BOCA
BOLETIM DE CONJUNTURA

DIREITOS DA PERSONALIDADE, INOVAÇÕES TECNOLÓGICAS E CRIANÇAS: RISCOS À PRIVACIDADE NA ERA DA SUPEREXPOSIÇÃO DIGITAL

PERSONALITY RIGHTS, TECHNOLOGICAL INNOVATIONS, AND CHILDREN: PRIVACY RISKS IN THE ERA OF DIGITAL OVEREXPOSURE

DERECHOS DE LA PERSONALIDAD, INNOVACIONES TECNOLÓGICAS Y NIÑOS: RIESGOS A LA PRIVACIDAD EN LA ERA DE LA SOBREEXPOSICIÓN DIGITAL

https://doi.org/10.56238/bocav25n82-016

Data de submissão: 29/08/2026 **Data de publicação:** 29/09/2026

Laura Leal Carvalho
Mestranda em Ciências Jurídicas
Instituição: Universidade Cesumar (UniCesumar)
Orcid: https://orcid.org/0009-0009-9387-093X
Lattes: http://lattes.cnpq.br/3873884563503791

Valéria Silva Galdino Cardin
Doutora em Direito
Instituição: Universidade Cesumar (UniCesumar)
Orcid: https://orcid.org/0000-0001-9183-0672
Lattes: http://lattes.cnpq.br/8121501433418182

Marcelo Negri Soares
Doutor em Direito
Instituição: Universidade Cesumar (UniCesumar)
Orcid: https://orcid.org/0000-0002-0067-3163
Lattes: http://lattes.cnpq.br/8798303423669514

Leticia Mayumi Almeida Takeshita
Doutoranda em Direito
Instituição: Universidade Cesumar (UniCesumar)
Orcid: https://orcid.org/0000-0002-6645-035X
Lattes: http://lattes.cnpq.br/5097813982617521

RESUMO

O avanço exponencial das inovações tecnológicas e a crescente inserção de crianças no ambiente digital têm suscitado debates prementes acerca da proteção dos direitos da personalidade, em especial o direito à privacidade e à imagem. A prática do sharenting (superexposição de crianças pelos pais nas redes sociais), aliada a novas ameaças como a inteligência artificial generativa e as deepfakes, coloca os menores em situação de extrema vulnerabilidade, expondo-os a riscos como o cyberbullying, roubo de identidade, exploração sexual e a manipulação de comportamento. Este artigo analisa os impactos da superexposição digital infantil sob a ótica dos direitos da personalidade, discutindo como o

ordenamento jurídico brasileiro — notadamente o Estatuto da Criança e do Adolescente (ECA) e a Lei Geral de Proteção de Dados (LGPD) — busca proteger os menores nesse cenário. Destaca-se, ainda, a importância e a urgência da responsabilização parental na mitigação desses riscos, argumentando que a autoridade parental contemporânea deve englobar, indissociavelmente, o dever de cuidado e proteção no ambiente virtual.

Palavras-chave: Direitos da Personalidade. Privacidade. Inovações Tecnológicas. Sharenting. Responsabilidade Parental. LGPD.

ABSTRACT

The exponential advancement of technological innovations and the growing insertion of children in the digital environment have raised pressing debates about the protection of personality rights, especially the right to privacy and image. The practice of sharenting (excessive exposure of children by parents on social media), combined with new threats such as generative artificial intelligence and deepfakes, places minors in a situation of extreme vulnerability, exposing them to risks such as cyberbullying, identity theft, sexual exploitation and behavioral manipulation. This article analyzes the impacts of digital child overexposure from the perspective of personality rights, discussing how Brazilian legal system — notably the Statute of Children and Adolescents (ECA) and the General Law for Personal Data Protection (LGPD) — seeks to protect minors in this scenario. The importance and urgency of parental accountability in mitigating these risks is highlighted, arguing that contemporary parental authority must indissociably encompass the duty of care and protection in the virtual environment.

Keywords: Personality Rights. Privacy. Technological Innovations. Sharenting. Parental Responsibility. LGPD.

RESUMEN

El avance exponencial de las innovaciones tecnológicas y la creciente inserción de niños en el ambiente digital han suscitado debates prementes acerca de la protección de los derechos de la personalidad, en especial el derecho a la privacidad y a la imagen. La práctica del sharenting (superexposición de niños por los padres en las redes sociales), aliada a nuevas amenazas como la inteligencia artificial generativa y los deepfakes, coloca a los menores en situación de extrema vulnerabilidad, exponiéndolos a riesgos como el ciberacoso, robo de identidad, explotación sexual y la manipulación del comportamiento. Este artículo analiza los impactos de la superexposición digital infantil bajo la óptica de los derechos de la personalidad, discutiendo cómo el ordenamiento jurídico brasileño — notadamente el Estatuto del Niño y del Adolescente (ECA) y la Ley General de Protección de Datos (LGPD) — busca proteger a los menores en este escenario. Se destaca, además, la importancia y la urgencia de la responsabilización parental en la mitigación de estos riesgos, argumentando que la autoridad parental contemporánea debe englobar, indisociablemente, el deber de cuidado y protección en el ambiente virtual.

Palabras clave: Derechos de la Personalidad. Privacidad. Innovaciones Tecnológicas. Sharenting. Responsabilidad Parental. LGPD.

1 INTRODUÇÃO

A evolução tecnológica das últimas décadas transformou radicalmente a forma como a sociedade interage, se comunica e constrói suas relações interpessoais. Se por um lado a *internet* democratizou o acesso à informação e encurtou distâncias geográficas, permitindo que famílias dispersas pelo mundo mantenham contato constante e que conhecimento seja compartilhado instantaneamente, por outro, inaugurou novos e complexos desafios jurídicos, especialmente no que tange à proteção dos direitos da personalidade. Nesse contexto, as crianças e os adolescentes, enquanto sujeitos de direitos em condição peculiar de desenvolvimento, encontram-se no epicentro de uma revolução digital que ameaça diretamente sua privacidade, intimidade e dignidade.

