manifesta de forma cada vez mais presente em plataformas de comunicação e interação social.

Segundo Fábio Gagliardi Cozman, entende IA como um campo que reúne sistemas computacionais capazes de reproduzir comportamentos identificados como inteligentes, envolvendo tanto abordagens simbólicas quanto baseadas em dados; à obra organizada por Cozman discute explicitamente a dificuldade de dar um único conceito fechado para IA e apresenta as tradições (simbólica, conexionista, aprendizado de máquina) que compõem o campo.

3.1 Conceito de IA

Anna Helena Reali Costa, ao tratar do futuro da pesquisa em IA, apresenta à IA como o estudo de agentes computacionais inteligentes que percebem um ambiente e tomam decisões para atingir objetivos (ênfase em aprendizado de máquina e modelos baseados em dados); ressalta também a fluidez conceitual e a mescla de técnicas simbólicas e estatísticas.

Sérgio Amadeu da Silveira, aborda IA em chave crítica/política: define e discute sistemas algorítmicos, machine learning e IA como tecnologias sociotécnicas que operam sobre dados e produzem efeitos políticos e econômicos; sua ênfase é conceituar IA não só tecnicamente, mas como prática integrada a regimes de vigilância e poder.

Virgílio Almeida, conceptualiza IA sobretudo pelo seu papel social e pelos desafios que coloca (transparência, explicabilidade, responsabilidade); em textos e entrevistas, descreve IA como tecnologia que reconfigura papéis humanos/máquinas e que deve alinhar-se a valores humanos.

Ronaldo Lemos, ao explicar IA ao público, define-a como um conjunto de algoritmos e sistemas computacionais que inferem padrões em dados e tomam decisões (ou sugerem ações) com graus variados de autonomia; ressalta aspectos práticos como IA generativa, LLMs e impacto regulatório.

3.2 Breve exposição sobre plataforma do Discord

O Discord, como ambiente digital de natureza híbrida, utiliza sistemas de IA em diferentes níveis de sua operação, desde mecanismos de moderação automatizada de conteúdo até ferramentas de personalização da experiência do usuário. Essa integração reflete uma tendência contemporânea de automatização das relações comunicacionais, em que os algoritmos assumem papel decisivo na mediação das interações humanas. Dessa forma, a análise do Discord sob a ótica da Inteligência Artificial revela que a tecnologia, embora essencial à gestão e moderação de grandes comunidades virtuais, também produz efeitos jurídicos relevantes. A compreensão desses efeitos é indispensável para o desenvolvimento de políticas regulatórias que conciliem inovação tecnológica e proteção de direitos fundamentais, especialmente quando se trata de crianças e adolescentes no ambiente digital.

3.3 O Discord e os riscos à integridade de crianças e adolescentes no ambiente digital

O Discord é uma plataforma digital de comunicação síncrona e assíncrona que opera a partir da lógica de servers (servidores), compostos por canais de texto e de voz, nos quais os usuários interagem em grupos de interesse. Além disso, a aplicação permite o envio de direct messages (mensagens diretas), recurso que amplia a possibilidade de contatos privados fora do espaço coletivo dos servidores (Discord, 2023).

O funcionamento da plataforma baseia-se, em grande medida, na descentralização da moderação, pois cada servidor possui administradores e moderadores locais responsáveis por definir as regras internas e aplicá-las aos membros. Esse modelo, conhecido como community-based moderation (moderação baseada na comunidade), transfere a responsabilidade primária de fiscalização a

usuários voluntários, cuja atuação é naturalmente heterogênea e sujeita a falhas (Gilbert et al., 2020).

Tal característica, embora eficaz para a manutenção de comunidades diversas e autônomas, revela-se problemática quando se consideram usuários em condição peculiar de desenvolvimento, como crianças e adolescentes. Isso porque a ausência de supervisão centralizada e a possibilidade de criar múltiplas contas com dados fictícios tornam o ambiente propício para práticas ilícitas, como o *grooming* (aliciamento), o cyberbullying (assédio virtual) e a chamada *sextortion* (extorsão sexual com base em imagens íntimas) (Whitty; Buchanan, 2016).

