

OS PAIS VEEM A CRIANÇA; A PLATAFORMA PODE VER O PERFIL COMPORTAMENTAL

Assimetria de capacidade preventiva e limites da responsabilização familiar na infância digital

PARENTS SEE THE CHILD; THE PLATFORM MAY SEE THE BEHAVIORAL PROFILE

Jandislei Antonio Genova

Advogado inscrito na OAB/SP, bacharel em Direito pela Universidade Paulista (UNIP), especialista em Gestão em Saúde, escritor e pesquisador jurídico independente em Direito e Inteligência Artificial. Autor da trilogia formada por *Autonomia decisória na era da inteligência artificial*, *A monetização da vulnerabilidade* e *A soberania capturada*.

ORCID: <https://orcid.org/0009-0008-8187-6309> | E-mail: jandislei.genova@gmail.com

Nota do autor. Este artigo desenvolve, em formulação autônoma e ampliada, premissas da obra *A monetização da vulnerabilidade: plataformas digitais, vício, ódio e responsabilidade civil na era algorítmica*, no prelo pela Editora Dialética. A análise considera a legislação e as fontes disponíveis até 14 de agosto de 2026.

RESUMO

O discurso segundo o qual a segurança digital de crianças e adolescentes dependeria principalmente de pais e professores reconhece deveres reais, mas pode ocultar uma diferença relevante de meios preventivos. Este artigo investiga se a responsabilidade compartilhada pela proteção infantojuvenil autoriza transferir o principal encargo de prevenção aos atores que não projetam nem operam o ambiente digital. Adota-se pesquisa jurídico-documental, qualitativa e exploratória, com análise de legislação, jurisprudência, documentos institucionais e literatura científica identificados até 14 de agosto de 2026. Propõe-se a **assimetria de capacidade preventiva** como lente analítica para comparar cinco dimensões relativas a uma funcionalidade e a um risco delimitados: controle arquitetural, acesso a dados pertinentes, capacidade analítica, temporalidade e escala de intervenção, e meios de mitigação e verificação. Previsibilidade, vulnerabilidade do grupo, benefício econômico e alternativa menos lesiva funcionam como fatores moduladores externos, não como componentes do índice heurístico proposto. A análise sustenta que responsabilidades familiares, pedagógicas, empresariais e estatais coexistem, mas não são equivalentes. A categoria não estabelece responsabilidade automática nem substitui os pressupostos aplicáveis ao caso concreto: defeito ou ilicitude, dano e nexos causal ou concausal devem ser demonstrados, com consideração de causas concorrentes e da esfera efetiva de atuação de cada agente. Conclui-se que educação digital e supervisão familiar são indispensáveis, porém não substituem segurança por concepção, transparência qualificada e deveres proporcionais de mitigação do fornecedor.

Palavras-chave: infância digital; assimetria de capacidade preventiva; arquitetura informacional; responsabilidade civil; ECA Digital.

ABSTRACT

The claim that children's digital safety depends mainly on parents and teachers recognizes genuine duties but may obscure a relevant disparity in preventive means. This article examines whether shared responsibility for protecting children and adolescents permits shifting the primary preventive burden to actors who neither design nor operate the digital environment. It adopts a qualitative, exploratory legal-documentary method and analyzes legislation, case law, institutional documents, and scientific literature identified through August 14, 2026. The article proposes **asymmetry of preventive capacity** as an analytical lens for comparing five dimensions tied to a defined feature and risk: architectural control, access to relevant data, analytical capacity, timing and scale of intervention, and means of mitigation and verification. Foreseeability, group vulnerability, economic benefit, and the availability of a less harmful alternative operate as external modifiers rather than components of the proposed heuristic index. The analysis argues that family, educational, corporate, and governmental responsibilities coexist but are not equivalent. The category does not establish automatic liability or displace the legal requirements applicable

to a concrete case: defect or unlawfulness, damage, and a causal or contributory nexus must be demonstrated, while considering concurrent causes and each actor's effective sphere of action. The article concludes that digital education and family supervision are indispensable, but cannot replace safety by design, qualified transparency, and providers' proportionate duties to mitigate risk.

Keywords: digital childhood; asymmetry of preventive capacity; information architecture; civil liability; children's digital protection.

1 INTRODUÇÃO

É recorrente atribuir a diferença entre experiências digitais mais ou menos seguras exclusivamente à atuação dos pais. A explicação reconduz um problema coletivo ao espaço doméstico, identifica um agente aparentemente capaz de agir e preserva a intuição de que educação, diálogo e presença ainda importam. Essa intuição é correta. Pais e responsáveis não são espectadores facultativos da vida digital dos filhos; professores tampouco podem ignorar os efeitos da tecnologia sobre aprendizagem e convivência. O erro começa quando uma obrigação real é convertida em explicação suficiente e, depois, em causa de exclusão da responsabilidade de quem concebe, testa, modifica e monetiza o ambiente no qual a interação ocorre.

O problema não está em reconhecer deveres familiares. Está em presumir que todos os participantes dispõem dos mesmos instrumentos preventivos. Uma família pode conversar, estabelecer horários, conhecer mudanças de humor e interromper o acesso a um dispositivo. A escola pode formular regras, desenvolver letramento digital e identificar padrões coletivos de distração, conflito ou sofrimento. O fornecedor, por sua vez, pode alterar a configuração-padrão de milhões de contas, inserir um ponto natural de parada, reduzir notificações, desativar personalização, modificar critérios de recomendação, testar salvaguardas e observar sinais agregados de uso. Cada ator conhece uma dimensão do problema; nenhum possui conhecimento total. Contudo, em relação aos riscos produzidos ou amplificados pela própria arquitetura do serviço, o domínio de intervenção não é equivalente.

Essa diferença tornou-se juridicamente mais visível no Brasil. A Constituição Federal e o Estatuto da Criança e do Adolescente estabelecem deveres da família, da sociedade e do Estado sob o regime da proteção integral e da prioridade absoluta. A Lei nº 15.211/2025 — Estatuto Digital da Criança e do Adolescente, doravante ECA Digital — preservou o cuidado ativo e contínuo dos responsáveis, mas simultaneamente impôs aos fornecedores deveres de prevenção, segurança por padrão, gerenciamento de riscos, supervisão parental acessível e limitação de recursos que sustentem ou prolonguem artificialmente o uso. O Decreto nº 12.880/2026 foi ainda mais explícito ao tratar de pontos de parada ocultos, acionamento de conteúdo não solicitado, recompensas por tempo de uso, notificações excessivas e arquiteturas que explorem vulnerabilidades cognitivas e etárias (BRASIL, 2025; BRASIL, 2026).

Surge, então, a pergunta de pesquisa: **a responsabilidade compartilhada autoriza transferir o principal encargo preventivo a pais e professores quando o fornecedor possui superior capacidade de observar, controlar e mitigar riscos arquiteturais?** A hipótese deste artigo é negativa. Compartilhar responsabilidade não significa igualar funções, meios ou intensidade dos deveres. Significa distribuir obrigações conforme a posição ocupada na cadeia de risco e segundo a capacidade concreta de prevenção.

Para demonstrá-lo, propõe-se a categoria operacional da **assimetria de capacidade preventiva**. Ela designa a diferença, entre os atores relevantes, quanto a cinco dimensões: domínio sobre a arquitetura; acesso a dados pertinentes; capacidade analítica de antecipação; velocidade e escala de intervenção; e disponibilidade de meios de mitigação. A intensidade do dever deve ainda

considerar a vulnerabilidade atingida, a previsibilidade do risco, o benefício econômico e a existência de alternativas menos lesivas.

A proposta não pretende provar que toda plataforma manipula, que todo uso produz dano ou que toda dificuldade infantojuvenil decorre de tecnologia. As evidências disponíveis recomendam cautela. O relatório de consenso das National Academies of Sciences, Engineering, and Medicine concluiu não haver base suficiente para atribuir, em nível populacional, causalidade ampla entre redes sociais e alterações de saúde de adolescentes; os efeitos podem ser benéficos, neutros ou prejudiciais e variam por sujeito, contexto e funcionalidade (NASEM, 2024). A cautela causal, entretanto, não torna racional a inércia preventiva. Ela exige que o debate migre de afirmações totais sobre “a tecnologia” para perguntas verificáveis sobre funcionalidades, populações, métricas, decisões de projeto e medidas de segurança.

O objetivo é, portanto, amplo no diagnóstico e restrito na atribuição. O artigo não substitui a análise do caso concreto nem elimina a agência humana. Oferece um modo de perguntar quem podia saber, quem podia modificar, quem se beneficiava e quem absorveu o custo. Essa mudança de perspectiva impede que o vocabulário da corresponsabilidade funcione como álibi para a concentração privada de dados e poder arquitetural.