As inovações tecnológicas, potencializadas pelo advento da inteligência artificial e pela onipresença das redes sociais, criaram um ambiente onde a coleta massiva de dados e a exposição da vida privada se tornaram a regra, não a exceção. Plataformas como *Instagram*, *TikTok, Facebook e YouTube* foram concebidas para maximizar o engajamento e a permanência do usuário, utilizando algoritmos sofisticados que analisam comportamentos e preferências para oferecer conteúdo cada vez mais personalizado e viciante. É neste cenário que emerge o fenômeno do sharenting — neologismo derivado da junção das palavras inglesas share (compartilhar) e parenting (paternidade/maternidade) —, que consiste no compartilhamento excessivo de informações, fotos e vídeos de crianças por seus próprios pais ou responsáveis nas plataformas digitais, muitas vezes sem considerar as implicações futuras (ALBERS, 2024).

Embora muitas vezes motivada por orgulho legítimo, desejo de conexão com familiares distantes ou busca de validação social através de curtidas e comentários, a superexposição digital infantil gera uma pegada digital precoce e indelével, muitas vezes criada sem o consentimento ou a compreensão do menor sobre as implicações futuras de tal ato. Pesquisas demonstram que mais de 75% dos pais compartilham informações sobre seus os filhos nas redes sociais, e menos de 25% solicitam consentimento antes de postar (ANDOH, 2026). Mais alarmante, contudo, é a interseção dessa prática com o uso malicioso de inovações como deepfakes, que têm sido utilizadas para a criação de material de abuso sexual infantil gerado por inteligência artificial, transformando fotos inocentes em conteúdo explorador (UNICEF, 2026).

Diante dessa realidade complexa e multifacetada, o presente artigo tem como objetivo analisar os riscos que o avanço das inovações tecnológicas e a superexposição na *internet* impõem à privacidade das crianças. Busca-se compreender como o ordenamento jurídico, fundamentado na doutrina da

proteção integral, pode salvaguardar os direitos da personalidade infantojuvenis, ressaltando o papel central da responsabilização parental na mediação e controle da inserção dos filhos no ambiente digital. A análise será conduzida sob uma perspectiva jurídico-constitucional, considerando tanto o direito interno brasileiro quanto as tendências do direito comparado, com especial atenção às legislações internacionais que se debruçam sobre a proteção de dados e privacidade de menores.

2 DIREITOS DA PERSONALIDADE E A PRIVACIDADE DA CRIANÇA NA ERA DIGITAL

Os direitos da personalidade são direitos subjetivos inerentes a toda pessoa, essenciais para a proteção de sua dignidade e para o livre desenvolvimento de sua identidade pessoal, social e profissional. Esses direitos, que compreendem a vida, a integridade física, a honra, a reputação, a privacidade, a intimidade e a imagem, constituem o núcleo duro dos direitos fundamentais, sendo indisponíveis e inalienáveis. O ordenamento jurídico brasileiro consagra, tanto na Constituição Federal quanto no Código Civil, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação. O art 5º, inciso X, da Constituição Federal é explícito ao afirmar que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

No que tange às crianças e aos adolescentes, a proteção desses direitos ganha contornos ainda mais rigorosos, fundamentados na doutrina da proteção integral, consolidada pelo art 227 da Constituição Federal e pelo Estatuto da Criança e do Adolescente (ECA - Lei nº 8.069/1990). Essa doutrina parte da premissa de que crianças e adolescentes são sujeitos de direitos em condição peculiar de desenvolvimento, merecedores de proteção especial não apenas do Estado e da família, mas de toda a sociedade. O art 15 do ECA é taxativo ao afirmar que a criança e o adolescente têm direito à liberdade, ao respeito e à dignidade como pessoas humanas em processo de desenvolvimento e como sujeitos de direitos civis, humanos e sociais, sem qualquer discriminação. Por sua vez, o art 17 do mesmo diploma legal elenca, entre os aspectos do direito ao respeito, a inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, das ideias e crenças, dos espaços e objetos pessoais.A privacidade, concebida tradicionalmente como o direito de estar só, ou right to be let alone, conforme formulado por Warren e Brandeis no século XIX, adquire na era digital uma dimensão radicalmente diferente. Não se trata mais apenas de um direito espacial, de não ser observado ou invadido em espaços privados, mas de

um direito informacional, relacionado à autodeterminação informativa e ao controle sobre dados pessoais. Para as crianças, cuja capacidade de discernimento e de compreensão dos riscos ainda estão em formação, o exercício da autodeterminação informativa é mediado por seus representantes legais. No entanto, essa mediação não pode ser absoluta ou irrestrita; deve ser sempre orientada pelo princípio do melhor interesse da criança, que exige que qualquer decisão tomada em relação ao menor considere primordialmente seu bem-estar integral e seu desenvolvimento harmonioso.A hiperconectividade contemporânea e o modelo de negócios das grandes plataformas de tecnologia, baseados fundamentalmente na extração e monetização de dados (economia de dados), colocam a privacidade infantil em constante e crescente ameaça. As plataformas digitais funcionam como máquinas de captura de dados, coletando informações não apenas sobre o que os usuários fazem, mas também sobre quem eles são, como pensam, o que desejam, quais são suas vulnerabilidades emocionais e psicológicas. Segundo relatório do Fundo das Nações Unidas para a Infância (UNICEF), a coleta, análise e perfilamento de dados de crianças podem minar profundamente seus direitos à privacidade e à proteção de informações pessoais, criando perfis comportamentais desde a mais tenra infância (UNICEF, 2019). Tais práticas permitem não apenas o direcionamento de publicidade abusiva e manipuladora, mas também a manipulação comportamental, a exposição a conteúdos inadequados e a discriminação algorítmica.