Apesar de a plataforma oferecer ferramentas automatizadas, como o AutoMod (moderador automático, voltado ao bloqueio de palavras-chave e spam), filtros de mídia sensível e o Family Center (centro familiar, que permite algum acompanhamento parental), tais recursos apresentam limitações técnicas e operacionais. Os filtros, por exemplo, não abarcam vídeos ou áudios em tempo real, tampouco impedem conversas privadas em mensagens diretas, cuja criptografia e confidencialidade restringem a supervisão parental e institucional (Attwood; Russell, 2021).

Estudos recentes e ações judiciais em diferentes jurisdições demonstram que a confiança exclusiva em filtros automáticos ou na moderação descentralizada não se mostra suficiente para proteger crianças e adolescentes. Autoridades norte-americanas, por exemplo, questionaram publicamente à eficácia dos mecanismos de *safety by design* (segurança por desenho) apresentados pela empresa, destacando a persistência de condutas abusivas na plataforma (New Jersey Attorney General, 2024).

Portanto, a natureza híbrida do Discord — simultaneamente espaço de socialização legítima e ambiente potencial para práticas criminosas — impõe desafios regulatórios e pedagógicos. À ausência de um corpo de moderadores institucionais (institutional moderators), aliado à capacidade técnica limitada de detecção automatizada, reforça a necessidade de medidas jurídicas mais eficazes e

de programas educativos voltados à conscientização de pais, escolas e usuários menores de idade.

3.4 A interação dentro das plataformas de jogos online

As plataformas de jogos online contemporâneas, como Roblox, Minecraft, Free Fire e Fortnite, configuram-se como ambientes digitais interativos, nos quais o jogo transcende a mera competição para se tornar um espaço de convivência social, expressão e comunicação entre seus usuários. Esses ambientes combinam elementos de jogo, rede social e criação colaborativa, permitindo que os jogadores interajam de múltiplas formas, por meio de chats de texto, voz, avatares personalizados e mundos virtuais compartilhados.

Essas plataformas têm em comum o fato de serem ambientes digitais interativos nos quais crianças e adolescentes jogam, criam conteúdos e interagem socialmente.

Entretanto, seus recursos internos de comunicação são limitados, principalmente em relação à moderação, à privacidade e à troca de mensagens de voz.

Por isso, é muito comum que os jogadores utilizem o Discord como plataforma complementar para conversar em tempo real, organizar partidas, compartilhar estratégias e criar comunidades específicas de cada jogo.

Assim, o Discord se torna um elo comunicacional que unifica comunidades de jogadores oriundas de diferentes plataformas.

Em síntese: enquanto os jogos são os espaços de ação e competição, o Discord é o espaço de socialização e comunicação contínua, tais plataformas funcionam como “espaços públicos digitais de sociabilidade”, nos quais os jovens experimentam novas formas de identidade e pertencimento. Essa interação ocorre em tempo real, mediada por sistemas automatizados e algoritmos de recomendação, que direcionam conteúdos, sugerem amigos e definem o tipo de experiência vivenciada por cada jogador Valente; Cerqueira, 2022).

No Roblox, por exemplo, a interação ocorre por meio de salas virtuais criadas pelos próprios usuários, onde é possível conversar, participar de missões conjuntas, comprar itens virtuais e realizar trocas simbólicas com moedas do jogo. Essa estrutura cria uma dinâmica social semelhante à das redes sociais, com formação de grupos, chats abertos e comunicação privada, o que, embora estimule a colaboração, também aumenta a exposição de crianças e adolescentes a riscos digitais, como contato com desconhecidos, discurso de ódio, manipulação ou exploração comercial indevida (Nic.br, 2024).

Em Minecraft, a interação é centrada na cooperação criativa: os jogadores constroem mundos coletivos, compartilham recursos e participam de projetos educativos, sendo a plataforma amplamente utilizada em contextos pedagógicos (Santos, 2023). Já em Fortnite e Free Fire, a interação assume um viés mais competitivo e comunicacional, com uso de chats de voz para coordenação de partidas em equipe, o que pode implicar riscos de exposição a linguagem inapropriada ou cyberbullying.