2 DELIMITAÇÃO, MÉTODO, ESTADO DA ARTE E PREMISSAS

2.1 Recorte e estratégia documental

A pesquisa é jurídico-documental, qualitativa e exploratória; não constitui revisão sistemática, metanálise nem estudo causal. O corpus normativo compreende a Constituição Federal, o Estatuto da Criança e do Adolescente, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet, o Código de Processo Civil, a Lei Geral de Proteção de Dados Pessoais, o ECA Digital e seu regulamento. Foram igualmente examinados precedentes do Supremo Tribunal Federal e do Superior Tribunal de Justiça, atos e orientações da Agência Nacional de Proteção de Dados (ANPD), documentos do Comitê dos Direitos da Criança das Nações Unidas, da Comissão Europeia, da Federal Trade Commission (FTC), das National Academies, do Cetic.br|NIC.br, do U.S. Surgeon General e do UNICEF, além de estudos revisados por pares sobre padrões manipulativos e influência digital.

O levantamento foi encerrado em 14 de agosto de 2026. As buscas foram realizadas nos repositórios oficiais do Planalto, STF, STJ, ANPD, Comissão Europeia, FTC, ONU, UNICEF, NASEM e Cetic.br, e por DOI ou página editorial para a literatura científica. Empregaram-se, isoladamente e em combinações, os termos “proteção digital de crianças e adolescentes”, “ECA Digital”, “perfilamento”, “responsabilidade de plataformas”, “defeito do serviço”, “ônus da prova”, “arquitetura de escolha”, “padrões obscuros”, “dark patterns”, “online manipulation”, “children online safety”, “recommender systems” e “safety by design”. Foram incluídas fontes primárias ou institucionais identificáveis, decisões com pertinência para defeito, causalidade, esfera de atuação e distribuição da prova, e estudos diretamente relacionados à arquitetura de escolhas. Foram excluídos textos opinativos sem documentação verificável, materiais duplicados e estudos sem relação funcional com o problema de pesquisa.

A análise seguiu quatro operações: delimitação da funcionalidade e do risco; identificação do ator que detinha cada capacidade C-D-A-T-M; separação entre evidência empírica, inferência jurídica e proposta normativa; e teste da conclusão contra hipóteses concorrentes, inclusive ausência de defeito, causa externa exclusiva e contribuição familiar. A categoria proposta é, portanto, uma

construção analítica derivada desse corpus, não um resultado estatístico. A busca por expressões idênticas ou próximas não autoriza reivindicação de novidade absoluta; o artigo sustenta apenas a utilidade da formulação específica e de sua operacionalização.

O recorte concentra-se em serviços digitais direcionados a crianças e adolescentes ou de acesso provável por eles, especialmente aqueles que utilizam personalização, recomendação, notificações, métricas de engajamento ou interação conversacional. Serviços sem essas características ou fornecedores de pequeno porte podem apresentar capacidades substancialmente diferentes; por isso, nenhuma conclusão é transferível sem análise da funcionalidade concreta.

2.2 Estado da arte e posição da proposta

A literatura sobre arquitetura de escolha já demonstrou que interfaces não apenas exibem opções: elas podem ordenar, ocultar, tornar salientes ou dificultar alternativas. Estudos sobre *dark patterns* identificaram estratégias recorrentes de indução em interfaces e sua presença em escala, enquanto a literatura sobre manipulação on-line examina como dados e personalização podem tornar influências menos visíveis e mais ajustadas ao destinatário (GRAY et al., 2018; MATHUR et al., 2019; SUSSER; ROESSLER; NISSENBAUM, 2019). Esses trabalhos não provam dano individual nem ilicitude automática, mas afastam a premissa de neutralidade formal da interface.

No direito do consumidor, a vulnerabilidade, a segurança legitimamente esperada, o dever de informação e a posição do fornecedor na organização do serviço oferecem bases já consolidadas para investigar riscos digitais (MIRAGEM, 2024; MARTINS, 2020). Na proteção de dados, a passagem do simples segredo para o controle sobre operações de tratamento reforça a exigência de finalidade, transparência e responsabilização (DONEDA, 2021). A análise econômica dos acidentes, por sua vez, oferece a pergunta adjacente sobre qual agente pode prevenir ou reduzir determinado custo com melhores condições, sem converter eficiência em critério exclusivo de justiça (CALABRESI, 1970).

A contribuição deste artigo é mais restrita. A **assimetria de capacidade preventiva** não substitui assimetria informacional, vulnerabilidade do consumidor, segurança por concepção, dever de cuidado ou causalidade. Ela organiza essas tradições em torno de uma pergunta funcional: para o risco e a funcionalidade delimitados, quem possuía meios materiais, informacionais e decisórios para agir antes da materialização ou do agravamento do dano? A categoria pretende auxiliar auditoria, perícia, regulação e argumentação jurídica; não pretende criar um novo fator autônomo de responsabilidade.

2.3 Delimitações conceituais

Três delimitações são indispensáveis.

Primeiro, **arquitetura** não é sinônimo de conteúdo. O termo abrange a organização das escolhas e dos fluxos: o que aparece primeiro, o que permanece visível, quais opções vêm ativadas, quantas etapas são necessárias para sair, quais sinais alimentam recomendações, quando surgem alertas, recompensas ou novos conteúdos. Um debate restrito à licitude de cada postagem pode deixar intocadas as decisões do fornecedor sobre distribuição, repetição, amplificação e monetização.

Segundo, **influência** não equivale automaticamente a manipulação ilícita. Toda interface orienta condutas em algum grau. A relevância jurídica cresce quando essa orientação é opaca, explora vulnerabilidade conhecida, restringe a autodeterminação, produz risco relevante e evitável, beneficia economicamente o controlador e não é acompanhada por mitigação proporcional. É nessa convergência, e não em uma condenação abstrata do projeto de interface, que se situa a responsabilidade civil por arquitetura digital (GENOVA, 2026).

Terceiro, **risco não equivale a dano**. Deveres de prevenção podem surgir antes do dano consumado, sobretudo diante de pessoas em desenvolvimento; a reparação civil, porém, exige demonstração dos pressupostos aplicáveis. Associação estatística não basta para afirmar causalidade individual. Em litígios concretos, será necessário reconstruir exposição, funcionalidade, temporalidade, vulnerabilidade, alternativas causais e contribuição do sistema. A categoria aqui formulada auxilia essa reconstrução, mas não a substitui.

O método de atribuição adotado segue uma premissa: deveres devem acompanhar o poder de intervir. Isso não significa que o ator com maior poder responda sempre por todo resultado. Significa que ele não pode invocar a conduta de quem detinha menos controle como explicação automática para a insuficiência de suas próprias salvaguardas.

3 A SEDUÇÃO DA CULPA DOMÉSTICA

A responsabilização concentrada nos pais pode oferecer três vantagens retóricas: personaliza um sistema complexo, desloca a discussão para escolhas observáveis — permitir ou proibir, acompanhar ou omitir — e dispensa acesso às informações internas do fornecedor. O comportamento familiar costuma ser mais visível; o processo que seleciona recomendações, mede retenção, define notificações e testa interfaces pode permanecer protegido por opacidade técnica e empresarial. Forma-se, então, o risco de julgar com maior intensidade o ator sobre o qual há mais informação pública e de examinar insuficientemente o ator que possui dados operacionais sobre o serviço.

O mesmo movimento pode alcançar a escola. Professores são instados a ensinar pensamento crítico, identificar desinformação, enfrentar a intimidação sistemática virtual, administrar distração e orientar o uso de inteligência artificial. Essas tarefas fazem parte da educação contemporânea. Contudo, uma política que transforma a escola em principal barreira de contenção corre o risco de transferir a instituições sem controle sobre o produto parte substancial do custo de administrar seus efeitos.

Em determinados serviços, o problema pode ser descrito como uma inversão de governança. O fornecedor decide a arquitetura em escala; famílias e escolas administram consequências em escala local. O fornecedor modifica o ambiente antes e durante o uso; responsáveis e docentes frequentemente reagem depois que sinais de conflito, privação de sono, gasto indevido ou uso problemático se tornam perceptíveis. Grandes fornecedores podem comparar milhões de interações; a família observa uma biografia. A escola reconhece padrões coletivos, mas normalmente não acessa a lógica de recomendação que pode produzi-los ou intensificá-los.