O conceito de perfilamento (ou profiling) é particularmente preocupante quando aplicado a menores. Diferentemente dos adultos, que possuem identidade consolidada e capacidade crítica desenvolvida, as crianças estão em processo contínuo de formação de sua personalidade, valores e preferências. Quando algoritmos analisam dados de crianças para criar perfis comportamentais e prever suas ações futuras, estão, em essência, moldando o desenvolvimento dessas crianças, influenciando suas escolhas de consumo, suas preferências políticas e ideológicas, e até mesmo sua autoestima e autoimagem. A pesquisadora Ana Carolina Brochado Teixeira, especialista em direitos da personalidade, argumenta que a perfilização de crianças representa uma ameaça existencial ao seu direito de se desenvolver livremente, de escolher seus próprios caminhos e de construir sua identidade de forma autônoma (GARCIA; NUNES, 2021).A vulnerabilidade das crianças é multiplicada quando consideramos que elas frequentemente não compreendem as implicações de seus atos *online*, não entendem como seus dados são coletados e utilizados, e não possuem a capacidade cognitiva para avaliar riscos de longo prazo. O desenvolvimento cognitivo infantil é um processo gradual que se estende até o final da adolescência, com diferentes capacidades emergindo em diferentes idades. A

capacidade de compreender consequências futuras e abstratas, por exemplo, não se desenvolve completamente até o final da adolescência ou início da vida adulta. Isso significa que uma criança que compartilha uma foto íntima ou que fornece informações sensíveis *online* pode não ser capaz de compreender que essas informações permanecerão na *internet* indefinidamente e poderão ser utilizadas contra ela no futuro.Além disso, as crianças são frequentemente alvo de práticas comerciais agressivas e enganosas por parte das plataformas digitais. Muitos aplicativos e sites são deliberadamente projetados para serem viciantes, utilizando técnicas de gamificação, notificações push e algoritmos de recomendação para manter as crianças engajadas o máximo possível. Quanto mais tempo uma criança passa em uma plataforma, mais dados são coletados sobre ela, mais publicidade direcionada ela recebe, e mais vulnerável ela se torna a conteúdos prejudiciais e a predadores *online*. Pesquisas mostram que o uso excessivo de redes sociais está correlacionado com aumentos em ansiedade, depressão, baixa autoestima e até pensamentos suicidas em adolescentes (ALBERS, 2024). A proteção dos direitos da personalidade de crianças no ambiente digital, portanto, não é uma questão meramente técnica ou administrativa, mas uma questão fundamental de direitos humanos e de dignidade. Requer uma compreensão profunda da vulnerabilidade específica das crianças, do poder assimétrico das grandes plataformas de tecnologia, e da necessidade de intervenção estatal e familiar para garantir que as crianças possam desenvolver-se em um ambiente que respeite sua privacidade, sua autonomia emergente e seus direitos fundamentais.

3 O FENÔMENO DO SHARENTING E AS NOVAS AMEAÇAS TECNOLÓGICAS

A inserção da criança no ambiente digital muitas vezes não se dá por sua própria iniciativa ou escolha, mas pela ação deliberada de seus pais ou responsáveis. O sharenting tem se tornado uma prática culturalmente aceita e amplamente disseminada nas sociedades ocidentais, particularmente entre pais de classe média e alta com acesso a smartphones e redes sociais. Pais documentam desde ultrassons (criando uma identidade digital pré-natal), passando pelo primeiro dia de aula, primeiros passos, primeiras palavras, até momentos de vulnerabilidade como crises emocionais ou situações constrangedoras, criando uma identidade digital para seus filhos antes mesmo que estes tenham capacidade de consentir ou opinar sobre o assunto (ANDOH, 2026). Essa prática é frequentemente justificada como forma de manter familiares distantes informados, de compartilhar alegrias com amigos, ou simplesmente de documentar momentos preciosos da infância.Os riscos associados ao sharenting são múltiplos, graves e frequentemente subestimados pelos pais. Em primeiro lugar, há a

violação clara da autonomia e da privacidade da criança. O que pode parecer uma foto inocente ou engraçada para os pais — uma criança em situação de vulnerabilidade, uma criança nua no banho, uma criança chorando ou tendo uma crise emocional — pode ser motivo de constrangimento profundo para a criança no futuro, afetando seu desenvolvimento psicológico, sua autoestima e sua autoimagem. Estudos demonstram que adolescentes frequentemente expressam arrependimento e constrangimento ao descobrir que seus pais compartilharam fotos suas nas redes sociais sem seu consentimento (KREIN, 2026). Esse constrangimento pode ser especialmente intenso quando a criança chega à adolescência e começa a desenvolver consciência de si mesma e preocupação com sua imagem social.Além disso, a exposição contínua de detalhes da vida cotidiana — nome completo, data de nascimento, escola, rotina diária, localização geográfica — facilita o rastreamento por predadores sexuais, criminosos e outros atores maliciosos. Um predador pode monitorar as postagens de um pai para aprender quando uma criança estará em um local específico em um horário específico, facilitando o sequestro ou o abuso. Muitos pais não percebem que as informações que compartilham, quando combinadas, criam um retrato completo da vida de seus filhos. Uma foto da criança em frente à escola, combinada com uma postagem sobre a rotina matinal, pode ser suficiente para que um predador determine quando e onde a criança estará vulnerável (KREIN, 2026).