Esses ambientes também se caracterizam por sua natureza híbrida, combinando elementos de entretenimento, comércio, rede social e tecnologia de inteligência artificial. Essa hibridização reflete a “convergência entre plataformas de interação e economias digitais”, nas quais os dados dos usuários se tornam o principal insumo de funcionamento e monetização das plataformas (Lemos, 2021). Assim, os sistemas de IA são utilizados para personalizar a experiência do jogador, identificar padrões de comportamento e direcionar publicidade, o que levanta importantes questões de privacidade e responsabilidade civil, sobretudo quando os usuários são menores de idade.

Dessa forma, a interação dentro dessas plataformas não é neutra: ela ocorre em contextos mediados por algoritmos e políticas empresariais, que moldam as experiências dos jogadores e podem gerar consequências jurídicas quando há violação de direitos da personalidade, tratamento indevido de dados pessoais ou exposição a riscos psicológicos e sociais. Compreender essa dinâmica é, portanto, indispensável para avaliar a responsabilidade civil das empresas desenvolvedoras e

mantenedoras de jogos online, especialmente frente à vulnerabilidade das crianças e adolescentes no ambiente digital.

4 RESPONSABILIDADE CIVIL

A seara da responsabilidade civil possui caráter multidisciplinar e ultrapassa o campo jurídico, travando implicações filosóficas, políticas e culturais. O dever de reparação é considerado um fato da vida, inerente ao convívio em sociedade, uma vez que a prática de atos que alteram o status prévio de equilíbrio e ocasionam danos é um acontecimento inevitável (Dias, 2012).

Sergio Cavalieri Filho (2012) explica que o intuito principal do regulamento jurídico é proteger o lícito e reprimir o ilícito, corrigindo seus efeitos prejudiciais. Para tanto, entende-se que existem deveres de positivos, de fazer algo, e deveres negativos, de não fazer determinada coisa. O dever jurídico consiste em conduta externa imposta pelo Direito como requisito à convivência em sociedade, que atribui obrigações a todos os indivíduos de forma simultânea.

Fala-se, então, do dever jurídico originário, que quando violado, gera o dever jurídico sucessivo ou secundário, consistente na obrigação de indenizar o prejuízo causado. Nesse sentido, surge a noção de responsabilidade civil, que busca a reparação do prejuízo decorrente da lesão do dever jurídico primário, a fim de colocar a vítima na situação em que estaria sem ocorrência do fato danoso, o chamado status quo ante (Gonçalves, 2021).

4.1 Conceito de responsabilidade

A responsabilização jurídica se diferencia da mera responsabilização moral, apesar de muitas vezes caminharem lado a lado. Isso porque o ato lesivo pode, além de ferir a norma jurídica, ofender normas informais no campo da moralidade e da religião de forma concomitante.

Ao passo que a reprovação moral atua na consciência individual de cada sujeito, não havendo uma preocupação com a existência de prejuízo à terceiro, a responsabilidade jurídica prescinde da existência de dano, que ocorre apenas mediante uma infração à norma formal (Gonçalves, 2021).

Além disso, diferencia-se o dever de responsabilidade do dever obrigacional. Este último consiste no direito do sujeito ativo da relação jurídica de exigir o cumprimento da prestação pactuada, que pode ser advir de diferentes fontes. O dever de reparação, por sua vez, surge a partir do inadimplemento da obrigação.

A violação do dever originário consiste num ato ilícito, que pode ser civil ou penal. A separação dos ilícitos é feita conforme o grau de gravidade e imoralidade do ato ou omissão, de modo que uma mesma conduta pode violar ambas as esferas de ilicitude (Cavaliere, 2012). O presente trabalho se limita aos ilícitos civis, que geram a responsabilidade civil do agente.

O dever jurídico lesionado pode ser oriundo de uma obrigação imposta pelo Direito, como mencionado anteriormente, ou pode advir de uma relação jurídica obrigacional preexistente, como numa relação contratual. Assim, a doutrina divide a matéria em responsabilidade civil contratual e extracontratual. Na esfera contratual, os indivíduos têm aptidão para criar deveres jurídicos entre si, de modo a contrair obrigações por meio dos negócios jurídicos por ele firmados, estes, sendo os contratos e manifestações unilaterais de vontade. Assim, a responsabilidade contratual resulta do inadimplemento, o ilícito contratual ou relativo. Já a contexto extracontratual, não há vínculo obrigacional preexistente e o dever de indenizar surge a partir do ilícito aquiliano ou absoluto, isto é, lesão a um dever jurídico imposta pela lei, não por um negócio jurídico privado. Antes da apresentação dos requisitos da responsabilidade civil, será exposto um ligeiro repasse do desenvolvimento da responsabilidade e a aceção de culpa como critério do dever de indenizar, matéria relevante para análise dos requisitos para a reparação dos danos causados pela IA.