Não se trata de declarar famílias impotentes. O conhecimento afetivo e contextual dos responsáveis é insubstituível. Uma plataforma pode inferir recorrência, preferência ou probabilidade de resposta; não conhece, por isso, o sentido integral daquela experiência na vida da criança. A tese é mais precisa: **o conhecimento da família e o conhecimento do fornecedor são distintos, mas, para prevenir riscos originados em decisões de produto, o fornecedor dispõe de um domínio técnico específico que a família não pode reproduzir.**

Os dados brasileiros ilustram essa desigualdade sem autorizarem acusações de negligência. A TIC Kids Online Brasil 2025 entrevistou presencialmente 2.370 usuários de Internet de 9 a 17 anos e seus pais ou responsáveis. Entre os jovens, 65% declararam usar inteligência artificial generativa em alguma atividade e 59% a utilizavam para pesquisar ou estudar. Entre os responsáveis, 44% afirmaram conversar com crianças e adolescentes sobre o que fazem na rede; ao buscar orientação sobre uso seguro, 50% recorriam às próprias crianças ou adolescentes e 48% a familiares ou amigos. Na

mediação técnica, 27% declararam utilizar recurso de limitação de tempo e 34% recurso de monitoramento de sites ou aplicativos (CETIC.BR, 2025a; CETIC.BR, 2025b).

Esses percentuais não medem amor, cuidado ou competência moral e não demonstram, isoladamente, assimetria causal. Eles são compatíveis, contudo, com a hipótese de que a supervisão depende de ferramentas disponíveis, conhecimento técnico, tempo, renda, organização doméstica e cooperação da própria indústria. Exigir que cada família monte, isoladamente, um sistema de defesa contra serviços continuamente atualizados confunde dever de cuidado com capacidade de engenharia.

4 RESPONSABILIDADE COMPARTILHADA NÃO É RESPONSABILIDADE EQUIVALENTE

4.1 A unidade do sistema protetivo

O artigo 227 da Constituição não elege um único guardião. Família, sociedade e Estado devem assegurar, com absoluta prioridade, direitos fundamentais de crianças e adolescentes e protegê-los de negligência, exploração e violência. O artigo 4º do ECA reproduz essa estrutura plural, enquanto o artigo 70 afirma ser dever de todos prevenir ameaças ou violações. Lidos superficialmente, esses dispositivos poderiam sustentar a ideia de uma obrigação indiferenciada. Lidos sistematicamente, conduzem à conclusão oposta: a proteção é comum, mas as prestações exigíveis variam conforme função, competência e poder de cada participante (BRASIL, 1988; BRASIL, 1990a).

O ECA Digital torna essa diferenciação inequívoca. Seu artigo 3º assegura proteção prioritária, melhor interesse e elevado nível de privacidade, proteção de dados e segurança. No mesmo dispositivo, atribui aos pais cuidado ativo e contínuo. O artigo 5º, porém, dirige aos fornecedores deveres de prevenção, proteção, informação e segurança e exige medidas técnicas que possibilitem à família prevenir acesso e uso inadequados. A família deve usar instrumentos; o fornecedor deve criá-los, torná-los acessíveis e inseri-los em uma arquitetura segura.

A distinção prossegue. O artigo 7º exige configuração mais protetiva por padrão. O artigo 8º determina gerenciamento de riscos e configurações que evitem uso compulsivo. Os artigos 16 a 18 obrigam o fornecedor a informar riscos, disponibilizar supervisão parental, permitir limitação do tempo de uso e restringir recursos de prolongamento artificial, como reprodução automática, recompensas e notificações. O artigo 18, § 2º, veda o projeto ou a manipulação de interfaces com objetivo ou efeito de comprometer autonomia, decisão ou escolha, especialmente quando enfraqueçam salvaguardas parentais. O artigo 15 impede que obrigações de um elo da cadeia eximam os demais (BRASIL, 2025).

O Decreto nº 12.880/2026 confirma que “responsabilidade compartilhada” não é cláusula de exoneração empresarial. Seu artigo 9º exige mecanismos contra uso excessivo, problemático ou compulsivo e identifica, entre os fatores de risco, ocultação de pontos naturais de parada, acionamento de conteúdo sem solicitação, recompensas por tempo e notificações excessivas. O artigo 10 alcança arquiteturas de escolha e fluxos que interfiram na autonomia ou explorem vulnerabilidades cognitivas e etárias. Para modelos de linguagem e agentes conversacionais, o artigo 11 requer transparência sobre o caráter automatizado, prevenção de manipulação comportamental, avaliação de risco algorítmico e salvaguardas ao desenvolvimento (BRASIL, 2026).

Portanto, a lei brasileira não opõe família e fornecedor. Ela organiza uma complementaridade assimétrica. Pais orientam, acompanham e aplicam controles; fornecedores antecipam riscos de produto, oferecem controles eficazes e não constroem o serviço para neutralizá-los. Professores

educam e identificam efeitos; o Estado regula, fiscaliza e provê políticas; o fornecedor responde pelo espaço de decisões técnicas que somente ele pode executar.

4.2 Diferenciação funcional dos deveres

A responsabilidade compartilhada pode ser dividida em quatro funções. A **relacional**, predominante na família, envolve presença, diálogo, percepção de mudanças, limites e autonomia progressiva. A **pedagógica**, compartilhada entre família, escola, sociedade e Estado, desenvolve competências para reconhecer publicidade e persuasão, compreender inferências e verificar fontes — em linha com o Comentário Geral nº 25 do Comitê dos Direitos da Criança (ONU, 2021). A **arquitetural**, concentrada no fornecedor, abrange padrões, recomendação, notificações, métricas, testes, fricções e salvaguardas implementáveis em escala. A **normativa e fiscalizatória**, atribuída ao poder público, converte princípios em padrões verificáveis, exige documentação, possibilita auditoria e sanciona descumprimentos.

Confundir essas funções produz duas distorções. A primeira é exigir da família uma capacidade técnica que ela não possui. A segunda é desonerar o fornecedor sob o argumento de que educação e supervisão poderiam compensar qualquer escolha de design. A educação digital é uma camada de proteção; não é uma licença para arquitetura insegura.

5 ASSIMETRIA DE CAPACIDADE PREVENTIVA

5.1 Definição

Propõe-se denominar **assimetria de capacidade preventiva** a distribuição desigual, entre atores relacionados a determinado risco, dos meios materiais, informacionais e decisórios necessários para: (a) identificar o risco antes de sua materialização; (b) estimar frequência, intensidade e grupos mais expostos; (c) modificar a fonte ou o percurso do risco; (d) intervir com velocidade e escala; e (e) verificar se a mitigação funcionou.

A categoria se distingue de três assimetrias conhecidas, embora dialogue com elas. A assimetria informacional refere-se à diferença no volume ou na qualidade de informações. A assimetria de poder de escolha descreve a desigual capacidade de estruturar alternativas. A assimetria econômica aponta a diferença de recursos e incentivos. A capacidade preventiva resulta da combinação dessas dimensões, mas tem objeto próprio: **quem consegue reduzir o risco antes que famílias, escolas ou serviços públicos tenham de reparar suas consequências?**

No ambiente digital, a resposta não é uniforme. Uma pequena aplicação sem personalização não possui a mesma capacidade de uma grande plataforma; um serviço de mensagens não controla todas as relações entre usuários; uma escola pode ter domínio integral sobre seu próprio ambiente virtual de aprendizagem; pais podem impedir o acesso a um aparelho em situações concretas. A categoria deve ser aplicada ao risco e à funcionalidade examinados, não ao rótulo genérico “plataforma”.

5.2 Cinco dimensões verificáveis

A capacidade preventiva relativa pode ser examinada por cinco dimensões:

Controle arquitetural (C). Poder de criar, ativar, modificar ou remover a funcionalidade associada ao risco, inclusive padrões, recomendação, recompensas, notificações e fluxos de saída.

Acesso a dados pertinentes (D). Disponibilidade de registros de uso, reclamações, incidentes, segmentos afetados, testes e métricas necessárias para reconhecer padrões.

Capacidade analítica e preditiva (A). Meios técnicos e humanos para detectar correlações, simular impactos, conduzir avaliações de risco e identificar grupos vulneráveis, sem pressupor que correlação corresponda a diagnóstico ou causalidade.

Temporalidade e escala de intervenção (T). Possibilidade de agir antes ou durante a exposição e de alcançar simultaneamente o universo afetado.

Meios de mitigação e verificação (M). Recursos para adotar alternativas menos lesivas, realizar testes de segurança, acompanhar resultados e corrigir efeitos adversos.