Outro risco tangível e bem documentado é o roubo de identidade. O compartilhamento de nomes completos, datas de nascimento, nomes de escolas, nomes de animais de estimação (frequentemente utilizados em senhas) e outras informações sensíveis fornece a cibercriminosos os elementos necessários para fraudes financeiras e apropriação indébita da identidade da criança. Pesquisas indicam que crianças cujas informações foram amplamente compartilhadas *online* têm maior risco de sofrer roubo de identidade na vida adulta, com consequências financeiras e legais que podem durar décadas (KREIN, 2026). Alguns estudos sugerem que o roubo de identidade infantil pode não ser descoberto até que a criança chegue à vida adulta e tente obter crédito ou um emprego.Agravando significativamente esse cenário já preocupante, o recente avanço das ferramentas de Inteligência Artificial (IA) generativa introduziu ameaças de proporções sem precedentes e inimagináveis. A tecnologia deepfake permite a criação de mídias sintéticas altamente realistas a partir de imagens e vídeos legítimos, utilizando técnicas de aprendizado profundo para manipular ou gerar conteúdo visual e de áudio. De acordo com a Child Rescue Coalition, fotos de crianças publicadas inocentemente nas redes sociais estão sendo capturadas, armazenadas em grandes bancos de dados, e manipuladas por ferramentas de IA para criar material de abuso sexual infantil (CSAM) gerado por inteligência artificial

(CHILD RESCUE COALITION, s.d.). Essa prática, conhecida como “nudificação”, utiliza algoritmos para remover ou alterar roupas em fotos de crianças, criando imagens sexualizadas completamente falsas.A Organização das Nações Unidas (ONU) e o UNICEF emitiram alertas contundentes e sem precedentes sobre o aumento exponencial de casos de “nudificação” de crianças por meio de ferramentas de IA. Em 2026, o UNICEF declarou inequivocamente que “o abuso por *deepfake* é abuso”, ressaltando que, mesmo quando a imagem é gerada artificialmente, se ela utiliza a identidade de uma criança real, esta é diretamente vitimizada, causando danos psicológicos devastadores e normalizando a exploração sexual infantil (UNICEF, 2026). Um relatório conjunto do UNICEF, ECPAT e INTERPOL revelou que, em um estudo realizado em 11 países, pelo menos 1,2 milhão de crianças relataram ter tido suas imagens manipuladas em *deepfake*s sexuais no ano anterior. Em alguns países, isso representa 1 em cada 25 crianças — o equivalente a uma criança em uma sala de aula típica.Além dos *deepfakes* sexuais, a IA está sendo utilizada para aprimorar técnicas de grooming *online* (aliciamento). Predadores agora utilizam algoritmos sofisticados para analisar o comportamento *online* de uma criança, suas preferências, seus interesses, seu estado emocional e suas vulnerabilidades psicológicas, permitindo-lhes personalizar suas abordagens de forma extremamente eficaz. Um predador pode utilizar IA para identificar crianças solitárias, deprimidas ou que buscam validação social, e então criar personas falsas que correspondem precisamente aos interesses e desejos da criança-alvo. Essa manipulação pode ser extraordinariamente convincente, especialmente quando o predador utiliza IA para gerar imagens falsas de um “amigo” que corresponde perfeitamente aos interesses da criança (CHILD RESCUE COALITION, s.d.).Tais inovações tecnológicas transformaram o sharenting de uma mera indiscrição parental ou falta de julgamento em um vetor de risco crítico e iminente para a segurança, privacidade e bem-estar das crianças. O que antes era considerado um comportamento inócuo — compartilhar fotos de filhos nas redes sociais — agora pode ter consequências devastadoras e permanentes. A pegada digital criada pelo sharenting, quando combinada com as capacidades de IA moderna, representa uma ameaça existencial à privacidade e à segurança das crianças, exigindo uma resposta urgente e coordenada de pais, plataformas, legisladores e da sociedade como um todo.

4 O PAPEL DO ORDENAMENTO JURÍDICO BRASILEIRO NA PROTEÇÃO DE DADOS INFANTIS

Frente à vulnerabilidade crescente das crianças no ambiente virtual, o ordenamento jurídico brasileiro tem buscado, ainda que de forma gradual e às vezes insuficiente, adaptar-se para oferecer respostas adequadas e proporcionais aos desafios contemporâneos. O marco regulatório mais significativo nesse sentido foi a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), que dedicou um regime protetivo específico e diferenciado para crianças e adolescentes em seu art 14, reconhecendo implicitamente que menores requerem proteção especial em relação ao tratamento de seus dados pessoais. Essa lei, que entrou em vigor em 2020, representa um marco importante na história do direito digital brasileiro, alinhando-se com tendências internacionais de proteção de dados e privacidade. A LGPD estabelece, como premissa basilar e inegociável, que o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado sempre em seu "melhor interesse", princípio que se tornou central na jurisprudência e na doutrina de proteção de menores. O parágrafo 1º do art 14 exige que o tratamento de dados de crianças seja realizado mediante o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, estabelecendo um padrão mais rigoroso do que aquele aplicável aos adultos (GARCIA; NUNES, 2021). Esse requisito reconhece que crianças não possuem capacidade jurídica para consentir autonomamente e que, portanto, seus representantes legais devem exercer essa função protetiva. No entanto, o consentimento parental não é absoluto; deve ser sempre orientado pelo melhor interesse da criança e não pode ser utilizado para justificar práticas abusivas ou exploratórias. A lei também impõe aos controladores de dados (empresas e organizações que coletam e utilizam dados) o dever de não condicionar a participação de crianças em jogos, aplicações de *internet* ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade (art. 14, § 4º). Esse dispositivo é particularmente importante porque reconhece uma prática comum em que plataformas exigem dados excessivos como condição para acesso a serviços. Por exemplo, um jogo *online* pode exigir que uma criança forneça seu endereço completo, número de telefone, data de nascimento e outras informações sensíveis para criar uma conta, quando na verdade apenas um nome de usuário e uma senha seriam necessários. A LGPD proíbe essa prática exploratória, estabelecendo que apenas dados essenciais podem ser coletados.

Além disso, a lei exige que as informações sobre o tratamento de dados sejam fornecidas de maneira simples, clara e acessível, adequada ao entendimento da criança (art. 14, § 6º). Isso significa

que os termos de uso e políticas de privacidade, frequentemente escritos em linguagem jurídica complexa e inacessível, devem ser traduzidos em linguagem que uma criança possa compreender. Muitas plataformas ainda não cumprem adequadamente esse requisito, fornecendo apenas versões adultas de seus termos de uso. A lei também reconhece que diferentes crianças em diferentes idades possuem diferentes capacidades de compreensão, exigindo que as informações sejam adaptadas às "características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário", com uso de "recursos audiovisuais quando adequado" (LGPD, art. 14, § 6º).