4.2 A responsabilidade civil no cenário da inteligência artificial

Uma vez compreendido o que é a inteligência artificial e verificada a urgência da regulação jurídica de seu funcionamento, passa-se a exposição do surgimento da responsabilidade civil e de seus requisitos nos dias atuais. Em seguida, serão analisados alguns marcos regulatórios internacionais que disciplinam o uso da nova

inteligência, uma vez que tais normativas exercem forte influência na construção de uma legislação nacional sobre o assunto.

4.3 Bases constitucionais da responsabilidade parental

A Constituição Federal de 1988, ao tratar da família, da criança e do adolescente, estabeleceu uma clara matriz normativa de responsabilidade parental solidária e intransferível. O art. 227 da CF dispõe que é dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, o direito à vida, à saúde, à educação, à dignidade, ao respeito e à convivência familiar e comunitária, bem como colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência e opressão.

Nesse contexto, a omissão parental diante dos riscos digitais, como o acesso a conteúdos impróprios, a interação com estranhos em ambientes virtuais ou a exposição indevida de dados pessoais em plataformas que utilizam algoritmos de machine learning (aprendizado de máquina), pode configurar uma violação indireta ao dever constitucional de proteção integral.

A negligência quanto ao ambiente virtual é, portanto, uma forma moderna de negligência, tão relevante quanto a omissão nos cuidados físicos ou educacionais tradicionais.

4.4 Fundamentação estatutária: o dever de cuidado no estatuto da criança e do adolescente (ECA)

O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) aprofunda esse dever de proteção. O art. 22 dispõe que "aos pais incumbe o dever de sustento, guarda e educação dos filhos menores", devendo estes zelar por sua segurança moral e física. Já o art. 4º reforça o princípio da prioridade absoluta, e o art. 5º assegura a inviolabilidade da integridade física, psíquica e moral de crianças e adolescentes.

Essas normas impõem aos pais o dever de atuar preventivamente diante dos riscos advindos do uso da tecnologia. Assim, permitir que uma criança utilize sistemas de inteligência artificial, plataformas de jogos online, assistentes virtuais

ou redes sociais sem qualquer orientação ou monitoramento pode configurar omissão culposa, traduzida em abandono digital. Esse tipo de negligência não apenas viola o dever de guarda, mas pode gerar responsabilidade civil e até mesmo reflexos na esfera penal e administrativa, dependendo do dano causado.

4.5 A inteligência artificial e os novos riscos à infância digital

Os sistemas de IA baseados em aprendizado de máquina (machine learning) e aprendizado profundo (deep learning) têm a capacidade de coletar, processar e interpretar grandes volumes de dados, muitas vezes de maneira autônoma. Em plataformas acessadas por crianças e adolescentes, como Roblox, Discord e outras, esses sistemas são utilizados para personalizar experiências, recomendar conteúdos e interagir com os usuários.

Essa interação, embora atraente e aparentemente inofensiva, esconde mecanismos de manipulação comportamental (conhecidos como *behavioral nudging*), que podem expor menores a conteúdos inadequados, riscos de aliciamento, cyberbullying, exploração sexual, consumo excessivo ou coleta de dados pessoais.

Nesse cenário, a ausência de orientação parental, o “abandono digital”, acentua a vulnerabilidade do menor e cria um nexos causal entre a omissão dos pais e os danos psicológicos ou morais decorrentes do uso indevido da IA.

4.6 Responsabilidade civil dos pais por omissão digital

Ao tratarmos da responsabilidade civil dos pais, reconhecemos o dever de indenizar quando há omissão culposa na vigilância ou educação dos filhos (arts. 932, I, e 933 do Código Civil).

No contexto digital, esse dever deve ser reinterpretado à luz das novas tecnologias.

Quando os pais permitem o uso irrestrito de dispositivos e aplicações de IA sem acompanhamento, sem filtros de segurança e sem orientação, estão, em essência, violando o dever de guarda digital que decorre do poder familiar.