5.3 Perfil C-D-A-T-M e índice heurístico experimental

A representação principal deve ser o **perfil C-D-A-T-M**, pois ele mantém visíveis as diferenças entre as dimensões. Para fins exploratórios de auditoria ou comparação, admite-se uma síntese escalar secundária:

$ICP_{Rexp}(a) = \sum w_j(s_{aj}/4)$, com $\sum w_j = 1$, em que a representa o ator, s é um escore ordinal de 0 a 4 e w é o peso previamente justificado para o risco analisado.

O **Índice Experimental de Capacidade Preventiva Relativa (ICP_{Rexp})** não é uma equação de responsabilidade, não mede causalidade, não produz presunção e não possui limiar validado. Como os escores são ordinais, a soma não autoriza interpretação de distância intervalar, significância estatística ou falsa exatidão. Sua função é heurística e documental: tornar explícitos critérios, evidências, incertezas e pesos. Sempre que dois atores apresentarem perfis cruzados ou a ordenação mudar sob pesos plausíveis, a conclusão correta será “indeterminada”, e não a escolha arbitrária de um vencedor numérico.

Quadro 1 — Âncoras ordinais do perfil C-D-A-T-M

Escore	Âncora comum	Exigência documental mínima
0	capacidade inexistente ou juridicamente indisponível para o risco delimitado	demonstrar ausência de acesso, poder ou meio pertinente
1	capacidade marginal, indireta ou apenas reativa	identificar ação excepcional, dependente de terceiro ou posterior ao risco
2	capacidade parcial, com alcance, tempo ou informação limitados	registrar quais etapas podem ser executadas e quais permanecem inacessíveis
3	capacidade substancial, embora não exclusiva	comprovar acesso regular, recursos técnicos e intervenção relevante
4	capacidade direta e dominante sobre a dimensão examinada	comprovar autoridade, dados, recursos e possibilidade de intervenção em escala

Fonte: elaboração própria (2026). Escala experimental, sem validação empírica.

Na aplicação, recomenda-se: definir a funcionalidade e o período antes da pontuação; anexar uma fonte para cada escore; adotar pesos iguais como cenário-base, salvo justificativa prévia; testar ao menos um cenário alternativo de pesos; utilizar dois avaliadores independentes quando o índice integrar auditoria ou perícia; e registrar divergências, dados ausentes e intervalo de incerteza. O perfil, os documentos e a análise de sensibilidade devem ser divulgados juntamente com qualquer valor agregado.

Um exemplo puramente didático esclarece o procedimento. Em controvérsia sobre reprodução automática, um grande fornecedor que controla a funcionalidade, possui telemetria, equipe de teste e capacidade de alteração global poderia receber o perfil (4, 4, 3, 4, 4); uma família com controle apenas sobre o aparelho e a rotina poderia receber (1, 1, 1, 1, 1). Com pesos iguais, os valores ilustrativos seriam 0,95 e 0,25. Esses números não provam defeito, dano ou nexó e não devem ser transportados para caso real: apenas mostram como as premissas precisam ser documentadas. Se a controvérsia envolver contato interpessoal conhecido pela família, os perfis e pesos podem mudar substancialmente.

A intensidade do dever também não decorre do ICPRexp. Deve ser examinada à luz de quatro fatores externos: **previsibilidade do risco**, **vulnerabilidade do grupo**, **benefício econômico** e **disponibilidade de alternativa menos lesiva**. Esses fatores modulam a avaliação jurídica, mas não entram no perfil C-D-A-T-M, evitando dupla contagem. Quanto maior a capacidade de prevenção e mais intensa a combinação dos fatores externos, mais difícil justificar a transferência do encargo a quem apenas reage ao resultado.

5.4 A matriz de posição preventiva

Quadro 2 — Matriz de posição preventiva dos atores

Ator	Conhecimento predominante	Controle direto	Momento e escala	Dever característico
Família	Contexto afetivo, rotina, história individual	Dispositivo, horários e permissões disponíveis	Antes e após sinais perceptíveis; escala individual ou doméstica	Orientar, acompanhar, limitar e buscar ajuda
Escola	Padrões de aprendizagem, convivência e efeitos coletivos	Ambiente pedagógico próprio	Preventivo e reativo; turma ou comunidade escolar	Educar, estabelecer regras, acolher e encaminhar
Fornecedor	Telemetria do serviço, testes, métricas e desempenho de funcionalidades	Interface, padrões, recomendação, notificações, dados e mitigação	Desde a concepção e em tempo real; escala sistêmica	Avaliar risco, proteger por padrão, informar, mitigar e auditar
Estado	Dados regulatórios, denúncias e impacto social agregado	Normas, fiscalização, sanções e políticas públicas	Ex ante e ex post; escala coletiva	Regulamentar, fiscalizar, pesquisar e garantir direitos

Fonte: elaboração própria (2026).

A matriz impede uma falsa hierarquia total de conhecimentos. Pais podem compreender melhor o sofrimento singular; professores podem perceber mais cedo a degradação de um ambiente coletivo; fornecedores podem detectar o comportamento recorrente associado a uma funcionalidade; autoridades podem enxergar efeitos distributivos. A pergunta correta não é quem “sabe mais” em abstrato, mas quem possuía o conhecimento e o controle relevantes para evitar aquele risco.

6 OS PAIS VEEM A CRIANÇA; A PLATAFORMA PODE VER O PERFIL COMPORTAMENTAL

O título do artigo utiliza deliberadamente o verbo **poder**. Nem todo serviço registra cada interação; nem todo dado permite inferência válida; nem toda inferência identifica uma criança; e nenhum perfil comportamental equivale à pessoa. A formulação rigorosa é a seguinte: certos fornecedores dispõem de capacidade técnica e finalidade operacional para registrar sinais como duração de sessão, recorrência, sequência de cliques, respostas a notificações, abandono, repetição, preferências e padrões agregados. Esses sinais podem alimentar segmentação, recomendação,

publicidade, segurança ou melhoria do produto. A relevância jurídica depende de como são coletados, usados, retidos e combinados.

O ECA Digital torna indispensável distinguir finalidades. O artigo 22 veda técnicas de perfilamento para direcionar publicidade comercial a crianças e adolescentes, bem como análise emocional e determinadas tecnologias imersivas para esse fim. Essa proibição não transforma toda personalização em prática equivalente. Devem ser analisados separadamente: perfilamento publicitário proibido; personalização funcional necessária à prestação; tratamento voltado à segurança; métricas agregadas para avaliação de risco; e monitoramento individual invasivo. A denominação empresarial não decide a licitude: finalidade, necessidade, base legal, proporcionalidade, transparência, risco e melhor interesse precisam ser demonstrados (BRASIL, 2025; ANPD, 2023).

O relatório *A Look Behind the Screens*, publicado pela FTC em 2024, oferece evidência institucional circunscrita. Com base em ordens dirigidas a nove grandes empresas de redes sociais e transmissão audiovisual, a agência encontrou coleta extensa de dados de usuários e não usuários, utilização de informações em sistemas automatizados, incentivos econômicos ligados à monetização e salvaguardas inconsistentes para crianças e adolescentes. A FTC também registrou que adolescentes eram frequentemente tratados como adultos e que usuários dispunham de pouco controle sobre certos usos automatizados de seus dados (FTC, 2024). O relatório retrata principalmente práticas de 2019 e 2020; não autoriza generalização temporal, empresarial ou territorial. Demonstra, contudo, que a vantagem informacional e analítica não é mera hipótese teórica em determinados serviços de grande escala.

Também seria incorreto transportar, sem prova, o modelo de negócio das redes sociais para toda inteligência artificial generativa. Assistentes por assinatura, modelos integrados a escolas, buscadores, agentes conversacionais e serviços financiados por publicidade podem coletar sinais diferentes, perseguir métricas diferentes e controlar funcionalidades distintas. A análise deve identificar o produto, a finalidade e a arquitetura efetivos. O ponto comum não é uma suposta intenção universal de manipular, mas a obrigação de avaliar riscos sempre que o sistema puder adaptar respostas, reter histórico, personalizar interações ou incentivar continuidade de uso por crianças e adolescentes.

Essa vantagem informacional é uma manifestação da assimetria de capacidade preventiva. A família conhece o cotidiano, mas não vê os testes internos, as métricas de retenção, a distribuição de exposição nem as decisões que alteraram o fluxo. O fornecedor pode não conhecer a criança como sujeito biográfico, mas, conforme o serviço, consegue observar o comportamento produzido dentro de seu sistema com granularidade muito superior. Quando dados são utilizados para otimizar engajamento, mas não há documentação comparável sobre testes de segurança, surge uma pergunta verificável de coerência preventiva: quais métricas, experimentos e salvaguardas foram empregados para avaliar riscos previsíveis?