Apesar dos avanços significativos trazidos pela LGPD, a doutrina jurídica aponta desafios interpretativos e práticos substanciais na sua aplicação. O requisito do consentimento parental, embora necessário e bem-intencionado, pode se revelar insuficiente se os próprios pais não possuem letramento digital adequado para compreender os riscos envolvidos nos termos de uso e nas políticas de privacidade das plataformas (FERNANDES; MEDON, 2021). Muitos pais simplesmente clicam em "aceitar" sem ler os termos, confiando que as plataformas estão agindo de boa fé. Além disso, há uma assimetria de poder significativa: as plataformas possuem recursos legais e técnicos vastamente superiores aos dos pais individuais, permitindo-lhes estruturar os termos de forma a maximizar a coleta de dados enquanto minimizam a responsabilidade legal.

Ademais, a legislação precisa ser interpretada em conjunto com outros diplomas legais para formar um microssistema coerente de proteção digital infantojuvenil. O Marco Civil da Internet (Lei nº 12.965/2014), que antecedeu a LGPD, estabelece princípios fundamentais para a governança da *internet* no Brasil, incluindo a proteção da privacidade e da liberdade de expressão. O Estatuto da Criança e do Adolescente (ECA - Lei nº 8.069/1990), embora tenha sido promulgado antes da era digital, continua sendo o fundamento constitucional para a proteção de menores e deve ser interpretado de forma evolutiva para abranger os desafios contemporâneos. A Constituição Federal de 1988, em seus arts 5º e 227, estabelece o fundamento constitucional para a proteção de direitos fundamentais, incluindo privacidade e proteção integral da criança.

No cenário internacional, legislações como a Children's Online Privacy Protection Act (COPPA) nos Estados Unidos e o General Data Protection Regulation (GDPR) na União Europeia também buscam impor limites rigorosos à coleta de dados de menores, servindo de paradigma para o aprimoramento contínuo da regulação brasileira. O GDPR, em particular, estabelece requisitos ainda mais rigorosos do que a LGPD em alguns aspectos, exigindo consentimento afirmativo e explícito de crianças maiores de 16 anos (ou menores de 16 com consentimento parental) para qualquer tratamento

de dados. A COPPA, por sua vez, proíbe completamente a coleta de dados de crianças menores de 13 anos sem consentimento parental verificável, estabelecendo um padrão muito mais protetor do que a LGPD, que permite coleta com consentimento parental sem verificação adicional.

5 A AUTORIDADE PARENTAL E A RESPONSABILIZAÇÃO DOS PAIS NA ERA DIGITAL

A proteção da privacidade da criança na *internet* não pode prescindir da atuação ativa, consciente e responsável dos pais ou responsáveis legais. O poder familiar (ou autoridade parental), previsto nos arts 1.630 a 1.690 do Código Civil Brasileiro, engloba não apenas o dever tradicional de sustento, guarda e educação, mas também, na contemporaneidade, o dever inegociável de proteção integral, que se estende necessariamente ao ambiente digital. A autoridade parental é um direito-dever, ou seja, não é um direito que os pais possam exercer livremente conforme sua vontade, mas um direito que deve ser exercido sempre em conformidade com o melhor interesse da criança e com os limites estabelecidos pela lei.

A prática do sharenting levanta um aparente conflito entre o direito à liberdade de expressão dos pais (garantido pelo art 5º, inciso IX, da Constituição Federal) e o direito à privacidade e à imagem dos filhos (garantido pelo artigo 5º, inciso X). No entanto, à luz do princípio do melhor interesse da criança, que é um princípio fundamental do direito infantojuvenil brasileiro e internacional, os direitos da personalidade do menor devem prevalecer sobre a liberdade de expressão dos pais. Os pais exercem a representação legal dos filhos para proteger seus interesses, e não para dispor de sua imagem de forma a colocá-los em risco ou a facilitar sua exploração. A Convenção sobre os Direitos da Criança, ratificada pelo Brasil, estabelece explicitamente que o melhor interesse da criança deve ser consideração primordial em todas as ações que lhe digam respeito.

A doutrina jurídica brasileira, particularmente aquela desenvolvida por especialistas em direito de família e direitos da personalidade, tem debatido extensivamente o conceito de “abandono digital”, que ocorre quando os pais negligenciam o dever de fiscalizar, orientar e proteger o acesso dos filhos à *internet*, deixando-os vulneráveis a ameaças virtuais graves. Esse conceito, embora ainda não formalmente reconhecido na legislação, tem sido invocado em discussões sobre responsabilidade parental. A ausência de supervisão, bem como a exposição imprudente e negligente promovida pelos próprios pais, pode configurar violação dos deveres inerentes ao poder familiar e, em casos extremos, pode justificar intervenção estatal, incluindo a perda da guarda (GARCIA; NUNES, 2021). O art 1.638 do Código Civil estabelece que o poder familiar pode ser perdido “por ato judicial” quando o pai ou a

mãe “deixar o filho em abandono”, e embora a lei não especifique qual tipo de abandono, a jurisprudência tem interpretado esse conceito de forma evolutiva.

A responsabilização parental, portanto, deve ser compreendida em duas vertentes complementares e igualmente importantes: a preventiva e a reparatória. Na vertente preventiva, exige-se dos pais a adoção de medidas concretas de letramento digital, o estabelecimento de diálogos abertos e honestos com os filhos sobre os perigos reais da *internet*, a configuração adequada de ferramentas de privacidade nas plataformas, o monitoramento responsável da atividade *online* dos filhos, e o exercício da moderação e do bom senso ao compartilhar conteúdos familiares *online* (KREIN, 2026). Isso não significa que os pais devem ser paranóicos ou proibitivos, mas que devem agir com prudência e consideração pelos direitos de seus filhos.