Assim, a responsabilidade parental assume também um aspecto tecnológico e ético, que demanda alfabetização digital, controle de acesso e diálogo familiar sobre riscos virtuais. A omissão, nesses casos, pode caracterizar negligência civil, ensejando a reparação de danos, especialmente se a inação resultar em exposição indevida, violação de privacidade ou traumas decorrentes de interações em ambientes digitais automatizados.

4.7 Proteção de dados e supervisão digital

Com a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 art.14), consolidou-se no Brasil um regime protetivo especial para dados de crianças e adolescentes. O dispositivo exige consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal para o tratamento de dados pessoais de menores de 12 anos.

Essa norma impõe aos pais o dever jurídico de compreender e controlar as tecnologias com as quais seus filhos interagem, especialmente aquelas que operam com inteligência artificial.

A omissão nessa vigilância reforça o conceito de abandono digital, podendo gerar responsabilidade compartilhada entre pais e provedores de serviço.

5 ANÁLISE DO ORDENAMENTO JURÍDICO BRASILEIRO

A responsabilização civil das plataformas de jogos online revela-se um dos temas mais complexos do Direito contemporâneo, sobretudo quando envolve danos sofridos por crianças e adolescentes. Isso ocorre porque a arquitetura digital dessas empresas opera em um ambiente transnacional, tecnologicamente opaco e juridicamente fragmentado, dificultando a imputação de responsabilidade. Como observa Flávio Tartuce (2024), a responsabilidade civil pressupõe a violação de um dever jurídico, cuja demonstração depende da comprovação de conduta, dano e nexo causal, elementos que se tornam significativamente mais difíceis de identificar quando o suposto ilícito ocorre em plataformas digitais privadas, cujos algoritmos e mecanismos internos são inacessíveis ao usuário.

Além disso, a maioria das plataformas de jogos possui sede no exterior, o que acarreta entraves processuais relevantes, como a dificuldade de citações internacionais e a ausência de representantes legais no Brasil. Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2022) lembram que o cenário digital globalizado desafia os modelos clássicos de responsabilização, pois “rompe fronteiras e enfraquece a eficácia imediata das normas nacionais”, criando zonas de inefetividade regulatória.

5.1 Dificuldades na responsabilização dos desenvolvedores e administradores de plataformas de jogos online

Outro obstáculo relevante decorre do regime jurídico aplicável. Embora o Código de Defesa do Consumidor pareça adequado para tutelar os usuários, inclusive os menores, seu uso concorre com o Marco Civil da Internet, que, no art. 19, condiciona a responsabilização de provedores ao descumprimento de ordem judicial específica. A doutrina de Danilo Doneda e Laura Schertel Mendes (2021) destaca que a aplicação desse dispositivo torna mais difícil responsabilizar plataformas quando a conduta ilícita decorre da interação entre usuários ou da recomendação algorítmica, uma vez que a lei não acompanha a complexidade tecnológica do ambiente digital.

No que se refere à proteção infantojuvenil, o problema se agrava. Conforme leciona Maria Berenice Dias (2023), a vulnerabilidade das crianças e adolescentes impõe às empresas um dever reforçado de diligência, compatível com o princípio da proteção integral previsto no Estatuto da Criança e do Adolescente. No entanto, as plataformas de jogos frequentemente não adotam mecanismos suficientes de moderação, prevenção ou filtragem de riscos, transferindo para os pais responsabilidades operacionais que, muitas vezes, extrapolam suas possibilidades reais de controle e conhecimento sendo assim, a proteção da infância no ambiente digital não pode ser depositada exclusivamente na família, sob pena de esvaziamento da responsabilidade social e empresarial das plataformas online.

A dificuldade probatória também representa um entrave substancial. Grande parte das interações realizadas em jogos online é volátil, ocorre por mensagens de voz ou chats que não ficam registrados, e depende de servidores inteiramente controlados pela empresa. Assim, a vítima raramente possui acesso às evidências

necessárias para comprovar a falha do serviço. Nas palavras de Bruno Miragem (2021), o ambiente digital cria uma “assimetria informacional estrutural”, na qual o fornecedor detém acesso privilegiado aos dados e às provas, enquanto o consumidor tem sua capacidade de demonstração severamente limitada.