O ECA Digital oferece resposta normativa ao exigir gerenciamento de riscos, configuração protetiva, relatórios de impacto em hipóteses relevantes e revisão regular de ferramentas de inteligência artificial. A lei não presume onisciência do fornecedor. Exige diligência compatível com as capacidades que ele efetivamente possui e com o risco de seu serviço. Esse ponto é decisivo: não se cobra previsão impossível, mas a ausência de dados, testes ou documentação sob controle do próprio fornecedor não pode ser tratada automaticamente como imprevisibilidade.

A diferença também aparece na temporalidade. Uma família tende a reconhecer o problema por sinais externos: alteração de sono, irritabilidade, queda de rendimento, isolamento, conflito ou

gasto. O fornecedor pode observar padrões dentro do serviço antes que se tornem legíveis fora dele. A plataforma não deve diagnosticar saúde mental sem base jurídica, finalidade legítima e salvaguardas — prática que criaria novos riscos de vigilância e discriminação. Ainda assim, pode avaliar o impacto de suas próprias funcionalidades por métricas de segurança menos invasivas, testes controlados, indicadores agregados e pontos de parada não manipulativos.

Portanto, a solução não é ampliar indiscriminadamente a vigilância empresarial sobre crianças. É subordinar a capacidade já existente aos princípios de minimização, finalidade, melhor interesse, segurança e prestação de contas, conforme também recomenda a orientação do UNICEF para sistemas de inteligência artificial voltados ou acessíveis a crianças (UNICEF, 2025). **O contrário da opacidade não é monitoramento ilimitado; é governança demonstrável.**

7 A ESCOLA E A TRANSFERÊNCIA DE CUSTOS PREVENTIVOS

O debate sobre infância digital costuma atribuir à escola uma tarefa dupla. De um lado, espera-se que incorpore tecnologias, forme para o mundo digital e ensine uso crítico de inteligência artificial. De outro, exige-se que neutralize distração, desinformação, conflitos, desigualdade de acesso, automatização indevida de tarefas e efeitos sobre atenção. As duas tarefas são legítimas; o problema reside em considerar a segunda uma substituta dos deveres de quem projeta o serviço.

A escola atua sobre consequências que chegam acompanhadas de múltiplas causas. Queda de rendimento, ansiedade ou privação de sono não podem ser automaticamente imputadas a uma plataforma. Ambiente familiar, condições econômicas, saúde, violência, carga escolar e outros fatores precisam ser considerados. A mesma cautela, entretanto, vale no sentido inverso: não é racional excluir a contribuição de funcionalidades digitais sem examinar exposição, padrões de uso e decisões arquiteturais.

Quando um serviço extrai valor da retenção e os custos de uso problemático são absorvidos por famílias, escolas, saúde pública e assistência social, pode ocorrer transferência ou externalização de **custos sociais, educacionais e preventivos**. A receita permanece privada; o trabalho de recompor atenção, convivência e bem-estar é distribuído socialmente. Essa externalização não se presume. Ela deve ser demonstrada por evidências de risco previsível, contribuição da arquitetura e insuficiência de mitigação. Também não deve ser excluída apenas porque os custos surgem fora do balanço do fornecedor (GENOVA, 2026).

As recomendações internacionais adotam uma lógica complementar. O Comitê dos Direitos da Criança defende alfabetização digital para crianças, pais e educadores, mas também exige que empresas realizem devida diligência e respeitem direitos desde a concepção (ONU, 2021). As diretrizes da Comissão Europeia sobre proteção de menores no âmbito do Digital Services Act recomendam contas privadas por padrão, ajustes nos sistemas de recomendação, prioridade a sinais explícitos em vez de sinais comportamentais e medidas contra design viciante ou uso problemático (COMISSÃO EUROPEIA, 2025). O relatório das National Academies combina formação docente com padrões de design, transparência, acesso a dados para pesquisa e auditoria de algoritmos (NASEM, 2024).

Esses documentos convergem em um ponto: letramento digital e segurança por concepção são camadas cumulativas. Ensinar uma criança a resistir a um fluxo otimizado para reduzir pontos de parada pode aumentar sua autonomia, mas não legitima o fluxo. Formar professores para reconhecer persuasão algorítmica é necessário, mas não substitui o dever de testar se a arquitetura explora sensibilidade a recompensas, pertencimento ou urgência.

A escola deve ser parceira da governança, e não destinatária automática de custos que não controla. Isso requer canais eficazes de denúncia, relatórios acessíveis, dados para pesquisa independente, protocolos de encaminhamento e mecanismos pelos quais instituições educacionais possam informar riscos recorrentes sem suportar sozinhas a prova de processos internos inacessíveis.

8 UM PROTOCOLO OPERACIONAL DE ATRIBUIÇÃO

A assimetria de capacidade preventiva pode ser convertida em protocolo para avaliação regulatória, pericial ou judicial. O objetivo não é criar um atalho condenatório, mas substituir impressões genéricas por perguntas verificáveis.

8.1 Passo 1 — delimitar a funcionalidade e o risco

Deve-se abandonar a pergunta ampla “a plataforma fez mal?” e identificar o objeto: reprodução automática, rolagem contínua, notificação, recomendação personalizada, recompensa por sequência de uso, publicidade perfilada, agente conversacional, compra facilitada, barreira ao cancelamento ou outro mecanismo. Em seguida, define-se o risco alegado, a população atingida e o período de exposição.

8.2 Passo 2 — reconstruir a arquitetura de escolha

É necessário registrar padrões, opções disponíveis, número de etapas, linguagem, saliência visual, pontos de parada, possibilidade de desativação e comportamento da funcionalidade para contas de diferentes idades. Capturas de tela isoladas são úteis, mas insuficientes quando o sistema é dinâmico. Testes reproduzíveis, contas controladas, documentação de versão e comparação entre configurações aumentam a força probatória.

8.3 Passo 3 — mapear conhecimento e controle

Para cada ator, aplica-se a matriz C-D-A-T-M: controle arquitetural, dados, análise, temporalidade/escala e meios de mitigação. Do lado do fornecedor, podem ser relevantes avaliações de impacto, registros de alteração, testes A/B, métricas de segurança, reclamações, documentos de produto, critérios de recomendação, incidentes e justificativas para padrões adotados. Do lado familiar, importam regras domésticas, comunicações, uso de controles, conhecimento do risco e respostas a sinais observáveis. Na escola, registros pedagógicos e mudanças coletivas podem contextualizar temporalidade e impacto.

8.4 Passo 4 — testar previsibilidade e alternativas

O risco era conhecido ou razoavelmente cognoscível? Havia alertas regulatórios, estudos, reclamações internas ou resultados de teste? Existiam alternativas tecnicamente disponíveis e menos lesivas, como ponto natural de parada, frequência reduzida de notificações, recomendação não personalizada ou padrão mais protetivo? A existência de alternativa não prova defeito, mas reduz a força da justificativa baseada em inevitabilidade.

8.5 Passo 5 — examinar mitigação efetiva, não apenas nominal

A presença de “controle parental” não encerra a análise. É preciso verificar se ele vem ativado por padrão, pode ser encontrado e compreendido, oferece granularidade adequada, resiste a caminhos de desativação persuasivos e produz resultado mensurável. Uma ferramenta escondida em menus

complexos ou neutralizada por notificações insistentes pode cumprir formalmente uma política e falhar materialmente como salvaguarda.

8.6 Passo 6 — reconstruir dano e causalidade

O protocolo preventivo não elimina os elementos da responsabilidade civil. Deve-se demonstrar dano juridicamente relevante e relação causal ou concausal. A análise inclui intensidade e duração da exposição, compatibilidade temporal, mecanismo plausível, condições preexistentes, outras causas, conduta da vítima e dos responsáveis, além de eventuais benefícios do serviço. Em fenômenos multicausais, a pergunta não é apenas se a arquitetura foi causa única, mas se contribuiu de forma juridicamente relevante para produzir ou agravar o resultado.

8.7 Quadro de evidências mínimas

Quadro 3 — Protocolo mínimo de evidências

Questão	Evidência do fornecedor	Evidência externa ou do usuário	Resultado esperado
Qual funcionalidade operou?	documentação de produto, versões, parâmetros	testes controlados, registros e capturas	objeto técnico delimitado
O risco era cognoscível?	avaliações, incidentes, reclamações, testes	literatura, alertas oficiais, relatos convergentes	previsibilidade graduada
Quem podia intervir?	permissões internas, recursos e tempo de resposta	controles disponíveis a pais e escolas	perfil C-D-A-T-M comparativo
Havia alternativa menos lesiva?	experimentos, justificativas e compensações de projeto	padrões técnicos e comparação de mercado	evitabilidade do risco
A mitigação funcionava?	métricas de eficácia e auditorias	experiência de uso, acessibilidade e resultados	segurança demonstrável
Houve contribuição para o dano?	dados de exposição e funcionamento	prontuários, rotina, temporalidade e causas concorrentes	nexo ou concausalidade avaliados

Fonte: elaboração própria (2026).