Na vertente reparatória, os pais podem ser chamados a responder civilmente pelos danos causados a terceiros por atos ilícitos praticados por seus filhos na *internet* (como o cyberbullying, a difamação ou o compartilhamento não autorizado de imagens), conforme estabelecido pelo art 932 do Código Civil, que responsabiliza os pais pelos atos ilícitos de seus filhos menores. Além disso, e ainda mais importante, os pais podem, em tese, ser responsabilizados pelos danos causados aos próprios filhos em decorrência de exposição indevida e negligente na *internet*. Embora ainda haja poucos casos de responsabilização parental por sharenting excessivo nos tribunais brasileiros, a tendência internacional sugere que essa será uma área crescente de litígio (GARCIA; NUNES, 2021).

Para mitigar efetivamente os riscos das inovações tecnológicas contemporâneas, como a inteligência artificial e os deepfakes, a conscientização parental e a educação são a primeira e mais eficaz linha de defesa. Os pais devem compreender que cada foto compartilhada, cada informação pessoal divulgada, contribui para a construção de uma pegada digital que pode ter consequências permanentes. Reduzir a pegada digital das crianças, evitar o compartilhamento de imagens em perfis públicos, utilizar configurações de privacidade restritivas, e respeitar a autonomia progressiva do menor ao solicitar seu consentimento antes de postar são práticas fundamentais para salvaguardar a dignidade infantojuvenil na era digital.

Além disso, os pais devem estar cientes de que a responsabilidade não termina com a decisão de não compartilhar ou de compartilhar com restrições. Os pais também têm o dever de educar seus filhos sobre privacidade digital, sobre a importância de proteger informações pessoais, sobre os riscos de predadores *online*, e sobre a necessidade de pensar criticamente sobre o que compartilham e com quem. Essa educação deve ser contínua, adaptada à idade e ao nível de desenvolvimento da criança, e

deve evoluir conforme a criança cresce e enfrenta novos desafios digitais. A pesquisa demonstra que crianças cujos pais as educam sobre privacidade digital têm menor risco de sofrer exploração *online* (KREIN, 2026).

6 INOVAÇÕES TECNOLÓGICAS EMERGENTES E RISCOS ESPECÍFICOS

O avanço acelerado das inovações tecnológicas, particularmente no campo da inteligência artificial, tem criado novos e sofisticados vetores de risco para as crianças. Além dos deepfakes e da "nudificação" digital já mencionados, existem outras ameaças emergentes que merecem atenção especial. Os algoritmos de recomendação, por exemplo, são projetados para manter os usuários engajados o máximo possível, frequentemente recomendando conteúdo cada vez mais extremo ou prejudicial. Para crianças e adolescentes, que ainda estão desenvolvendo sua capacidade de julgamento crítico e são particularmente suscetíveis a influência social, esses algoritmos podem criar "bolhas de filtro" que as expõem a conteúdo radicalizado, violento ou que promove automutilação ou suicídio (UN NEWS, 2026).

A discriminação algorítmica é outra preocupação crescente. Os algoritmos utilizados por plataformas e por empresas que coletam dados de crianças frequentemente incorporam vieses presentes nos dados de treinamento, levando a decisões discriminatórias baseadas em raça, gênero, classe socioeconômica ou outras características protegidas. Uma criança de uma minoria racial pode receber recomendações de conteúdo estereotipado ou prejudicial, enquanto uma criança de uma família de baixa renda pode ser direcionada para publicidade de produtos predatórios. Esses vieses algorítmicos podem ter impactos duradouros na autoestima, nas oportunidades educacionais e nas perspectivas de vida das crianças.

A coleta de dados biométricos de crianças é outra área de preocupação emergente. Alguns aplicativos e dispositivos coletam dados biométricos como reconhecimento facial, impressões digitais, ou até mesmo análise de voz de crianças. Esses dados são extremamente sensíveis e permanentes — ao contrário de uma senha que pode ser alterada, uma impressão digital não pode ser mudida. Se esses dados forem vazados ou utilizados indevidamente, as consequências podem ser graves e duradouras. A LGPD reconhece dados biométricos como uma categoria especial de dados sensíveis, mas a proteção oferecida ainda pode ser insuficiente.

Os brinquedos conectados ("Internet of Toys") representam outra fronteira de risco. Brinquedos inteligentes que se conectam à *internet* e coletam dados sobre as atividades, preferências e até mesmo

conversas das crianças estão se tornando cada vez mais comuns. Esses dispositivos frequentemente possuem câmeras, microfones e capacidades de rastreamento de localização. Se não forem adequadamente protegidos, podem ser hackeados, permitindo que predadores ouçam ou vejam crianças em ambientes privados. Além disso, os dados coletados por esses brinquedos frequentemente são compartilhados com terceiros para fins de marketing, criando um fluxo contínuo de informações sensíveis sobre as crianças.

A realidade aumentada (AR) e a realidade virtual (VR) apresentam desafios únicos. Essas tecnologias imersivas podem ser utilizadas para criar experiências prejudiciais ou exploratórias para crianças. Por exemplo, um ambiente de realidade virtual poderia ser projetado para expor uma criança a conteúdo sexual ou violento de forma particularmente impactante. Além disso, essas tecnologias coletam dados detalhados sobre os movimentos, as ações e as reações emocionais do usuário, criando perfis comportamentais extremamente granulares.

A manipulação comportamental através de IA é talvez uma das ameaças mais insidiosas. Algoritmos sofisticados podem ser utilizados para identificar vulnerabilidades psicológicas em crianças e para explorar essas vulnerabilidades de forma sistemática. Uma criança solitária pode ser direcionada para comunidades *online* que a isolam ainda mais. Uma criança com baixa autoestima pode ser direcionada para conteúdo que a faz sentir pior sobre si mesma. Uma criança com tendências viciantes pode ser direcionada para conteúdo e aplicativos especificamente projetados para ser viciantes. Tudo isso acontece de forma invisível, mediada por algoritmos que os pais e até mesmo a criança não conseguem compreender ou controlar.