Por fim, a ausência de legislação específica sobre jogos online e a velocidade com que novas tecnologias, como sistemas de recompensa gamificada e mecanismos automatizados de interação, são incorporados às plataformas geram um quadro de insegurança jurídica. A inovação tecnológica avança em ritmo muito superior à capacidade regulatória do Estado, o que exige interpretação principiológica e aplicação ampliada dos deveres de segurança, lealdade e informação.

Diante dessas circunstâncias, percebe-se que a responsabilização das plataformas de jogos online esbarra em desafios jurídicos, técnicos e probatórios que comprometem a tutela efetiva de crianças e adolescentes. O cenário reforça a necessidade de uma legislação específica que estabeleça deveres claros de prevenção, transparência e governança, a fim de reduzir a assimetria entre usuários e empresas e garantir a proteção integral dos menores no ambiente digital.

5.2 Ausência de regulações específicas para ia aplicada a menores

A expansão das plataformas digitais de jogos e interação, como Roblox e Discord, insere crianças e adolescentes em um ambiente repleto de riscos associados à exposição, coleta de dados, convivência com desconhecidos, indução a comportamentos inadequados e conteúdos prejudiciais. Embora o ordenamento jurídico brasileiro disponha de um conjunto robusto de normas protetivas, especialmente a Constituição Federal, o Código Civil, o Estatuto da Criança e do Adolescente (ECA), o Código de Defesa do Consumidor (CDC) e o Marco Civil da Internet (MCI), persistem lacunas significativas quanto à responsabilização civil de plataformas digitais globais que operam sem sede no Brasil ou sem mecanismos efetivos de moderação para o público infantojuvenil.

A Constituição Federal, em seu art. 227, estabelece o princípio da proteção integral e prioridade absoluta, determinando que a família, a sociedade e o Estado devem assegurar todos os direitos fundamentais às crianças e adolescentes.

Todavia, ao transpor esse comando constitucional para o ambiente virtual, nota-se que a concretização prática desse dever encontra barreiras estruturais. As plataformas digitais têm natureza transnacional, utilizam algoritmos opacos e adotam padrões de moderação e segurança alheios à regulação brasileira.

No campo da responsabilidade civil, Maria Helena Diniz (2022) ressalta que esta visa “reparar o dano e prevenir sua ocorrência”, constituindo mecanismo essencial para a tutela dos direitos da personalidade, especialmente em situações de vulnerabilidade. Contudo, a autora também destaca que a responsabilidade deve acompanhar “as novas formas de lesão que surgem com a evolução social e tecnológica”, o que evidencia a insuficiência das normas atuais frente à complexidade das dinâmicas digitais.

Para Carlos Roberto Gonçalves (2023), a responsabilidade civil contemporânea é marcada pelo “deslocamento do foco da culpa para a proteção efetiva da vítima”, sobretudo quando o consumidor é hipervulnerável, como é o caso de crianças em plataformas de jogos. Entretanto, as estruturas normativas existentes não definem claramente o dever de segurança das empresas que exploram ambientes digitais infantis, nem trazem critérios objetivos para responsabilizar provedores internacionais que estimulam a interação entre menores — um fenômeno cotidiano em plataformas como Roblox e Discord.

Conforme o Marco Civil da Internet (Brasil, 2024, art.19) embora avance na proteção de dados e na disciplina da responsabilidade dos provedores, apresenta limitações claras. Conforme observa Pablo Stolze Gagliano (2022), o regime de responsabilidade condicionado à ordem judicial para remoção de conteúdo cria uma barreira temporal incompatível com a proteção integral infantojuvenil, pois a lesão pode ocorrer de forma imediata e massiva antes de qualquer intervenção judicial possível. Ademais a legislação vigente não prevê deveres específicos de segurança para serviços frequentemente utilizados por menores, como plataformas de jogos.

No âmbito do Direito Digital, Danilo Doneda (2021) destaca que o tratamento de dados de crianças demanda cuidado superior, dada a fragilidade da autodeterminação informativa nesse grupo. No entanto, plataformas como Roblox

coletam metadados, preferências e padrões comportamentais de crianças sem mecanismos verificáveis de consentimento parental, evidenciando a insuficiência da Lei Geral de Proteção de Dados (LGPD) para lidar com plataformas internacionais de difícil fiscalização.