O protocolo também protege fornecedores contra atribuições especulativas: documentação de avaliação adequada, padrão protetivo, resposta diligente, ausência de exposição relevante ou causa externa exclusiva enfraquece a imputação. Transparência qualificada diferencia falha arquitetural de resultado inevitável ou alheio ao serviço.

9 REPERCUSSÕES PARA A RESPONSABILIDADE CIVIL

9.1 Relação de consumo e defeito da arquitetura própria

A incidência do Código de Defesa do Consumidor deve ser verificada no caso concreto, conforme os sujeitos, a destinação do serviço, a atividade do fornecedor e a forma direta ou indireta de remuneração. Quando configurada a relação de consumo, o CDC reconhece a vulnerabilidade do consumidor, assegura informação adequada, prevenção de danos e facilitação da defesa de direitos. Nos termos do artigo 14, o fornecedor responde objetivamente por defeitos do serviço e por informações insuficientes ou inadequadas sobre fruição e riscos. O serviço é defeituoso quando não oferece a segurança legitimamente esperada, consideradas a forma de fornecimento, os riscos razoáveis e a época (BRASIL, 1990b; MIRAGEM, 2024; MARTINS, 2020).

Em serviços digitais, o modo de fornecimento pode incluir a arquitetura própria: padrões, interface, recomendação, notificações, controles, autenticação, fluxo de saída e medidas de segurança. Se a funcionalidade foi desenhada para crianças ou por elas provavelmente acessada, a expectativa legítima de segurança é informada pela proteção integral, pelo melhor interesse e pelas obrigações específicas do ECA Digital. A simples utilização intensa não prova defeito; tampouco a alegação genérica de “mau uso” exclui a análise de como o serviço sustentou, induziu ou dificultou a interrupção desse uso.

Para fins analíticos deste artigo — e não como classificação legal exaustiva — a falha arquitetural pode ser investigada como: **falha de concepção**, quando alternativa razoável poderia reduzir risco relevante; **falha de informação**, quando riscos e controles não são apresentados com clareza adequada à idade; **falha de configuração-padrão**, quando a opção inicial favorece exposição desnecessária; e **falha de mitigação**, quando sinais cognoscíveis de risco não são acompanhados por teste ou correção proporcional. A classificação apenas organiza a prova; não dispensa a demonstração do defeito jurídico, do dano e do nexo.

9.2 Arquitetura própria, conteúdo de terceiros e esfera de atuação

É necessário separar danos atribuídos ao conteúdo produzido por terceiros de danos alegadamente associados a decisões próprias do serviço. O artigo 19 do Marco Civil da Internet foi redigido para a responsabilidade por conteúdo de terceiros. No Tema 987, concluído após embargos em 17 de junho de 2026, o STF reconheceu sua inconstitucionalidade parcial e progressiva e definiu regime transitório de responsabilização, inclusive deveres estruturais e hipóteses de falha sistêmica, até que sobrevenha nova legislação (BRASIL, 2014; STF, 2026).

Este artigo não propõe transpor automaticamente esse regime para qualquer dano digital. Seu objeto principal é a arquitetura sob controle do próprio fornecedor. A distinção evita dois erros opostos: usar a proteção relativa ao conteúdo de terceiros como imunidade para decisões próprias de produto ou, inversamente, imputar ao fornecedor todo fato ocorrido depois que o usuário acessou o serviço.

A esfera efetiva de atuação permanece limite causal. No REsp 2.250.674/MG, a Terceira Turma do STJ afastou a responsabilidade de uma plataforma de intermediação quando a fraude ocorreu em carteira externa, sob custódia de outra empresa, e não se comprovou falha do serviço prestado pela ré (STJ, 2026). O precedente não trata de infância ou arquitetura persuasiva, mas oferece um contrapeso metodológico útil: capacidade preventiva deve ser vinculada à funcionalidade, ao serviço efetivamente executado e ao ponto da cadeia em que o dano ocorreu.

9.3 Melhor interesse, dados, perfilamento e autonomia progressiva

O artigo 14 da LGPD exige que o tratamento de dados de crianças e adolescentes observe seu melhor interesse e que informações sejam simples, claras e acessíveis. O Enunciado CD/ANPD nº 1/2023 esclarece que as hipóteses dos artigos 7º e 11 da LGPD podem fundamentar o tratamento, desde que o melhor interesse seja observado e prevaleça no caso concreto. Logo, o consentimento parental específico e destacado, quando aplicável, não é a única base possível nem funciona como autorização geral. Finalidade, adequação, necessidade, segurança, prevenção, não discriminação e responsabilização permanecem exigíveis (BRASIL, 2018; ANPD, 2023).

No plano mais específico, o artigo 22 do ECA Digital veda o perfilamento para publicidade comercial dirigida a crianças e adolescentes. Essa proibição deve ser articulada com a distinção já

proposta entre personalização funcional, tratamento de segurança, métricas agregadas e monitoramento individual invasivo. A finalidade protetiva não legitima coleta ilimitada, e a ausência de publicidade não torna automaticamente lícito qualquer perfil comportamental.

A autonomia progressiva evita outra distorção: proteção não significa vigilância total nem exclusão indiscriminada. Crianças e adolescentes são sujeitos de direitos, inclusive de expressão, participação, privacidade e acesso a oportunidades digitais. As medidas devem ser proporcionais à idade, ao risco e à finalidade. O objetivo é ampliar condições de decisão, não trocar o controle opaco da plataforma por controle doméstico absoluto.

Em 14 de agosto de 2026, a implementação administrativa do ECA Digital ainda se encontrava em etapas. A ANPD havia publicado orientações preliminares, iniciado monitoramento e previsto período de adaptação e consolidação de parâmetros de aferição de idade entre agosto e novembro de 2026, sem prejuízo de outras ações fiscalizatórias. Por isso, este artigo trata como vigentes os deveres legais e regulamentares já editados, mas não presume que todos os parâmetros procedimentais secundários estejam definitivamente consolidados (ANPD, 2026).

9.4 Conduta dos responsáveis, exclusividade e concorrência causal

O dever familiar permanece juridicamente relevante. Omissão grave, desativação consciente de salvaguardas, fornecimento de informação falsa sobre idade ou descumprimento reiterado de orientação específica podem contribuir para o resultado e devem ser examinados. Contudo, o artigo 14, § 3º, II, do CDC exige culpa **exclusiva** do consumidor ou de terceiro para afastar integralmente a responsabilidade objetiva. Em cenário concausal, a conduta familiar não apaga automaticamente eventual defeito do serviço.

A culpa concorrente, quando juridicamente cabível, requer prova de conduta causalmente relevante e pode repercutir na quantificação segundo o artigo 945 do Código Civil; não constitui rótulo moral nem presunção derivada do simples acesso da criança ao serviço (BRASIL, 2002). A jurisprudência do STJ admite a culpa concorrente do consumidor como possível fator de redução, sem convertê-la em excludente total, e também rejeita sua aplicação quando o dano decorre de falha de segurança e não há assunção consciente do risco pela vítima (STJ, 2023; STJ, 2025).

A tese da assimetria de capacidade preventiva ajuda a evitar raciocínio circular. Não se pode exigir que pais neutralizem uma funcionalidade cujo risco não foi informado, cujo controle é oculto ou cuja operação muda sem transparência e, depois, usar a ausência de neutralização como prova de exclusividade causal. Para que a conduta familiar seja valorada com rigor, é necessário demonstrar o que os responsáveis podiam conhecer, quais meios efetivos possuíam e se sua intervenção teria evitado o dano apesar da arquitetura.

9.5 Distribuição da prova e assimetria informacional

A assimetria de capacidade preventiva não inverte automaticamente o ônus da prova. O autor deve delimitar a funcionalidade, apresentar elementos mínimos de exposição, indicar o dano e oferecer hipótese causal plausível. A inversão prevista no artigo 6º, VIII, do CDC e a distribuição dinâmica do artigo 373, § 1º, do CPC dependem de decisão fundamentada, das peculiaridades do caso e da maior facilidade concreta de uma parte produzir a prova contrária; a parte onerada deve receber oportunidade efetiva de cumprir o encargo (BRASIL, 1990b; BRASIL, 2015).