A monetização da infância através de plataformas como TikTok, YouTube e Instagram também representa um risco específico. Quando crianças se tornam “kidfluencers” (influenciadores mirins), sua vida privada é transformada em conteúdo comercializável. Os pais, motivados pela perspectiva de ganhos financeiros, podem expor seus filhos a riscos crescentes, compartilhando conteúdo cada vez mais íntimo ou sensível para manter o engajamento e as visualizações. Estudos demonstram que algoritmos frequentemente favorecem conteúdo que mostra crianças em situações de vulnerabilidade, constrangimento ou até mesmo abuso, criando incentivos perversos para que os pais compartilhem conteúdo prejudicial (UN NEWS, 2026).

7 DIREITO COMPARADO: MODELOS INTERNACIONAIS DE PROTEÇÃO

O Brasil não está sozinho em sua luta para proteger crianças no ambiente digital. Diversos países e regiões ao redor do mundo têm desenvolvido legislações e políticas para enfrentar os desafios específicos da privacidade infantil na era digital. Compreender essas abordagens comparativas pode oferecer insights valiosos e servir como base para o aprimoramento contínuo da regulação brasileira. Os Estados Unidos, através da Children's Online Privacy Protection Act (COPPA), estabeleceu um dos primeiros marcos regulatórios específicos para proteção de dados de crianças *online*. A COPPA, promulgada em 1998 e atualizada várias vezes desde então, proíbe a coleta de dados de crianças menores de 13 anos sem consentimento parental verificável. Embora a COPPA tenha sido pioneira, ela possui limitações significativas, particularmente o fato de que a idade limite de 13 anos é arbitrária e não reflete o desenvolvimento cognitivo real das crianças.

A União Europeia adotou uma abordagem mais rigorosa através do General Data Protection Regulation (GDPR), que entrou em vigor em 2018. O GDPR estabelece que crianças menores de 16 anos (ou menores de 13 em alguns Estados-membros) não podem consentir autonomamente com o tratamento de seus dados; o consentimento deve ser dado por seus representantes legais. Além disso, o GDPR exige que as informações sobre o tratamento de dados sejam fornecidas em linguagem clara e acessível, adequada à compreensão da criança. O GDPR também estabelece o princípio de "privacy by design", exigindo que as organizações considerem privacidade desde o início do desenvolvimento de novos produtos e serviços, e não como uma consideração posterior.

A Austrália tomou uma abordagem radical e controversa em 2025, tornando-se o primeiro país do mundo a banir contas de redes sociais para crianças menores de 16 anos. O governo australiano argumentou que os riscos dos conteúdos compartilhados nas redes sociais — incluindo conteúdo prejudicial, *cyberbullying* e exploração — superam em muito os benefícios potenciais. Embora essa abordagem seja extrema e levante questões sobre liberdade de expressão e acesso à informação, ela reflete uma crescente preocupação internacional com os impactos negativos das redes sociais na saúde mental e no bem-estar das crianças. Vários outros países, incluindo Malásia, Reino Unido, França e Canadá, estão considerando legislações similares.A Coreia do Sul implementou a Juvenile Protection Act, que estabelece proteções específicas para menores *online*, incluindo restrições ao acesso a conteúdo prejudicial e requisitos de verificação de idade. O Japão, por sua vez, adotou a Act on the Protection of Personal Information (APPI), que, embora não seja específica para crianças, oferece proteções robustas para dados pessoais em geral, incluindo dados de menores. Esses exemplos

internacionais demonstram uma tendência global crescente de reconhecer que crianças requerem proteção especial no ambiente digital e que as legislações existentes muitas vezes são insuficientes.A Organização das Nações Unidas (ONU) e agências especializadas como o UNICEF têm desempenhado um papel importante na promoção de padrões internacionais para proteção de crianças *online*. A Convenção sobre os Direitos da Criança, ratificada por quase todos os países do mundo (com a notável exceção dos Estados Unidos), estabelece que os direitos das crianças, incluindo privacidade e proteção contra exploração, devem ser protegidos. Recentemente, a ONU emitiu diretrizes sobre inteligência artificial e direitos das crianças, reconhecendo os riscos específicos que a IA representa para menores e chamando por ação coordenada de governos, empresas e da sociedade civil.A tendência internacional também aponta para uma responsabilização crescente das plataformas de tecnologia. Muitos países estão implementando legislações que exigem que as plataformas implementem medidas de proteção específicas para crianças, como controles parentais robustos, ferramentas de denúncia de conteúdo prejudicial, e algoritmos que não promovam conteúdo prejudicial para menores.

8 CONSIDERAÇÕES FINAIS

O avanço a das inovações tecnológicas e a hiperconectividade contemporânea impuseram novos e complexos paradigmas para a proteção dos direitos da personalidade, afetando de forma aguda e profunda as crianças e os adolescentes. A superexposição digital, impulsionada pelo fenômeno amplamente disseminado do sharenting e agravada por tecnologias emergentes como a inteligência artificial generativa, os deepfakes, os algoritmos de recomendação sofisticados e a coleta massiva de dados, converteu o ambiente virtual em um terreno fértil para violações de privacidade, exploração sexual, manipulação comportamental e danos psicológicos duradouros. O que antes era considerado uma mera indiscrição parental ou falta de julgamento — compartilhar fotos de filhos nas redes sociais — transformou-se em um vetor de risco crítico e iminente para a segurança, privacidade e bem-estar das crianças.

O ordenamento jurídico brasileiro, através da Constituição Federal de 1988, do Estatuto da Criança e do Adolescente (ECA) de 1990, do Marco Civil da Internet de 2014, e mais recentemente da Lei Geral de Proteção de Dados Pessoais (LGPD) de 2018, oferece um arcabouço protetivo robusto e multifacetado, fundamentado no princípio fundamental do melhor interesse da criança. Esses diplomas legais reconhecem que crianças e adolescentes são sujeitos de direitos em condição peculiar de desenvolvimento, merecedores de proteção especial não apenas do Estado e da família, mas de toda a

sociedade. Contudo, a eficácia dessa proteção legal depende intrinsecamente da atuação responsável, consciente e ativa de múltiplos atores: o Estado, através da regulação e fiscalização; as plataformas de tecnologia, através da implementação de medidas de proteção desde a concepção dos produtos; e, fundamentalmente, a família.