A teoria da responsabilidade civil também enfrenta obstáculos técnicos. Sérgio Cavalieri Filho (2020) aponta que a multiplicidade de agentes digitais torna mais complexa a prova do nexo causal, especialmente quando o dano decorre de interações entre milhares de usuários, uso de chats por voz, mensagens privadas e servidores independentes como ocorre em Discord. Essa fragmentação dificulta identificar quem falhou: a plataforma, seus moderadores, seus usuários ou terceiros estrangeiros.

O Código de Defesa do Consumidor, embora reconheça expressamente a hipervulnerabilidade da criança, não regulamenta as práticas de segurança específicas para plataformas digitais. Flávio Tartuce (2024) afirma que o atual sistema de responsabilidade civil brasileiro permanece “reativo diante dos riscos tecnológicos”, falhando em impor obrigações preventivas aos agentes econômicos, que deveriam adotar modelos de “safety by design” e “privacy by design”.

Ademais, o Estatuto da Criança e do Adolescente, criado em 1990, não contempla as dinâmicas das plataformas virtuais modernas, deixando lacunas quanto à verificação de idade, mecanismos de denúncia, algoritmos de segurança e responsabilidade solidária entre empresas de tecnologia. A ausência de previsão normativa específica permite que plataformas transfiram a responsabilidade aos pais ou responsáveis, ignorando suas próprias falhas de moderação ou design.

Em síntese, embora o ordenamento jurídico brasileiro contenha princípios sólidos de proteção integral, responsabilidade objetiva, defesa do consumidor e tutela dos direitos da personalidade, falta regulamentação específica e eficaz para responsabilizar civilmente plataformas digitais globais que expõem crianças e adolescentes a riscos graves. O desafio contemporâneo consiste em adaptar as bases civilistas clássicas, especialmente a função preventiva da responsabilidade civil, às complexas estruturas virtuais que permeiam a vida infantojuvenil.

Enquanto o direito não avança com normas mais claras e específicas, a vulnerabilidade de crianças e adolescentes permanece ampliada, e a responsabilização civil dos agentes, especialmente plataformas estrangeiras, continua sendo um dos maiores desafios do direito brasileiro.

6 CONCLUSÃO

A análise desenvolvida ao longo deste trabalho evidencia que a inteligência artificial, embora represente um avanço significativo na forma como nos relacionamos com a informação e a tecnologia, também impõe desafios éticos e jurídicos profundos, sobretudo quando aplicada em contextos que envolvem crianças e adolescentes. A ausência de uma legislação específica para a IA no Brasil agrava a dificuldade de responsabilização civil por danos decorrentes de sistemas autônomos, especialmente em ambientes digitais como Roblox e Discord, nos quais há grande circulação de menores de idade.

É imprescindível, portanto, que o ordenamento jurídico brasileiro avance na construção de marcos regulatórios próprios para a inteligência artificial, baseados no princípio da proteção integral e no melhor interesse da criança, de modo a garantir um ambiente digital seguro, ético e compatível com os direitos fundamentais. A responsabilidade civil, nesse contexto, deve ser interpretada de forma evolutiva e preventiva, assegurando que o desenvolvimento tecnológico caminhe em harmonia com a dignidade humana e a proteção dos grupos vulneráveis.

REFERÊNCIAS

A ADNEWS. **Nike, YouTube e Roblox são as marcas mais populares entre jovens.** São Paulo, 2025. Disponível em: <https://adnews.com.br/nike-youtube-e-roblox-sao-as-marcas-mais-populares-entre-jovens/>. Acesso em: 5 out. 2025.

ALMEIDA, Virgílio. **Desafios da IA responsável na pesquisa científica.** Jornal da USP / materiais da USP (texto/PDF sobre IA responsável e pilares como transparência, responsabilidade e explicabilidade), p. 3-7, 2024.

ATTWOOD, F.; RUSSELL, L. **Online sexual grooming: shifting narratives and new challenges.** Journal of Sexual Aggression, v. 27, n. 1, p. 1-15, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília: Senado Federal, 1988.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil.** 14. ed. São Paulo: Atlas, p. 23-48, 2020.

COSTA, Anna Helena Reali. **O futuro da pesquisa em inteligência artificial.** Revista da Universidade de São Paulo (RevUSP) / publicação vinculada à USP, 2024. Disponível em: documento/entrada sobre “O futuro da pesquisa em inteligência artificial”.