A jurisprudência fornece parâmetros úteis, sem resolver antecipadamente litígios digitais. No REsp 1.955.890/SP, relativo a acidente de consumo por produto, o STJ exigiu do consumidor a

demonstração da relação entre produto e dano e atribuiu ao fornecedor o ônus de comprovar a inexistência de defeito ou excludente. No REsp 2.097.352/SP, o Tribunal reconheceu a relevância da assimetria técnica, informacional e econômica e da maior facilidade de provar o fato contrário. Aplicados com cautela, esses critérios sustentam pedidos de documentação sobre versões, testes, avaliações de risco e métricas que se encontram exclusivamente sob controle empresarial, mas não dispensam o início de prova nem autorizam devassa genérica (STJ, 2021; STJ, 2024).

9.6 Critérios convergentes de atribuição restrita

Uma responsabilidade civil por arquitetura digital deve ser ampla na investigação e restrita na conclusão. A imputação ganha consistência quando convergem **controle relevante sobre a funcionalidade; risco previsível ou razoavelmente cognoscível; vulnerabilidade infantojuvenil pertinente; benefício econômico associado à arquitetura ou à ausência de mitigação; opacidade impeditiva de escolha ou controle informado; alternativa razoável e menos lesiva; falha de prevenção, informação ou mitigação; e contribuição causal ou concausal para dano demonstrado.**

Nenhum fator, isoladamente, basta. Uma plataforma lucrativa não responde por todo sofrimento de seus usuários; uma interface persuasiva não produz necessariamente dano; a vulnerabilidade da criança não elimina sua autonomia; a ausência de transparência não prova causalidade. É a convergência probatória que transforma uma crítica social em atribuição jurídica responsável.

10 OBJEÇÕES, RISCOS DA TESE E LIMITES

Uma categoria nova deve sobreviver às objeções mais fortes, inclusive àquelas que expõem seus possíveis abusos.

10.1 “Pais têm o dever de educar; logo, a diferença está neles”

A premissa é verdadeira e a conclusão não decorre dela. O dever de cuidado familiar coexiste com deveres de produto. Em outras áreas, orientar uma criança a atravessar a rua não autoriza a supressão de sinalização; ensinar consumo consciente não legitima publicidade abusiva; explicar privacidade não dispensa segurança de dados. A família influencia a experiência, mas não controla a infraestrutura.

10.2 “O produto é neutro; o problema é o uso”

Serviços digitais não são causalmente onipotentes, mas tampouco são recipientes vazios. Padrões, ordenação, recomendação, fricção, recompensa e notificações alteram probabilidades de ação. A neutralidade precisa ser demonstrada no nível da funcionalidade e não afirmada por rótulo. Ao mesmo tempo, reconhecer influência arquitetural não autoriza concluir que todo comportamento foi determinado pelo sistema.

10.3 “Controles parentais já existem”

Existência formal não equivale a eficácia. O ECA Digital exige acessibilidade, proteção elevada por padrão, informações claras e controles que não sejam enfraquecidos por interfaces manipulativas. A avaliação deve considerar descoberta, compreensão, ativação, persistência e

resultado. Controles eficazes também reforçam a autonomia familiar; controles meramente simbólicos transferem reputacionalmente o risco sem transferir poder real.

10.4 “A tese incentiva vigilância e paternalismo”

Esse risco é real. Se mal aplicada, a busca por prevenção pode legitimar coleta adicional de dados, restrição excessiva e apagamento da voz de crianças e adolescentes. Por isso, a capacidade preventiva deve ser exercida sob minimização, finalidade, proporcionalidade, privacidade e participação. O artigo não propõe perfilamento emocional para proteger crianças; propõe testes de produto, dados agregados, configurações seguras e prestação de contas. A autonomia progressiva é critério de desenho, não obstáculo à proteção.

10.5 “Não há prova causal suficiente sobre saúde mental”

A objeção exige precisão. As National Academies apontaram limitações severas da evidência causal em nível populacional e recomendaram estudos de funcionalidades específicas, auditorias e acesso a dados. O U.S. Surgeon General afirmou, por sua vez, que não se pode concluir que redes sociais sejam suficientemente seguras para crianças e adolescentes e recomendou ação multifacetada de famílias, empresas e governos (HHS, 2023; NASEM, 2024). A resposta jurídica adequada não é declarar causalidade universal nem esperar certeza absoluta. É separar prevenção baseada em risco de reparação baseada em prova individualizada.

10.6 “A inovação será inviabilizada”

O ECA Digital considera funcionalidades, riscos e porte. Segurança por concepção não exige risco zero, mas processo responsável, documentação e melhoria. Regras claras podem favorecer inovação ao diferenciar diligência de vantagem competitiva obtida pela externalização de custos.

10.7 Limitações da proposta

Este estudo é jurídico-documental e exploratório. Não mede danos na população brasileira, não observa diretamente decisões internas de fornecedores e não estabelece causalidade entre uma funcionalidade e um resultado individual. O levantamento, embora explicita bases, termos e critérios, não é revisão sistemática nem pretende exaurir a literatura multidisciplinar. O recorte temporal também importa: a implementação administrativa do ECA Digital permanecia em desenvolvimento na data de encerramento da pesquisa.

O perfil C-D-A-T-M e o ICPRexp ainda não foram submetidos a validação de construto, confiabilidade entre avaliadores ou teste empírico em amostra de casos. Não há pesos estimados, limiar decisório ou interpretação intervalar legítima. A agregação de escores ordinais pode ocultar perfis distintos; por isso, o vetor dimensional, as fontes, as divergências e a análise de sensibilidade têm precedência sobre o número agregado. Até que estudos independentes demonstrem validade e utilidade, o índice não deve fundamentar sozinho decisão regulatória, pericial ou judicial.

Há, por fim, um limite de acesso. Parte relevante das evidências sobre versões, testes, métricas e incidentes permanece sob controle empresarial. Um programa empírico futuro deverá aplicar o protocolo a funcionalidades delimitadas, comparar codificadores independentes, testar pesos e cenários, incorporar a participação de crianças, responsáveis e educadores e examinar desigualdades de renda, raça, gênero, deficiência e território. Transparência qualificada, relatórios de impacto,

fiscalização da ANPD e acesso responsável de pesquisadores serão necessários para converter a categoria em instrumento empiricamente refutável, e não apenas doutrinário.

11 CONCLUSÃO

O debate público acerta ao insistir que pais conversem, acompanhem e ensinem seus filhos a perguntar. Erra quando converte essa verdade em teoria suficiente de segurança digital. Uma criança não interage apenas com uma resposta de inteligência artificial ou uma postagem; interage com um ambiente que organiza padrões, saliências, sequências, recompensas, notificações e possibilidades de saída. A família não projetou esse ambiente, e a escola não opera seus sistemas de recomendação.

À pergunta de pesquisa, a análise oferece uma resposta condicionada: a responsabilidade compartilhada não autoriza transferir o principal encargo de prevenção de um risco arquitetural a pais ou professores quando, para a funcionalidade delimitada, o fornecedor detém capacidade materialmente superior de conhecer, controlar e mitigar esse risco. Essa conclusão é jurídico-analítica, não causal ou estatística. Não estabelece que o fornecedor sempre possua a maior capacidade, nem que responda por todo resultado ocorrido no serviço.

A **assimetria de capacidade preventiva** organiza a investigação sem abolir a agência individual. Famílias possuem conhecimento relacional; escolas, conhecimento pedagógico e coletivo; fornecedores, conhecimento operacional e controle arquitetural; o Estado, poder normativo e fiscalizatório. O perfil C-D-A-T-M torna essas capacidades comparáveis. O ICPRexp pode documentar premissas e testar a estabilidade de uma ordenação, mas permanece heurística experimental: não prova defeito, ilicitude, dano ou nexo e não cria presunção de responsabilidade.

O ECA Digital e o Decreto nº 12.880/2026 expressam elementos compatíveis com essa distribuição funcional. Preservam o cuidado parental e, simultaneamente, exigem gerenciamento de riscos, proteção por padrão, controles acessíveis e restrições a mecanismos que comprometam autonomia ou explorem vulnerabilidades cognitivas e etárias. No campo reparatório, contudo, permanecem indispensáveis a delimitação do serviço e da funcionalidade, a demonstração do defeito ou da ilicitude, do dano e da contribuição causal ou concausal, bem como o exame de causas externas, condutas concorrentes e esfera efetiva de atuação.