A autoridade parental deve ser ressignificada e reinterpretada para incorporar, de forma inegociável, o dever de cuidado, proteção e educação no ecossistema digital contemporâneo. A responsabilização dos pais não se limita a responder por danos causados a terceiros ou a sofrer sanções legais por negligência; vai muito além. Trata-se de uma responsabilidade moral, social e jurídica de atuar como guardiões vigilantes da identidade, da privacidade, da segurança e da dignidade de seus filhos no ambiente virtual. Isso exige que os pais desenvolvam letramento digital adequado, que mantenham diálogos abertos e honestos com seus filhos sobre os perigos reais da *internet*, que configurem adequadamente as ferramentas de privacidade nas plataformas, que monitorem responsavelmente a atividade *online* dos filhos, e que exercitem moderação e bom senso ao compartilhar conteúdos familiares *online*.A educação digital é absolutamente fundamental. Crianças e adolescentes devem ser educados sobre a importância de proteger informações pessoais, sobre os riscos de predadores *online*, sobre como reconhecer conteúdo prejudicial, sobre a necessidade de pensar criticamente sobre o que compartilham e com quem, e sobre as implicações de longo prazo de suas ações *online*. Essa educação deve ser contínua, adaptada à idade e ao nível de desenvolvimento da criança, e deve evoluir conforme a criança cresce e enfrenta novos desafios digitais. Os pais, as escolas e a sociedade como um todo têm um papel crucial a desempenhar nessa educação.

Somente através da conjugação de esforços coordenados e sincronizados entre o Estado (através de regulação efetiva e fiscalização rigorosa), as plataformas de tecnologia (através da implementação de medidas de proteção robustas desde a concepção dos produtos, do privacy by design, e da responsabilidade corporativa), a família (através da educação digital e do exercício responsável da autoridade parental), e a sociedade civil (através da conscientização e da advocacia pelos direitos das crianças), será possível garantir que as crianças e adolescentes desfrutem plenamente das oportunidades e benefícios oferecidos pelo mundo digital sem o sacrifício de seus direitos mais fundamentais e inalienáveis. A proteção da privacidade, da imagem e da dignidade das crianças na era digital não é uma questão meramente técnica ou administrativa, mas uma questão fundamental de direitos humanos, de justiça social e de responsabilidade intergeracional.

REFERÊNCIAS

ALBERS, Susan D. Sharing Isn't Always Caring: The Risks and Dangers of 'Sharenting'. Cleveland Clinic, 29 maio 2024. Disponível em: https://health.clevelandclinic.org/sharenting. Acesso em: 22 jul. 2026.

ANDOH, Efua. What you need to know before sharing your child's life online. Monitor on Psychology, v. 57, n. 4, p. 24, 1 jun. 2026. Disponível em: https://www.apa.org/monitor/2026/06/parents-children-sharing-online. Acesso em: 22 jul. 2026.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, DF, 16 jul. 1990.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CHILD RESCUE COALITION. The Dark Side of AI: Risks to Children. [s.d.]. Disponível em: https://childrescuecoalition.org/educations/the-dark-side-of-ai-risks-to-children/. Acesso em: 22 jul. 2026.

FERNANDES, Elora; MEDON, Filipe. Proteção de Crianças e Adolescentes na LGPD: desafios interpretativos. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ, Rio de Janeiro, v. 4, n. 2, p. 1-30, maio/ago. 2021.

GARCIA, Maria Carolina Brunharotto; NUNES, Paula Freire Santos Andrade. Tratamento de dados pessoais de crianças e adolescentes: proteção e livre desenvolvimento do menor cercados pela LGPD e responsabilidade parental. Instituto Brasileiro de Direito de Família (IBDFAM), 7 abr. 2021. Disponível em: https://ibdfam.org.br/artigos/1673. Acesso em: 22 jul. 2026.

KREIN, Meghan. The Dangers of Sharenting: Protecting Children's Privacy in a Digital Age. Childhelp, 9 fev. 2026. Disponível em: https://childhelp.org/the-dangers-of-sharenting-protecting-childrens-privacy-in-a-digital-age/. Acesso em: 22 jul. 2026.

SIEBENEICHLER DE ANDRADE, Fabio. Reflexões sobre o direito à privacidade de crianças e adolescentes em perspectiva comparada. Pensar - Revista de Ciências Jurídicas, Fortaleza, v. 28, n. 2,

p. 1-17, jun. 2023. Disponível em: https://ojs.unifor.br/rpen/article/view/13378. Acesso em: 22 jul. 2026.

UNICEF. Children and Online Privacy in the Digital Age. Brief for Policymakers. 2019. Disponível em: https://www.unicef.org/childrightsandbusiness/media/226/file/Brief-Children-and-Online-Privacy.pdf. Acesso em: 22 jul. 2026.

UNICEF. 'Deepfake abuse is abuse': Statement by UNICEF on AI-generated sexualised images of children. Nova York, 4 fev. 2026. Disponível em: https://www.unicef.org/press-releases/deepfake-abuse-is-abuse. Acesso em: 22 jul. 2026.

UN NEWS. From deepfakes to grooming: UN warns of escalating AI threats to children. 26 jan. 2026. Disponível em: https://news.un.org/en/story/2026/01/1166827. Acesso em: 22 jul. 2026.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO (ITS Rio). Privacidade e Proteção de Dados de Crianças e Adolescentes. 2. ed. Rio de Janeiro: ITS Rio, 2016. Disponível em: https://itsrio.org/pt/publicacoes/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes-2-edicao/. Acesso em: 22 jul. 2026.