COZMAN, Fabio G.; PLONSKI, Guilherme Ary; NERI, Hugo (orgs.). **Inteligência artificial: avanços e tendências.** São Paulo: Instituto de Estudos Avançados (IEA-USP), 2021. p 77-102.

DIAS, Maria Berenice. **Manual de Direito das Famílias**. 14. ed. São Paulo: Revista dos Tribunais, 2023. P. 101-145

DISCORD. **Transparency Report – Second Half of 2023**. San Francisco: Discord Inc., 2023. Disponível em: <https://transparency.discord.com>. Acesso em: 22 set. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2019. P.51-88.

DONEDA, Danilo; MENDES, Laura Schertel. **Curso de Proteção de Dados Pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, p. 75-80. 2021.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil – Responsabilidade Civil**. 6. ed. São Paulo: Saraiva, p. 110-145. 2020.

GAMING ERA. **71% da Geração Alfa joga online: Roblox e Minecraft lideram entre crianças e adolescentes**. São Paulo, 2024. Disponível em: <https://gamingera.biz/criancas-adolescentes-71-geracao-alfa-games-roblox/>. Acesso em: 5 out. 2025.

GILBERT, S.; BERKOWITZ, D.; SAMPSON, T. **Community moderation in online platforms**. Social Media + Society, v. 6, n. 2, p. 1–12, 2020.

GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 20. ed. São Paulo: Saraiva, p, 101-115, 2022.

LEMONS, André. **Cultura da convergência e plataformas híbridas: tecnologias digitais, interação e sociabilidade**. Salvador: EDUFBA, 2021, p. 71-79.

LEMOS, Ronaldo. **Para entender a inteligência artificial de uma vez por todas. InvestNews (série explicativa / material público)**, 07 mai. 2024 (série de textos/vídeos explicativos sobre IA e termos: LLM, IA generativa, prompt, etc.).

MEDON, Filipe. **Responsabilidade civil e inteligência artificial**. Rio de Janeiro: Lumen Juris, 2022.

MEU PS. **Roblox foi o jogo mais pesquisado no Brasil em 2023, revela Semrush**. São Paulo, 2023. Disponível em: <https://meups.com.br/noticias/semrush-roblox-mais-pesquisado-brasil-2023/>. Acesso em: 5 out. 2025.

MIRAGEM, Bruno. **Vulnerabilidade informacional e relações de consumo digitais**. In: **Direito do consumidor**. 6. Ed. São Paulo: Revista dos Tribunais, 2021. P. 210-217.

NEW JERSEY ATTORNEY GENERAL. **State v. Discord Inc.: Complaint and Allegations of Misleading Safety Claims**. Newark, 2024. Disponível em: <https://www.njoag.gov>. Acesso em: 22 set. 2025.

NIC.br. **TIC Kids Online Brasil 2023: pesquisa sobre o uso da internet por crianças e adolescentes no Brasil**. São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: https://nic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf. Acesso em: 5 out. 2025.

SANTOS, Cláudia Regina dos. **Minecraft e aprendizagem colaborativa: um estudo sobre o uso de jogos digitais na educação básica**. Revista Brasileira de Educação e Tecnologia, v. 16, n. 2, p. 45-59, 2023.

SILVEIRA, Sérgio Amadeu da. **Discursos sobre regulação e governança algorítmica**. Estudos Sociológicos (Araraquara), v.25, n.48, p.63-85, jan.-jun. 2020.

TARTUCE, Flávio. **Manual de Direito Civil. 31.** ed. São Paulo: Método, p. 501-530, 2024b.

TEIXEIRA, Ana Carolina Brochado. **A exposição infantil na internet: reflexões sobre o sharenting.** Revista Brasileira de Direito Civil, v. 19, p. 210-238. 2019.

TERRA. **Conheça 14 plataformas de jogos para jogar online.** São Paulo, 2023. Disponível em: <https://www.terra.com.br/gameon/conheca-14-plataformas-de-jogos-para-jogar-online>. Acesso em: 5 out. 2025.

VALENTE, Mariana; CERQUEIRA, Diego. **Infância conectada: jogos, redes e privacidade.** São Paulo: InternetLab, p. 55-89, 2022.