No plano probatório, a proposta substitui a acusação genérica por perguntas controláveis: quem podia conhecer o risco; quem podia modificar sua fonte; quais alternativas existiam; quais medidas foram testadas; que exposição ocorreu; e que causas concorrentes permanecem plausíveis. A documentação sob controle exclusivo do fornecedor pode justificar distribuição probatória adequada, mas não dispensa um objeto técnico delimitado nem um início de prova.

Pais veem a criança em sua história e em seus vínculos. A plataforma pode ver um perfil comportamental limitado ao ambiente que opera. Nenhuma dessas perspectivas é completa. Quando o risco alegado nasce de uma decisão de produto, porém, não se pode exigir que o olhar doméstico substitua o controle técnico. **Educar para resistir é necessário; projetar para não explorar é dever de quem detém a arquitetura.**

DECLARAÇÕES EDITORIAIS

Autoria e responsabilidade

O autor declara ter definido o problema de pesquisa, a tese, a estrutura, os critérios de análise, as interpretações jurídicas e as conclusões; ter revisado as fontes, as citações e a versão final; e assumir integral responsabilidade pelo conteúdo publicado.

Financiamento e conflitos de interesse

A pesquisa foi desenvolvida de forma independente, sem financiamento externo. O autor declara não possuir conflitos de interesse pertinentes ao objeto do artigo.

Uso de inteligência artificial

Ferramentas de inteligência artificial generativa da OpenAI foram utilizadas como apoio à descoberta bibliográfica, à revisão linguística e de consistência, à conferência formal de referências e à programação do documento. A IA não foi tratada como autora, fonte probatória ou substituta da avaliação jurídica. A seleção dos argumentos, a interpretação das fontes e a decisão de publicação permanecem sob responsabilidade humana do autor.

Dados, materiais e ética

O artigo utiliza exclusivamente fontes públicas indicadas nas referências e não criou conjunto de dados pessoais ou sensíveis. Não houve entrevistas, experimentos ou participação de seres humanos; por isso, não se aplica submissão a comitê de ética em pesquisa. Materiais documentais adicionais podem ser solicitados ao autor pelo e-mail informado na identificação.

REFERÊNCIAS

- AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Enunciado CD/ANPD nº 1, de 22 de maio de 2023: tratamento de dados pessoais de crianças e adolescentes**. Brasília, DF: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes>. Acesso em: 14 ago. 2026.
- AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ECA Digital**. Brasília, DF: ANPD, 2026. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/eca-digital>. Acesso em: 14 ago. 2026.
- BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 ago. 2026.
- BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990a. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18069.htm. Acesso em: 14 ago. 2026.
- BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990b. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 14 ago. 2026.
- BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/10406compilada.htm. Acesso em: 14 ago. 2026.
- BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 14 ago. 2026.
- BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm. Acesso em: 14 ago. 2026.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 14 ago. 2026.
- BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/115211.htm. Acesso em: 14 ago. 2026.
- BRASIL. **Decreto nº 12.880, de 18 de março de 2026**. Regulamenta a Lei nº 15.211/2025 e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm. Acesso em: 14 ago. 2026.

- CALABRESI, Guido. **The costs of accidents: a legal and economic analysis**. New Haven: Yale University Press, 1970.
- CETIC.BR. **TIC Kids Online Brasil 2025: crianças e adolescentes**. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2025a. Disponível em: <https://cetic.br/pt/pesquisa/kids-online/indicadores/>. Acesso em: 14 ago. 2026.
- CETIC.BR. **TIC Kids Online Brasil 2025: pais e responsáveis — mediação técnica realizada sobre o uso da Internet**. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2025b. Disponível em: <https://cetic.br/pt/tics/kidsonline/2025/pais/F/>. Acesso em: 14 ago. 2026.
- COMISSÃO EUROPEIA. **Guidelines on the protection of minors under the Digital Services Act**. Bruxelas, 14 jul. 2025. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>. Acesso em: 14 ago. 2026.
- DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da LGPD**. 3. ed. São Paulo: Revista dos Tribunais, 2021.
- FEDERAL TRADE COMMISSION (FTC). **A look behind the screens: examining the data practices of social media and video streaming services**. Washington, DC: FTC, 2024. Disponível em: <https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services>. Acesso em: 14 ago. 2026.
- GENOVA, Jandislei Antonio. **A monetização da vulnerabilidade: plataformas digitais, vício, ódio e responsabilidade civil na era algorítmica**. São Paulo: Dialética, no prelo, 2026.
- GRAY, Colin M. et al. The dark (patterns) side of UX design. In: **CHI Conference on Human Factors in Computing Systems**. New York: ACM, 2018. p. 1–14. DOI: <https://doi.org/10.1145/3173574.3174108>.
- MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na internet**. 3. ed. São Paulo: Revista dos Tribunais, 2020.
- MATHUR, Arunesh et al. Dark patterns at scale: findings from a crawl of 11K shopping websites. **Proceedings of the ACM on Human-Computer Interaction**, New York, v. 3, n. CSCW, art. 81, 2019. DOI: <https://doi.org/10.1145/3359183>.
- MIRAGEM, Bruno. **Curso de direito do consumidor**. 9. ed. Rio de Janeiro: Forense, 2024.
- NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE (NASEM). **Social media and adolescent health**. Washington, DC: The National Academies Press, 2024. DOI: <https://doi.org/10.17226/27396>.
- ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Comitê dos Direitos da Criança. **General comment No. 25 (2021) on children's rights in relation to the digital environment**. Genebra: ONU, 2021. Disponível em: <https://digitallibrary.un.org/record/3906061>. Acesso em: 14 ago. 2026.
- SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Recurso Especial nº 1.955.890/SP**. Relatora: Ministra Nancy Andrighi. Terceira Turma, julgado em 5 out. 2021, DJe 8 out. 2021. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/18022022-Cabe-ao-fornecedor-comprovar-inexistencia-de-defeito-em-acao-de-consumo--afirma-Terceira-Turma.aspx>. Acesso em: 14 ago. 2026.
- SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Recurso Especial nº 1.742.102/MG**. Relator: Ministro Marco Buzzi. Quarta Turma, julgado em 23 mar. 2023, DJe 4 abr. 2023.
- SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Recurso Especial nº 2.097.352/SP**. Relatora: Ministra Nancy Andrighi. Terceira Turma, julgado em 19 mar. 2024, DJe 22 mar. 2024. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/08082024-Cabe-inversao-do-onus-da-prova-em-acao-que-discute-vicios-de-construcao-em-imovel-para-baixa-renda.aspx>. Acesso em: 14 ago. 2026.
- SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Recurso Especial nº 2.220.333/DF**. Relator: Ministro Ricardo Villas Bôas Cueva. Terceira Turma, DJe 13 out. 2025. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/13112025-Falha-de-seguranca-do-banco-afasta-alegacao-de-culpa-concorrente-do-consumidor-em-caso-de-golpe.aspx>. Acesso em: 14 ago. 2026.
- SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Recurso Especial nº 2.250.674/MG**. Relator: Ministro Ricardo Villas Bôas Cueva. Terceira Turma, julgado em 7 abr. 2026, DJe 10 abr. 2026. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2026/21052026-Plataforma-de-intermediacao-nao-responde-por-envio-de-criptomoedas-a-carteira-falsa-de-outra-corretora.aspx>. Acesso em: 14 ago. 2026.
- SUPREMO TRIBUNAL FEDERAL (STF). **Recurso Extraordinário nº 1.037.396/SP (Tema 987 da repercussão geral)**. Relator: Ministro Dias Toffoli. Tribunal Pleno. Embargos de declaração concluídos em 17 jun. 2026. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?classeProcesso=RE&incidente=5160549&numeroProcesso=1037396&numeroTema=987>. Acesso em: 14 ago. 2026.
- SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. Online manipulation: hidden influences in a digital world. **Georgetown Law Technology Review**, Washington, DC, v. 4, n. 1, p. 1–45, 2019. Disponível em: <https://georgetownlawtechreview.org/online-manipulation-hidden-influences-in-a-digital-world/GLTR-01-2020/>. Acesso em: 14 ago. 2026.
- UNITED NATIONS CHILDREN'S FUND (UNICEF). **Guidance on AI and children: version 3.0**. Florence: UNICEF Innocenti, 2025. Disponível em: <https://www.unicef.org/innocenti/reports/policy-guidance-ai-children>. Acesso em: 14 ago. 2026.
- UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS). Office of the Surgeon General. **Social media and youth mental health: the U.S. Surgeon General's advisory**. Washington, DC: HHS, 2023. Disponível em: <https://www.hhs.gov/surgeongeneral/reports-and-publications/youth-mental-health/social-media/index.html>. Acesso em: 14 ago. 2026.